

# Legislative Brief

## The National Identification Authority of India Bill, 2010

The Bill was introduced in the Rajya Sabha on December 3, 2010 by the Ministry of Planning.

The Bill was referred to the Standing Committee on Finance (Chairperson: Shri Yashwant Sinha) on Dec 12, 2010. It was scheduled to submit its report within three months.

### Related Briefs:

The Protection of Women Against Sexual Harassment at Work Place Bill, 2010  
May 20, 2011

The Direct Taxes Code Bill, 2010  
April 21, 2011

**Rohit Kumar**  
rohit@prsindia.org

**Kaushiki Sanyal**  
kaushiki@prsindia.org

June 2, 2011

### Highlights of the Bill

- ◆ The Bill seeks to establish the National Identification Authority of India (NIAI) to issue unique identification numbers (called 'Aadhaar') to residents of India.
- ◆ Every person residing in India is entitled to obtain an Aadhaar number after furnishing relevant demographic and biometric information. No information related to race, religion, caste, language, income or health shall be collected.
- ◆ The information collected shall be stored in the Central Identities Data Repository. This shall be used to provide authentication services.
- ◆ Sharing of data is prohibited except by the consent of the resident; by a court order; or for national security, if directed by an authorised official of the rank of Joint Secretary or above.
- ◆ The Bill also establishes an Identity Review Committee which shall monitor the usage patterns of Aadhaar numbers.

### Key Issues and Analysis

- ◆ The Bill does not make it mandatory for an individual to enroll with the NIAI. However, it does not prevent any service provider from prescribing Aadhaar as a mandatory requirement for availing services.
- ◆ The information collected by NIAI may be shared with agencies engaged in delivery of public benefits and services with prior written consent of the Aadhaar holder. The safeguards provided for preventing misuse of this information may be inadequate.
- ◆ The Bill requires the NIAI to disclose identity information in the interest of national security, if so directed by an authorised officer. The safeguards for protection of privacy differ from the Supreme Court guidelines on telephone tapping.
- ◆ The Bill states that no court shall take cognizance of any offence, except on a complaint made by the NIAI. This could result in a conflict of interest situation if the offence is committed by a member of the NIAI.
- ◆ Details of demographic and biometric information to be recorded have been left to regulations. This empowers the NIAI to collect additional information without prior approval from Parliament.

---

## PART A: HIGHLIGHTS OF THE BILL

### Context

---

At present, the central and the state governments in India issue different identity documents for specific purposes. These documents may be issued to individuals (passport, Election Card, PAN Card, driving license), or to households (ration card, Rashtriya Swasthya Bima Yojana card).<sup>1</sup>

In April 2000, a Group of Ministers was set up to review the national security system and to consider the recommendations of the Kargil Review Committee. The report on “Reforming the National Security System”, submitted in 2001, recommended that a multi-purpose National Identity Card (MNIC) should be issued, starting from the border districts.<sup>2</sup> The purpose was to prepare a National Register of Indian Citizens.<sup>3</sup> In 2003, the Citizenship Act, 1955 was amended to allow the central government to compulsorily register every citizen and issue them with identity cards.<sup>4</sup> In March 2006, another project called the “Unique ID for the Below Poverty Line families” was approved by the Department of Information Technology. It was decided to merge the two schemes for which an Empowered Group of Ministers (chaired by Shri Pranab Mukherjee) was set up in December 2006.<sup>5</sup>

In November 2008, the EGoM approved certain decisions: (i) initially the Unique Identification Authority of India (UIDAI) would be notified as an executive authority (statutory authority to be constituted later); (ii) an initial database would be created from electoral rolls; (iii) UIDAI would take its own decision on how to build the database; and (iv) it would be anchored in the Planning Commission for five years.<sup>6</sup> The UIDAI was notified by the Planning Commission on January 28, 2009 and Shri Nandan Nilekani was appointed as the Chairman.

