Law & Policy BRIEF

O.P. Jindal Global University
A Private University Promoting Public Service

THE UNIQUE IDENTIFICATION PROJECT AND THE NATIONAL IDENTIFICATION AUTHORITY OF INDIA BILL, 2010

Vol. I | Issue 4 | April 2015

Criticisms and support for the Unique Identification (UID) project have largely hinged on its impact on welfare schemes, privacy of individuals, nature of governance, overall security and confidentiality of information and potential unauthorized access to data, among others. Given that the huge costs of the UID Project would have necessitated serious consultation with the public and adequate cost benefit analysis, the absence of both have generated much controversy. This issue of the Law & Policy Brief scrutinizes the larger project of providing Unique Identification numbers and the National Identification Authority of India Bill, 2010, that seeks to retrospectively validate the project.

The Unique Identification Authority of India (UIDAI) was formed under the Planning Commission by an executive order issued in January 2009, with the goal of issuing Unique Identification numbers to every resident of India. This number was to be linked to the resident's demographic and biometric information in order to provide not only identification but also to effectively deliver welfare services and allow the Government to monitor various programs and schemes. The Government in 2010 proposed to make the said Authority a statutory authority and tabled the National Identification Authority of India Bill, 2010 (hereinafter, the Bill). The Bill has been pending in the Rajya Sabha since 2010.

In an ongoing case before the Supreme Court of India [*Unique Identification Authority of India v Central Bureau of Investigation,* Appeal (Crl.) No. 2524/2014], the constitutional validity of the UIDAI has been challenged. The primary questions before the Court hinge on the appropriateness of the project collecting and storing biometric and other information in the face of limited government envisaged by the Constitution. The final hearings in this case are posted for second week of July, 2015, which makes scrutinizing the project and the Bill, a timely endeavor.

Bill Summary

The 2010 Bill creates the National Identification Authority of India (NIAI) with the objective of issuing unique identification numbers (called 'Aadhaar') to residents of India and to "certain other classes of individuals" upon providing his demographic and biometric information. The Bill does not define "certain other persons" but stipulates that the Central Government may from time to time notify such other category of individuals who may receive the Aadhaar number. The Bill provides that information so collected shall be stored in the Central Identities Data Repository (CIDR) and shall be used to provide authentication services.

The Bill contains important definitions of terms used in the first part; the properties and authentication purpose of Aadhaar numbers to certain categories of people (elderly, disabled, migrant workers, unorganized workers etc.) in the second part; establishment of the National Identity Authority of India and the powers and functions of its members, officers and Chairman in the third part; finances, annual audits of the UIDAI in the fourth part; the Bill establishes an Identity Review Committee to monitor the usage patterns of Aadhaar numbers in the fifth part;

Law and Policy Research Group, *at the Jindal Global Law School, brings the tools of legal analysis and policy analysis in conversation with each other. Its* ***Law & Policy Brief*** *presents inter-disciplinary analyses of Bills pending before the Parliament, recent court judgments, amendments to existing laws, recently enacted laws, and other topical legal issues that have important policy implications.*

Editors
Dr. Ashish Bharadwaj
Saptarshi Mandal
jgls-lpb@jgu.edu.in
www.jgu.edu.in
www.jgls.edu.in

protection of information held with the Central Identities Data Repository in the sixth part; offences, corresponding penalties for impersonation, unauthorized disclosure or access to such information are listed in the seventh part; and finally, certain miscellaneous provisions are laid down, including delegating role of the Authority, power of the central government to make new rules etc., in the eighth part.

Key Features of the Bill

Aadhaar and Process of Issuing and Authenticating Aadhaar Numbers

Aadhaar number is not connected to citizenship and therefore every resident of India is entitled to it, conditional upon furnishing of demographic and biometric information. "Demographic information" includes information relating to the name, age, gender and address and such other information as may be specified in the regulations for the purpose of issuing an Aadhaar number, but does not include information related to race, religion, caste, language, income or health. This is potentially a self-defeating provision because although the Bill forbids collection of such information related to religion, health or income, various other information and documentary proof that are collected by it adequately bear out these factors.

