Issues for Consideration: Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Bill, 2016

The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Bill, 2016 was introduced in Lok Sabha on March 3, 2016.[1] Some issues in the Bill are presented below:

1. Allowing private agencies to use Aadhaar contradicts statement of objects and reasons of the Bill

Clause 7 of the Bill: *The government, for the purpose of delivering subsidies, benefits or services, may require an individual to: (i) verify his identity under Aadhaar, (ii) show proof of possessing an Aadhaar number, or (iii) if a person does not have Aadhaar, enrol for Aadhaar. Further, if a person does not have Aadhaar, the Bill requires that an alternative be provided to establish his identity.*

Clause 57 of the Bill: *Any public or private person may use the Aadhaar number for establishing the identity of any individual for any purpose.*

Issue: The Statement of Objects and Reasons of the Bill states that identification of targeted beneficiaries for delivery of various government subsidies and services has become a challenge for the government. The Bill allows the government to establish Aadhaar as a means of identification to ensure efficient and targeted delivery of government subsidies and services. At the time of the introduction of the Bill, the government stated that "the Bill confines itself only to governmental expenditure."[2]

However, the Bill also allows private persons to use Aadhaar as a proof of identity for any purpose. This provision will enable private entities such as, airline, telecom, insurance, real estate etc. companies, to require Aadhaar as a proof of identity for availing their services.

2. Issues with sharing information collected under Aadhaar

Under the Bill, the UID authority maintains a database which includes: (i) identity information of individuals which includes biometric information, demographic information and Aadhaar number, and (ii) authentication records of an individual's identity (i.e. time of request, identity of the entity requesting for authentication, and the response provided). The Bill prohibits the UID authority from sharing this information with anyone. This information may be disclosed in the interest of national security, or on the orders of a court.

In this context, we highlight some specific issues related to: (i) power to order disclosure of information in the interest of national security, and (ii) the potential to profile individuals using Aadhaar.

Note that provisions in the Bill with regard to protection of identity information and authentication records may be affected by an ongoing writ petition in the Supreme Court.[3] The petition claims that Aadhaar may be in violation of right to privacy. A five judge bench of the court is examining whether right to privacy is a fundamental right.

Disclosure of information to intelligence or law enforcement agencies

Clause 33(2) of the Bill: *Identity information and authentication records may be disclosed in the interest of national security. This will be on the direction of an officer who is at least a Joint Secretary in the central government. Such a direction has to be reviewed by an Oversight Committee (comprising Cabinet Secretary, Secretaries of Legal Affairs and Information Technology) and will be valid for 6 months.*

Issue: The provisions regulating disclosure of private information under the Bill differ from guidelines specified under another law. In 1996, the Supreme Court interpreted provisions under the Indian Telegraph Act, 1885 with regard to the state being allowed to tap telephones. The Court held that the state may tap telephones only at the occurrence of any public emergency or in the interest of public safety if: (i) it is authorised by the Home Secretary of the central or state government; and (ii) it is for a maximum period of six months. Each order of telephone tapping must also be investigated by a separate Review Committee within a period of two months from the date of issuance.[4]

The Bill differs from the guidelines for phone tapping in the following two ways. First, the Bill permits sharing in the interest of 'national security' rather than for public emergency or public safety. Second, the order can be issued by an officer of the rank of Joint Secretary, instead of a Home Secretary. Under the Indian Telegraph Act, 1885 it is only in 'urgent situations' that directions for phone tapping may be given by a Joint Secretary.[5]

Mandira Kala mandira@prsindia.org | **Anviti Chaturvedi** anviti@prsindia.org | **Roopal Suhag** roopal@prsindia.org | **March 9, 2016**

Potential to profile individuals

Issue: The Bill does not specifically prohibit law enforcement and intelligence agencies from using the Aadhaar number as a link (key) across various datasets (such as telephone records, air travel records, etc.) in order to recognise patterns of behaviour.