The Bill seeks to establish the National Identification Authority (earlier UIDAI) as a statutory authority and to specify its functions. It also entitles every resident of India to obtain a unique identification number.

### Key Features

---

- The National Identification Authority of India (NIAI) will issue unique identification numbers (called ‘Aadhaar’ numbers) to residents of India and any other category of people that may be specified. The NIAI shall have a chairperson and two part-time members.

### Aadhaar Numbers

- Every resident of India (regardless of citizenship) shall be entitled to obtain an Aadhaar number after furnishing demographic and biometric information. Demographic information shall include items such as name, age, gender and address. Biometric information shall include some biological attributes of the individual. Collection of information pertaining to race, religion, caste, language, income or health is specifically prohibited.
- The Aadhaar number shall be issued after the information provided by the person is verified. It shall serve as proof of identity, subject to authentication. However, it should not be construed as proof of citizenship or domicile. The Aadhaar number holder may be required to update his biometric and demographic information.
- The Aadhaar number shall be a random number and shall not bear any information of the individual. An Aadhaar number issued to an individual shall not be re-assigned to any other person.

### Process of Issuing and Authenticating Aadhaar Numbers

- There are three main steps in the process. First, information for each person shall be collected and verified after which an Aadhaar number shall be allotted. Second, the collected information shall be stored in a database called the Central Identities Data Repository. Finally, this repository shall be used to provide authentication services.
- The NIAI shall appoint registrars and enrolling agencies to collect demographic and biometric information for the purpose of issuing Aadhaar numbers. Special measures shall be taken to issue Aadhaar numbers to certain groups such as women, children, migrant workers and others without a permanent address.
- Service providers (such as banks, fair price shops etc.) may ask a customer to provide his Aadhaar number and biometrics as proof of identity. The service provider shall submit this information to NIAI through an electronic channel for online authentication. The NIAI, after verifying the correctness of the information provided, shall respond to the query with a positive or negative response but shall not divulge any demographic or biometric information.
- The NIAI shall establish a grievance redressal mechanism to redress grievances of residents, registrars, enrolling agencies and service providers.

### Disclosure of information

- The NIAI shall be responsible for the security and confidentiality of information. It is required to take measures to protect information against loss or unauthorised access.
- The NIAI or any agency which maintains the Central Identities Data Repository is forbidden from revealing any information stored in the repository.
- There are four exceptions to this rule. First, an Aadhaar number holder may request the NIAI to provide access to his own identity information. He may also ask for information on authentication requests of his Aadhaar number. Second, the NIAI may share information of Aadhaar number holders, based on their written consent, with agencies engaged in delivery of public benefits and services. Third, the NIAI may reveal information in response to a court order. Finally, information may be revealed in the interest of national security, if directed by an authorised official of the rank of Joint Secretary or above in the central government.

### Identity Review Committee

- The central government may constitute an Identity Review Committee to analyse the extent and pattern of usage of Aadhaar numbers across the country. The Committee shall prepare a report annually and submit its recommendations to the central government. The report shall be laid before Parliament.
- The Committee shall consist of a Chairperson and two members who shall be appointed on the advice of the Prime Minister, a Union Cabinet Minister and the Leader of Opposition in the Lok Sabha.

### Offences and Penalties

- The Bill lists several offences such as unauthorised collection of information, impersonation, manipulation of biometric information, and unauthorised access or damage to the Data Repository. Penalties vary from three years imprisonment and a fine of Rs 10,000 (for impersonation) to a fine of Rs 1 crore (for unauthorised access to the Data Repository). Penalties have also been prescribed for offences committed outside India.
- The Bill states that no court shall take cognizance of any offence except on a complaint made by the NIAI.

## PART B: KEY ISSUES AND ANALYSIS

The Bill aims to issue unique identification numbers to residents of India and to provide for a reliable method of identifying individuals. The UIDAI Strategy Overview<sup>7</sup> states that identification will facilitate access to benefits and services, especially for vulnerable groups such as homeless persons, migrant labour etc. Issuance of biometric based identities is expected to reduce problems of identity frauds and ghost beneficiaries.