The process of issuing and authentication of Aadhaar numbers is fourfold. The first step is *collection* of information. The Bill provides for enrolling agencies to collect information. Section 2(o) defines the role of the Registrar as the authority permitted to enroll individuals under the program. The second step is *verification*. Section 3(2) provides that verification will follow the receipt of the information, but the term is not explained in the Bill. There is an implication that the Aadhaar numbers and information collected will be submitted or *enrolled* to the CIDR for verification which essentially appears to be referring to the process of authentication. The *authentication* will happen by a simple check for compliance with the date available with the CIDR.

The NIAI, as per the framework of the Bill shall also take special measures to issue Aadhaar numbers to certain groups such as women, children, migrant workers and others who may not have permanent address.

Disclosure of Information

Security and confidentiality of information has been made the sole responsibility of the NIAI. Any authority including the NIAI which maintains the CIDR is forbidden from revealing any information. However, the Bill stipulates that sharing of data is prohibited except by the consent of the resident, by a court order, or for national security when it shall be directed by an authorized official of the rank of Joint Secretary or above. It must be stressed that 'national security' has not been defined anywhere in the Bill and its interpretation is left to the discretion of the authorized officials. A powerful framework to collect and *disclose* information must be doubly careful to avoid a potential abuse of a clause which purportedly has an indeterminate and indefinite meaning. National security must therefore be properly and narrowly defined.

The Scheme of UID, 'Voluntary Information' and Privacy

The UIDAI Strategy Overview – a document prepared by the Planning Commission – states loftily that identification will facilitate access to benefits and services, especially for vulnerable groups such as homeless persons and migrant labourers. However, the project has come in the face of criticisms owing to several factors, most notably privacy considerations in the absence of data protection laws in India and financial considerations (absence of any feasibility study, cost-benefit analysis etc.).

Legal scholar Usha Ramanathan has posed some troubling questions about the UID project. For instance, what constitutes identity in the scheme of UID and how will it be established? Is the project about identity or identification? The Strategy Overview document emphasizes that the project is about identity, stressing that the UID will be a single-step identity verification document. However, the approach of the UIDAI apparatus in collecting, containing and using information makes it abundantly clear that the project is more about identification and less about identity. Identification, in the classic Benthamian sense is a transaction between two parties, in this case, the resident and the State. Proving who one is, is an active process of identification and not a subjective condition of identity as the UID purports to be. Assuming that the objective of the project is to *provide* 'identity', one is left to wonder, how different is UID from PAN Card, Driving Licence, Voter Id, Ration Card and Passport, all of which are equally valid and acceptable forms of establishing one's identity. Since the very objective of the project remains unconvincing, more questions surface: Is UID about transparency or control and tracking? Is it about information or data? Is UID voluntary or mandatory? Is UID part of a surveillance apparatus or is it only to deliver entitlements? Is biometrics unimpeachable or is this an experiment? In order to engage with these questions more meaningfully, we must scrutinize the Bill closely.

The Standing Committee on Finance submitted its 42nd Report on the NIAI Bill on December 13, 2011 and echoed some of these concerns that emerged from civil society groups and recommended that the government reconsider the UID program and introduce a new Bill. The Committee had several reservations about the bill, most notably that the passage of a national data protection law was a pre-requisite for any initiative dealing with large scale collection of information from individuals and linkages across databases. The Committee also disapproved that no comprehensive feasibility study for financial implications and identity theft were undertaken.

At the heart of the UID project is the notion that technology will 'fix' everything. The tone of the strongest advocates of the project seems to suggest that UID will give an identity to a hitherto identity-less mass of people—a single step towards the right direction as far as availing services and entitlements which the state provides for the poor. In the popular imagination, the project is a pro-poor one. Reimagining

India's social and political problems as technical (or perhaps technological) ones, the project seeks to offer technical fixes. It is imagined that the KYC (Know Your Customer) facility will help those with multiple documents, by not having to identify themselves over and over again. If they have multiple identity documents, the enrolling agency will 'de-duplicate' them through the use of biometrics (fingerprints and iris metrics). With the question on the need of adding another form of identity i.e. Aadhaar number, without adequately studying the possibility of using the existing forms of identity like passport, voter ID, driving license etc. has been identified as a potential waste of resources. In the submission by the Planning Commission before the Standing Committee, it was stated by the government that the "reason for starting the project is not for overriding existing IDs. All the above documents are relevant to a domain and for a service. Aadhaar number is to be used as a general proof of identity and proof of address." However, continuance of various existing forms of identity and the requirement of furnishing 'other documents' for proof of address, even after the issue of Aadhaar number would render the claim of the government that Aadhaar number is to be used as a general proof of identity and address completely meaningless.