Techniques such as running computer programmes across datasets for pattern recognition can be used for various purposes such as detecting potential illegal activities.[6] However, these can also lead to harassment of innocent individuals who get identified incorrectly as potential threats.[7] As a safeguard against such inappropriate profiling, the US has enacted a law that requires each agency that is engaged in data mining to submit an annual report to Congress on all such activities.[8]

3. Conflict of interest: UID authority's exclusive power to make complaints

Clause 47(1) of the Bill: *Courts cannot take cognizance of any offence punishable under the Act, unless a complaint is made by the UID authority, or a person authorised by it.*

Issue: This provision implies that no complaint will be admitted before a court unless it has been filed by the UID authority. This may present a conflict of interest as under the Bill the UID authority is responsible for the security and confidentiality of identity information and authentication records. There may be situations in which members or employees of the UID authority are responsible for a security breach.

4. Discretionary powers under delegated legislation

Demographic and biometric information collected

Clause 2(k) of the Bill*: Demographic information will include name, date of birth, address and other information that is specified by the UID authority. However, such information cannot include race, religion, caste, tribe, ethnicity, language, records of entitlement, income or medical of the individual.*

Issue: The Bill empowers the UID authority to specify demographic information that may be collected. The only restriction imposed on the authority is that it shall not record information pertaining to race, religion, caste, language, records of entitlements, income or health of the individual. This power will allow the authority to collect additional personal information, without prior approval from Parliament.

It may be noted that the enrolment form currently being used contains fields for capturing information such as the National Population Register (NPR) receipt number, mobile number, bank account number, etc.[9] Though these fields are labelled 'optional', it is unclear why this additional information is being recorded.

Clause 2(g) of the Bill*: Biometric information includes photograph, fingerprints, iris scans and other biological attributes of an individual specified by the UID authority.*

Issue: The Bill specifies biometric information to include photograph, fingerprints, and iris scans. Further it empowers the UID authority to specify other biological information that may be collected. Therefore, the Bill does not prevent the UID authority from requiring the collection of biometric information such as DNA.

Time period for maintaining authentication records

Clauses 32(1) and 54(w) of the Bill: *The Bill provides that the UID authority will maintain details of every request for authentication (i.e. time of request, identity of the entity requesting for authentication, and the response provided). The time period for which this information is stored will be specified by regulation.*

Issue: The Bill does not specify the maximum duration for which authentication records may be stored by the UID authority. Instead it allows the UID authority to specify this through regulations. Authentication records contain information regarding: (i) the time of authentication request, (ii) names of entities that seek to verify an individual's identity, and (iii) response received. This information could provide insights into activities of an Aadhaar holder through their use of Aadhaar. Maintaining authentication records over a long time period may be misused for activities such as profiling an individual's behaviour.

---

1. The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Bill, 2016, http://www.prsindia.org/administrator/uploads/media/AADHAAR/Aadhaar%20Bill,%202016.pdf.

2. Introduction of Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Bill, 2016, Uncorrected Debates Lok Sabha, March 3 2016, 12-1pm.

3. Justice K. Puttaswamy (Retd) and Another vs Union of India and Others, Supreme Court, Writ Petition (Civil) No. 494 of 2012, September 23, 2013, August 11, 2015, October 15, 2015.

4. PUCL vs Union of India, AIR 1997 SC 598, December 18,1996.

5. Paragraph no. 35 of PUCL vs Union of India, AIR 1997 SC 598, December 18,1996.

6. "Data Mining: Federal Efforts Cover a Wide Range of Uses," US General Accounting Office, May 2004.

7. Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, UN Human Rights Council, Dec 28, 2009.

8. The Federal Agency Data Mining Reporting Act of 2007, United States, https://www.law.cornell.edu/uscode/text/42/2000ee-3.

9. Enrolment Form of UID, http://uidai.gov.in/images/uid_download/enrolment_form.pdf, Last visited March 8, 2016.