However, any database that stores personal information carries the risk of its misuse by various agencies (both public and private), which may affect an individual's privacy. The UK National Identity Card scheme was scrapped in 2011. Some of the main reasons cited for scrapping the scheme were the cost of implementing the scheme and the infringement of civil liberties.<sup>8</sup> The Real ID Act passed by the US in 2005 has also been opposed by many states on grounds of privacy and threat to data security.<sup>9</sup>

We discuss below the safeguards that are built into this Bill to protect Aadhaar holders against invasion of their privacy.

### Enrolment – Voluntary or Mandatory

Clause 3(1)

The Bill does not make it mandatory for an individual to obtain an Aadhaar number. However, it does not prevent any service provider from prescribing Aadhaar as a mandatory requirement for availing services. This differs from the US where government agencies cannot deny benefits to individuals who do not possess or refuse to disclose their Social Security Number, unless specifically required by law.<sup>10</sup>

However, it must be noted that the success of Aadhaar in weeding out 'ghost' beneficiaries (in programmes such as the public distribution system) depends on mandatory enrollment. If enrollment is not mandatory, both authentication systems (identity card based and Aadhaar based) must coexist. In such a scenario, 'ghost' beneficiaries and people with multiple cards will choose to opt out of the Aadhaar system.

## **Safeguards for maintaining confidentiality and privacy of information**

Information collected may be misused if safeguards to maintain privacy are inadequate. Though the Supreme Court has included privacy as part of the Right to Life,<sup>11</sup> India does not have a specific law governing issues related to privacy. The government has formed a committee to draft a suitable law.<sup>12</sup>

We examine whether the Bill has sufficient safeguards if information is (a) shared with agencies engaged in delivery of public benefits and services; (b) disclosed to intelligence or law enforcement agencies; and (c) used to identify behaviour patterns through data mining.

### **Sharing information with agencies engaged in delivery of public benefits and services**

Clause 23(1)(k) The Bill allows NIAI to share the information of an Aadhaar number holder, based on his written consent, with agencies engaged in the delivery of public benefits and public services. However, it does not specify whether consent should be taken only once or at each instance a person avails of a new service. A one-time consent may be prone to misuse and this may affect an individual's privacy.

### **Disclosure of information to intelligence or law enforcement agencies**

Clause 33(b) The Bill requires the NIAI to disclose information (including identity information of individuals) in the interest of national security. This will be on the direction of an authorised officer of the rank of Joint Secretary or above in the central government.

In 1996, the Supreme Court held that the state may tap telephones "only at the occurrence of any public emergency or in the interest of public safety" if (a) it is authorised by the Home Secretary of the central or state government; and (b) 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.<sup>13</sup>

The safeguards for protection of privacy in this Bill differ from those set out for phone tapping. 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. Third, there is no limit for the time period for which the authentication data may be collected. Fourth, there is no mechanism for review.

### **Potential to profile individuals**

The Bill does not specifically prohibit intelligence agencies from using the UID as a link (key) while running computer programmes across various datasets (such as telephone records, air travel records etc.) in order to recognise patterns of behaviour. Such techniques for pattern recognition can be used for various purposes such as detecting potential illegal activities.<sup>14</sup> However, these can also lead to harassment of innocent individuals who get identified incorrectly as potential threats.<sup>15</sup> As a safeguard against misuse, the US had introduced (but not passed) a legislation that required each agency that was engaged in data mining to submit an annual report to Congress on all such activities.<sup>16</sup>

### **Compensation for loss or unauthorised disclosure of information**

Clauses 30, 37, 38, 39, 40 The Bill requires all persons with access to Aadhaar related information to keep it secure and confidential. It prescribes penalties for unauthorised access or intentional disclosure of information. However, it does not penalise any negligence that leads to loss of information. Also, it does not have a specific provision to compensate an individual in case his personal information is misused. This differs from the Information Technology Act, 2000, which states that a company handling 'sensitive personal data' is liable to pay compensation upto Rs 5 crore if it is 'negligent in implementing and maintaining reasonable security practices and procedures' with respect to such data.