Another controversial aspect of the project has been the 'voluntary' as opposed to the (implied) mandatory nature of enrolment. While the project document does not make it mandatory for an individual to obtain an Aadhaar number, neither does it prohibit any other agency from demanding that a person must have an Aadhaar number to receive a service. For a project with an ambition of achieving universal enrolment, it is likely that agencies may demand enrolment as a prerequisite. Experience from the ground in several states go on to prove this point

Service by State/Department

Delhi/Revenue Department: Vide Notification dated 20th December 2012, made the Aadhaar number mandatory for a range of services, including Scheduled Caste/Scheduled Tribe and Other Backward Classes certificates, income and domicile certificates and birth certificates and for the registration of marriages, various documents and deeds at the sub-registrars' offices.

Jharkhand/UIDAI: Vide Notification dated 25th January, the UIDAI nodal officer in Jharkhand's Khunti district, following a meeting with the BDO, issued a notification asking officials at the panchayat level to achieve 100 per cent seeding of the UID in the NREGS management information system. The notification stated that the salaries of panchayat officials would be withheld if they failed to achieve the target.

Delhi/Department of Food and Supplies: In the Department's guidelines for identifying families eligible for rations, top priority is given to Aadhaar numbers, which must be on the ration card of each family member. The Guidelines reiterates the still operational December 2012 order which states that Aadhaar would be used to deliver all services within its jurisdiction. The guidelines state "Non submission of copy of Aadhaar..may lead to removal of the family from the list."

Maharashtra: Aadhaar compulsory for registration of Marriages

The linking of Aadhaar to social schemes has ironically created more barriers for the marginalized who are in dire need of access to limited benefits provided by the State. This markedly differs from the United States, where no government agency can deny benefit to an individual who does not possess or refuse to disclose their Social Security Number unless there is an express requirement under law to do so. In September 2013, the Supreme Court passed an interim order in a case challenging the constitutional validity of the UIDAI, directing that the Aadhaar card cannot be a prerequisite for public services. As late as 16th March 2015, the Supreme Court has ordered that the Centre and States "adhere" to its earlier order that no person shall be denied any benefit or "suffer" for not having Aadhaar card issued by the UIDAI.

Privacy Protection and UID

India does not currently have a data protection law. The right to privacy does not find explicit mention in the Constitution. However, the Supreme Court has derived the right to privacy from the rights available under Articles 19(1)(a) and Article 21 of the Constitution. In *People's Union of Civil Liberties v the Union of India* [(2003) 4 SCC 399], where the right of government authorities to intercept messages transmitted or received by any telegraph, in the interest of national security and sovereignty, was challenged, the Supreme Court elaborated that tapping a person's telephone line violated his right to privacy, unless it was required in the gravest of grave circumstances. Although the Court upheld the restrictions on the fundamental freedom, it insisted that the government must use restraint while exercising these powers. The right to privacy has evolved over the years and the right is no longer limited to certain protected spaces, such as the home. The spatial understanding of privacy has been watered down, especially with a wide meaning of privacy adopted by the court in *Selvi v State of Karnataka* [(2010) 7 SCC 263], where the Court stressed that privacy extended to 'personal knowledge of fact'. In *R. Rajagopal v State of Tamil Nadu* [AIR 1995 SC 264] again, the Supreme Court held that the right to privacy was a fundamental right, enforceable against private persons as well.

Apart from the derivative constitutional protection referred to above, the only legal instrument to protect privacy, is the Information Technology Act, 2000 (the IT Act). Recent

amendments to the IT Act with Section 43-A and 72-A are the operative provisions for data protection. Section 43-A prescribes compensation in the event a body that possesses sensitive personal data or information in a computer resource is negligent in implementing and maintaining reasonable security practices and procedures causing wrongful loss or wrongful gain to any person. However, this provision is woefully inadequate since it makes no mention of non-digital data.

