India's national biometric ID scheme

Legal and policy challenges

India is currently implementing the world's largest biometric identification programme: the nationwide Unique Identification Number (UID) system. The project aims to provide biometric IDs to all Indian residents, a total of more than 1.2 billion people. The eventual successes and challenges of the Indian project are likely to have an important influence on the development of national ID programmes in other countries. This policy brief examines legal and policy challenges related to national biometric registration and the forming of a biometric database. What are the challenges and lessons to be drawn from the Indian ID project?

Elida K. U. Jacobsen — *Peace Research Institute Oslo (PRIO)*

Priyanka Vij — *Sciences Po, Paris*

India's Unique ID project

Launched by the Indian government in 2009, the Unique Identification Number (UID) project is currently the largest application of biometric identification technologies in the world. The UID is an ambitious project that seeks to increase efficiency in the delivery of private and public services to the poor and marginalized, while reducing fraud in the welfare system.

One of the main agendas of the Indian scheme is to provide an 'identity' – that is, a unique ID number – to each resident. This number will be the main identifier for each individual, and thus is popularly called an *Aadhaar* – meaning 'foundation' – for a range of private and public services in the country. The unique ID number is expected to be used for banking, cash transfers, school enrolments, and property and marriage registration, as well as in the delivery of public programmes such as the Public Distribution System for subsidized food. At the same time, the UID project is expected to modernize the nature of security governance in the country.[1]

This policy brief asks what are the policy and legal challenges involved in the introduction of national biometric IDs in India, and highlights three main challenges related to the implementation of the UID scheme. First, it looks at the issue of establishing clear jurisdiction: a large-scale project of this type must have clear coordination between the different agencies involved in the implementation. Second, the brief addresses the tension between issues of privacy and data protection and the challenges that arise as a result of the large-scale collection of private data. Lastly, we look into the potential problem of convergence – that is, the possibilities for combining information on individuals – which can lead to profiling and discriminatory treatment of individuals and groups.

Biometric identification

In the last decade, there has been a vast increase in the use of biometric technology. Creating biometric IDs involves using bodily features – such as fingerprints – as the anchor for personal identification. A biometric is a physical or biological feature or attribute that can be measured. The biometric data of a particular kind taken from an individual are
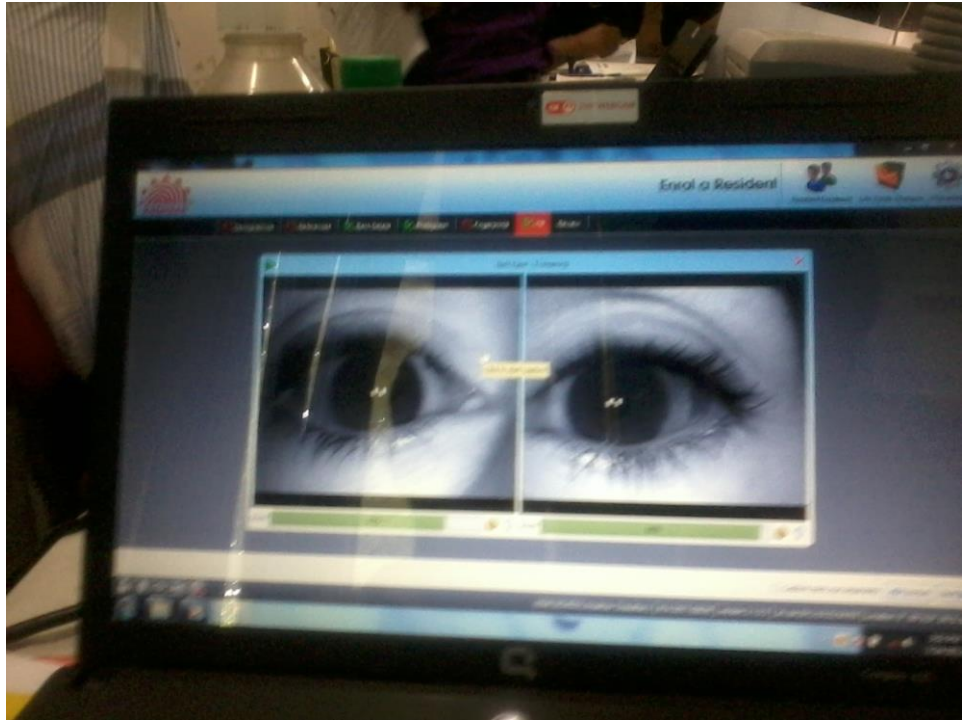
The iris is scanned and the algorithms are recorded into templates by using the unique software called GINGER which has been developed to secure and make UID enrolment tamper proof. Photo: Priyanka Vij