## **Conflict of interest**

Clause 46(1) The Bill states that no court shall take cognizance of any offence punishable under the Act, except on a complaint made by the NIAI. Such a provision is usually included to ensure that the regulatory body vets all complaints before a criminal charge is filed.

However, unlike regulators such as the Securities and Exchange Board of India or the Reserve Bank of India, the NIAI also has a role in implementation and its members and employees have duties related to data security. This could result in a conflict of interest situation if the offence is committed by an employee of the NIAI.

## Discretionary powers under delegated legislation

### Regulation of demographic and biometric information to be recorded

Clause 2(e), (h) **Demographic information:** The Bill empowers the NIAI to specify demographic information that may be recorded. The only restriction imposed on NIAI is that it shall not record information pertaining to race, religion, caste, language, income or health of the individual. Keeping this definition in the Regulations provides the NIAI with the power 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.<sup>17</sup> Though these fields are labelled ‘optional’, it is unclear why this additional information is being recorded.

**Biometric information:** The definition of biometric information will be specified in the Regulations. Currently, the UIDAI is capturing 10 fingerprints, iris scan and photograph as biometric information of each resident.<sup>18</sup> However, the Bill does not prevent it from collecting other biometric information such as DNA.

### Storage of authentication information

Clause 32(1) The NIAI is required to maintain details of every request for authentication and the response provided. The Bill does not specify the maximum duration for which authentication data may be stored by the NIAI. This has been left to Regulations. Authentication data provides insights into usage patterns of an Aadhaar number holder. Data that has been recorded over a long duration of time may be misused for activities such as profiling an individual’s behaviour.

### Different dates for notification of different clauses

Clause 1(3) Some clauses of the Bill provide the NIAI with the power to collect and maintain data. Some other clauses provide safeguards against misuse. The Bill contains a blanket provision that allows the central government to notify different clauses on different dates. There is no requirement that the safeguard clauses should come into force by the time the provisions enabling collection of data are notified.

### Notes

1. Report of the Committee on Financial Sector Reforms, Planning Commission, Govt of India, 2009
2. “Group of Ministers’ Report on Reforming the National Security System,” Press Information Bureau, May 23, 2001
3. “Parliamentary Consultative Committee of MHA discusses Multi-purpose National Identity Card Project,” Press Information Bureau, Aug 21, 2003
4. Section 12 of The Citizenship (Amendment) Act, 2003
5. Unique Identification Authority of India, Planning Commission, Govt of India (see <http://uidai.gov.in>)
6. “Government approves issue of unique identity (UID) number to all residents,” PIB, Nov, 10, 2008
7. “UIDAI Strategy Overview”, UIDAI, Planning Commission, Govt of India, April 2010
8. Identity Documents Act, 2010 cancelled the ID card; “Identity cards scheme will be axed ‘within 100 days,’ BBC News, May 27, 2010; House of Commons debate on Identity Documents Bill on 9<sup>th</sup> July, 2010 (see <http://www.publications.parliament.uk/pa/cm201011/cmhansrd/cm100609/debtext/100609-0006.htm>).
9. Real ID Act, 2005 (see <http://thomas.loc.gov/cgi-bin/bdquery/z?d109:H.R.418:>).
10. Section 7 of the Privacy Act, 1974 (see <http://www.justice.gov/opcl/1974ssnu.htm>).
11. See, for example, *Kharak Singh vs State of UP*, 1 SCR 332 (1964) and *R. Rajagopal v. State of T.N* (1994) 6 SCC 632.
12. “Approach Paper for a Legislation on Privacy,” Oct 18, 2010, Ministry of Personnel, Public Grievances and Pensions, Govt of India.
13. Writ Petition (C) No. 256 of 1991, *People’s Union of Civil Liberties (PUCL) Vs. Union of India (UOI)*
14. “Data Mining: Federal Efforts Cover a Wide Range of Uses,” US General Accounting Office, May 2004.
15. 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.
16. US Federal Agency Data Mining Reporting Act of 2007 (Introduced on Jan 10, 2007) (see <http://thomas.loc.gov/cgi-bin/bdquery/z?d110:SN00236:@@L&summ2=m&>).
17. Enrolment Form of UID (see <http://uidai.gov.in/images/FrontPageUpdates/ROB/D9%20Enrolment%20Form.JPG>).
18. Biometrics Design Standards for UID Applications, UIDAI Committee on Biometrics, December 2009.