The NIAI Bill nowhere lays down that the information to be provided to UIDAI is of voluntary nature. However, subsequent clarifications in official responsespoint out that the nature of information furnished to the agency is 'voluntary'. The extent of this 'voluntariness' must be interrogated. This voluntariness extends to the disclosure of information to the enrolling agencies. Given that it is unclear how this information will be utilized and who will access it, the very nature of voluntary information becomes subject to scrutiny. 'Information privacy' is protected by comprehensive data protection laws in the UK (Data Protection Act, 1998) and multiple privacy laws like the Privacy Act, 1974 and the Computer Matching and Privacy Act, 1988 in the USA. In the absence of a clear legislative and juridical understanding of information privacy which extends to knowing how the data is being utilized and safeguarded and who is safeguarding it and not merely to knowing that data is being submitted to the agency as imagined by UIDAI, the project needs to be more effectively safeguarded. It must also be reiterated that in the UK, in spite of having strong data protection laws, the government abandoned a similar ID Project. In 2010, UK repealed the National Identity Cards Act, 2006, citing a range of reasons including high cost, unsafe, untested and unreliable technology and the changing relationship between the state and the citizen etc.

Information about individuals that are provided to governmental agencies, banks, companies are held in discrete towers (silos) which hold specific information for specific purposes. Single institution or agency must have as little as possible correlated data. When it is necessary to access this personal information, it is imperative that this data be vested in different databases under the rigorous control of different institutions. Usha Ramanathan and many other legal academics argue that UIDAI will link these silos together by a process of 'convergence'. Convergence of data is potentially problematic as a tool to be put to intrusive purposes. Additionally the Bill in its current state does not lay down a 'reasonable cause or requirement' clause that should be present to access any information in the centralized database. It is an additional security that any centralized database must have.

According to the National Research Council in the US, the current state of biometrics is “inherently fallible”. The Council stated in a report that while the technology may work in small scale, it is prone to falter when used over a wide scale. The report noted that in the current state of biometrics, the results are probabilistic and technology assumed that the parameters are static, which they are not. The UIDAI Biometrics Committee had cautioned that fingerprint quality, the most important factor for determining accuracy has not been studied in the Indian context in great detail. Manual labour causes calloused hands and poor fingerprint quality and debunks that biometrics can be infallible.

Conclusion

The Standing Committee has articulated some of the major lacunae in the Bill. The Committee has rightly noted that the collection of biometric information and its linkage with personal information of individuals without a parallel amendment to the Citizenship Act, 1955 as well as the Citizenship (Registration of Citizens and Issue of National Identity Cards) Rules, 2003 may be well beyond the scope of subordinate legislation and needs to be examined in detail by the Parliament. Moreover, in the absence of sufficient safeguards relating to maintaining confidentiality and privacy of information, it is recommended that storing and sharing of sensitive information in centralized agencies must be discontinued to prevent an Orwellian state.

It is strongly recommended that the Bill be amended to include an 'opt-out' option to give strength to the voluntariness of enrollment. Additionally there should be more clarity in the information that is furnished to the agency. A one-time consent may be prone to misuse and affect the individual's privacy. It is recommended that the individual should be asked to give consent at each stage of the receiving a service. In the current form, the Bill allows NIAI to share information of an Aadhaar number holder, based on his/her written consent, with agencies engaged in the delivery of public benefits and services. Given that many states and agencies are making Aadhaar compulsory for availing benefit of social services, it is strongly recommended that a clause be inserted in the Bill to expressly prohibit any service provider from prescribing Aadhaar as a mandatory requirement for availing the said services. ■

About the Authors

Jhuma Sen [LL.M (Berkeley); BA.LL.B (Symbiosis, Pune)] is Assistant Professor and Assistant Director, Centre for Human Rights Studies at the Jindal Global Law School. Prior to joining JGLS, Jhuma practiced as an advocate in the Supreme Court of India and also served as an advisor to several national and international human rights organizations based in New Delhi.