usually transformed via algorithms to produce a so-called template. The identity of an individual can be verified by the reproduction of the template of the biometric initially submitted. The Indian system relies on multimodal biometrics, and collects fingerprints of all ten fingers, iris scans and digitalized profile pictures for all residents.

Because the body becomes the anchor of identification, biometric technologies are seen as improving accuracy and security in schemes where proving one's identity is important. Since 9/11, the USA and the European Union have intensified the role of biometric technology in identity management.[2] The USA implemented its US VISIT programme in 2004, making it mandatory for all foreigners entering U.S. territory to submit their biometrics for scrutiny either when applying for a U.S. visa or at the port of entry. The EU has similarly implemented the European Union Visa Information System, requiring biometrics from all third-country nationals requiring Schengen visas. However, biometric technologies can be used for other purposes than verifying travellers' identities.

While the most frequent area in which these systems have been used in the past decade has been in travel documents, the implementation of biometric identification documents on a national basis is currently gaining salience. Industry analysts expect biometrics to become a major feature in national ID schemes in the coming decade.

The ambition and size of the Indian scheme paves the way for innovative governance mechanisms, and at the same time presents the Indian government and policymakers with a range of challenges as a result of large-scale application of biometrics. The successes and failures of the scheme will undoubtedly have ramifications for similar projects in other countries, both in the South Asia region and beyond.

Legal challenges

The Indian project is being implemented by a central authority, the Unique Identification Authority of India (UIDAI), which is a part of the Indian Planning Commission. At the same time, however, responsibility for the task of identifying citizens belongs to the

At UID enrolment camps, instructions about the procedure for enrolment are provided in the regional languages to facilitate the voluntary enrolment. Photo: Priyanka Vij

mechanisms currently being developed, which allocate responsibility for looking into complaints against staff and officials of the enrolling authorities to the grievance officer appointed by the UIDAI. There is still no independent authority where a grievance against the UIDAI can be filed. As currently proposed by the UIDAI, this system of in-house review of beneficiary grievances contravenes the basic principle of natural justice that no one should be a judge in his or her own case. Issues such as lack of transparency will accordingly need to be addressed.

Surveillance and privacy

Privacy concerns the right to control one's own private sphere. In India, the right to privacy is seen as something sacred, and carefully guarded by the Indian constitution.[4] What is perhaps even more important, however, is the right to control and protect *personal data* – that is, any data that make it possible to identify a natural person, whether directly or indirectly.

In the Indian project, the challenge is to find the correct balance between protection of the right to privacy and the centralized collection of private information and data that can lead to misuse and increased surveillance.

To date, there are no clear restrictions on the use of biometric data collected on citizens in India, or clear guidelines on the kinds of private and public services where such data will be used. There is a possibility that such data could be misused, or used in ways that the enrolled citizen is not currently aware of. The legal frames surrounding the scheme are not adequately addressing the extent to which the information collected under the ambit of the scheme can be used for a variety of surveillance purposes.

Protecting privacy would imply preventing unauthorized access to the personal information on citizens stored in the UIDAI database and other linked servers. In order to uphold the right to privacy of every citizen enrolled in the programme, the UIDAI has developed GINGER – an encryption program that seeks to ensure that information collected during the process of enrolment is preserved and stored safely. Nevertheless, it is admitted that the UID database may be vulnerable to leaks and attacks in the future.[5]

Home Ministry, which is implementing a parallel project of biometric National Population Registration (NPR). During the implementation phase of the UID and the NPR the two agencies have had difficulties collaborating, and the fact that they have been operating under different legal frameworks has led to problems.[3] Questions of unresolved jurisdiction have been further complicated by the fact that the UIDAI was established without first seeking the Indian parliament's approval of the proposed UIDAI Bill (2010).