## Appendix 1: Possible Applications of UID

We list below some possible applications of the Aadhaar number in facilitating access to benefits and services.

**Table 1: Potential benefits of UID**

Application	Potential Benefits	Remarks
<b>Proof of Identity</b>	The Aadhaar number would provide proof of identity to every resident including migrants, homeless people, etc. The number is unique to each individual and a person's biometric information is linked to it. This could facilitate access to various services, which need identity proof.	Presently, various identity cards such as PAN card, voter's identity card, ration card etc are accepted as proof of identity. About 82% of the adult population have the election card, 74% of the population have ration cards and 38% of the population have Rashtriya Swasthya Bima Yojana card.
<b>Public Distribution System</b>	The Aadhaar number can eliminate duplicate cards and cards for non-existent persons (estimated to be about 17% of all cards). It could also reduce diversion at Fair Price Shops by ensuring that goods are distributed to the beneficiaries only after their biometrics are verified.	UID cannot address errors in targeting of Below Poverty Line (BPL) families. Some estimates suggest that about 61% of the eligible population is excluded from the BPL lists while 25% of the non-poor household are included in the BPL list.
<b>Financial Inclusion</b>	RBI has declared Aadhaar to be sufficient proof of identity to open a bank account. It could also facilitate authentication with Business Correspondents in remote areas.	Currently, 41% of the adult population do not have bank accounts.
<b>National Rural Employment Guarantee Act, 2005</b>	It would be possible to identify duplicate and fake beneficiaries of NREGA.	UID cannot address other problems of NREGA such as incorrect measurement of work, payment delays etc.

Sources: "Envisioning a role for Aadhaar in the Public Distribution System," Working Paper, UIDAI, 2010; Performance Evaluation of Targeted Public Distribution System, Planning Commission, March 2005; "Management of Food Grains," 73<sup>rd</sup> Report of the Public Accounts Committee, 2007-08, "Report of the Expert Group to Advise the Ministry of Rural Development on the Methodology for Conducting the Below Poverty Line Census for the 11<sup>th</sup> Five Year Plan," Chairperson: Shri N.C. Saxena, August 2009; Discussion Paper on Aadhaar based Financial Inclusion, Report of the Working Group to Review the Business Correspondent Model, RBI, August 2009, Know Your Customer Guidelines, RBI, 2004; UID and NREGA, Working Paper; Lok Sabha Unstarred Question No. 2357, Dec 3, 2009; Lok Sabha Unstarred Question no. 4135 Answered on Dec 15, 2009; Public Distribution System and Other Sources of Household Consumption, 2004-05, NSSO Report (see [http://mospi.nic.in/press\\_note\\_510-Final.htm](http://mospi.nic.in/press_note_510-Final.htm)), Lok Sabha Unstarred Question no. 2838 Answered on March 14, 2011.

**DISCLAIMER:** This document is being furnished to you for your information. You may choose to reproduce or redistribute this report for non-commercial purposes in part or in full to any other person with due acknowledgement of PRS Legislative Research ("PRS"). The opinions expressed herein are entirely those of the author(s). PRS makes every effort to use reliable and comprehensive information, but PRS does not represent that the contents of the report are accurate or complete. PRS is an independent, not-for-profit group. This document has been prepared without regard to the objectives or opinions of those who may receive it.