Another concern relates to the grievance

Data sharing

Convergence is about combining information. The biometric digitalization of individual bodies leads to new ways of identifying people. As the biometric data are abstracted into code, the citizen can be identified in a variety of contexts. Since an individual's UID number will be used in place of actual documentation to prove his or her identity, it is clear that the number will need to be available to numerous agencies. This dependence on one number may prove problematic. The numerous memorandums of understanding signed by the UIDAI with a range of private- and public-sector agencies give rise to concerns about the possible creation of an information-sharing network between various agencies without residents being aware that their private information is being shared in such a way. This linking of the UID number with functionalities of various other agencies may enable the UIDAI to become a kind of profile manager for those interested in creating individual profiles for a given target population.

In the US, the Automated Targeting System by US Homeland Security assigns risk profiles terror scores based on methods of payment, frequent flyer records, meals ordered, etc. Individual travellers can be marked as security risks merely on the basis of travel-related information. Similar surveillance is enabled in India by the provision of Clause 33(b) of the NIAI Bill that requires individuals to disclose identity information in the interest of national security. This clause could be relevant for NATGRID and other upcoming surveillance projects. This may lead to increased profiling of individuals.[6] The current lack of legal tools to prevent and control data mining and profiling in India is also a source of some concern.

Policy recommendations

At this early stage, it is important that legal and policy implications of the UID project be given serious consideration. The following policy recommendations are also applicable to similar national biometric ID programmes in other countries:

● Government authorities should avoid any centralization of biometric data and information on individuals, as this increases the risk of data theft and misuse.

● There is a need for stronger legal safeguards on privacy and data protection in relation to the collection, storage and usage of biometric data from both public and private instances. Personal information should not be compromised during the implementation of the biometric scheme. The legal provisions of the UIDAI bill must be competent to prevent the infringement of the right to privacy and personal dignity enshrined in Article 21 of the Indian constitution.

● The potential for combining data on individuals and making profiles of residents is as yet not accounted for in the legal framework of the proposed bill and complementary documents. The government must provide clearer guidelines regarding the use of information in the data bank.

● The legal framework protecting individuals and groups from discrimination on the basis of the data collected should be strengthened.

● An independent review body should be established to enable a transparent grievance mechanism for the UIDAI.

● The UID scheme is for the moment voluntary. However, since it is linked with the National Population Registration (NPR) and enrolment is increasingly seen as being essential for access to various welfare and development services, having a biometric number is in fact becoming mandatory. The government should assess the social and legal consequences of this shift to heavy reliance on a centralized system, and preferably make sure there are alternatives in place in the event of failure of the system and/or problems of verification.

Notes

[1] Unique Identification Authority of India (2010) *Strategy overview creating a unique identification number for every resident in India*, edited by the Planning Commission of India, 42. New Delhi: Unique Identification Authority of India

[2] Maghiros, I., Punie, Y., Delaitre, S., Lignos, E., Rodríguez, C., Ulbrich, M., Cabrera, M., Clements, B., Beslay, L., & van Bavel, R. (2005) *Biometrics at the Frontiers: Assessing the Impact on Society. Study for the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE)*, IPTS: Sevilla

[3] Lok Sabha, Standing Committee on Finance (2011–12) Lok. *The National Identification Authority of India Bill, 2010*, edited by the Ministry of Planning, 49. New Delhi: Ministry of Planning

[4] *Ram Jethmalani vs Union of India* (2011) Supreme Court of India, All India Reporter

[5] See note 3 above.

[6] Usha Ramanathan (2008) 'Ostensible poverty, beggary and the law', *Economic & Political Weekly*

THE AUTHORS

Elida K. U. Jacobsen is a Researcher at the Peace Research Institute Oslo. Email: elida@prio.no

Priyanka Vij is a master's degree student at the Paris School of International Affairs, Sciences Po, Paris. Email: priyanka.vij@sciences-po.org

THE PROJECT

This policy brief is a product of the 7th Framework Programme project 'Cultures of Governance and Conflict Resolution in Europe and India'. The project analyses the premises and operation of governance initiatives in conflict transformation processes through a combination of fieldwork, qualitative analysis and theory development.