INDICUS FOUNDATION

INDICUS CENTRE FOR FINANCIAL INCLUSION

POLICY BRIEF
MARCH
2016

Aadhaar: Understanding Content, Intent and Portent

Summary

In March 2016, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Bill, 2016 was passed by the Lok Sabha as a money bill. At the same time, the National Identification Authority of India Bill 2010 was withdrawn from the Rajya Sabha, where it was pending approval. The passage of this Bill allows the smooth rollout of the Direct Benefits Transfer programme using JAM (Jan Dhan account number+Aadhaar number+Mobile number) as this piece of legislation focuses on Aadhaar as an efficient enabler for government welfare payments.

Since 2013, there has been an accelerating trend of enrolments and induction of Aadhaar-based authentication for delivering Direct Benefit Transfers (DBT) under an increasing number of schemes. Aadhaar's e-KYC and authentication protocols have proved themselves on the ground, enabling significantly more efficient government transfers for financial inclusion. However, these have happened without due legal and statutory empowerment of the world's largest biometrics database inching close to one billion records. Meanwhile, several opportunities wait on the horizon for using the identity database as the underlying foundation for providing a whole range of services by both public agencies and private actors. With the growing utility of Aadhaar, there have been a number of concerns relating to personal rights, state responsibility and affixed accountabilities of the security of the underlying information, which have remained indeterminate in the absence of due legislation.

With the National Identification Authority of India Bill languishing in Parliament since 2010 and the increasing debate and litigation over the right to privacy, the Supreme Court has intervened from time to time. In a specific order passed in 2015, the Supreme Court had limited the use of Aadhaar to certain specific government programmes, emphasising the need to ensure voluntary usage, while referring the larger debate of constitutional issues of right to privacy to a Constitutional Bench.

The 2016 Aadhaar Bill has established the primary purpose of Aadhaar as an enabler of government transfers and benefits instead of a mandatory identification document. While the current Bill addresses several issues positively, this policy brief highlights areas that merit further thought.

Key asks

- With the passage of the 2016 Aadhaar Bill, the government needs to engage more proactively with the public and highlight the various safeguards built into the design of Aadhaar to: a) allay the general concerns that are partly rooted in insufficient knowledge; and b) demonstrate openness to engage in constructive debate to make the systems more robust and fool proof.
- Given its rather specific purpose as titled, and its introduction as a money bill, it is necessary to have more discussion on the wider use of the Aadhaar database. In particular, whether Aadhaar authentication is a broader 'public good' to be used by public and private actors for instance in the banking space, or is it to remain an exclusive governance-enabler for the state to deliver public services. The use of Aadhaar for payment transfers not covered under the Consolidated Fund of India may require specific (state level) legislation as well.
- As there will understandably be many actors delivering Aadhaar-based services, the debate over issues of security and privacy will only heighten. It is imperative to affix unambiguous responsibilities for the integrity and security of the database and build appropriately strong deterrents and penalties for breach and unauthorised usage. A National Privacy Law can effectively address these issues and the government should accord high priority to such a law in the parliamentary process.

Background

No public utility or service in India has generated so much debate and attracted controversies as the ambitious Aadhaar, India's Unique Identity Number initiative. Since its conceptualization in 2009 under the Unique Identification Authority of India (UIDAI) – under the Planning Commission– the world's largest personal database project has remained mired in controversy and doubts over its intent, content and ultimately, its portent. All this even as Aadhaar's e-KYC and authentication protocols have proved themselves on the ground, enabling significantly more efficient government transfers for financial inclusion. This policy brief seeks to traverse its evolution and take stock of the potential benefits and risks associated with the multiple possibilities of using Aadhaar. The subsequent sections examine Aadhaar on three main fronts – its content, intent and portent.

INDICUS FOUNDATION

INDICUS CENTRE FOR FINANCIAL INCLUSION

Time line

April 2000: Group of Ministers on National Security System recommends a multi-purpose NIC beginning with border areas.

March 2003: Citizenship Act 1955 amended allowing government to compulsorily register every citizen and issue IDs.

March 2006: Project for Unique ID for BPL families launched by Ministry of Information Technology. Empowered Group of Ministers (EGoM) set up for the same merged both projects,

December 2008: EGoM approved an executive body UIDAI (to become statutory later), to create an initial database from electoral rolls

28th January 2009: UIDAI constituted and notified by the Planning Commission as an attached office under the aegis of Planning Commission

2010: National Identification Authority of India Bill introduced

September 2010: First Aadhaar card issued

December 2010: Government of India notification recognises the letter issued by UIDAI containing details of name, address and Aadhaar number, as an officially valid document

September 2011: Aadhaar accepted as valid identity document by Reserve Bank of India

January 2013: Aadhaar seeding notified as precondition for government benefits transfer

September 2013: Reserve Bank of India accepts e-KYC of Aadhaar for opening bank accounts

April 2014: Supreme Court interim order declaring Aadhaar card as non-mandatory for availing government benefits and services

2015: Aadhaar extended to MNREGA, PDS

August 2015: Supreme Court order limiting Aadhaar only to LPG, PDS and Kerosene

September 2015: UIDAI shifted to the administrative control of the Ministry of Communication and Information Technology from NITI Aayog (erstwhile Planning Commission)

October 2015: Supreme Court order expanding Aadhaar use for MNREGA, Pension and PF, PMJDY, while making it purely voluntary for beneficiaries

March 2016: Government withdraws NIAI 2010 Bill from Rajya Sabha and passes The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Bill, 2016 as a money bill.

April 2016: Aadhaar enrolment crosses one billion mark

Content

Shorn of the sensationalism that has haloed the Aadhaar, it would be useful to recap its initial intent: to provide an irrefutable, untamperable identification of an Indian resident. Resident, not citizen. The need for such a tool was perceived despite multiple identity documents in place: ration card, election card, driving license, passport, etc. Aadhaar's principal differentiator is that, unlike all other documents which are based on depositions and other proofs, it is an absolute and primary identifier, using biometrics, which by definition, remains unique to a person and is thus immune to misrepresentation. Thus, the UIDAI aimed at creating a centralized repository containing a resident's basic demographic information – name, address and photograph, which are available in many other documents –and biometric information – the ten fingerprints and two iris scans. Using fool-proof, real-time, machine-based authentication against biometrics stored in the repositor, the Aadhaar can establish whether you are who you claim to be, given the improbability of two persons (even identical twins) having the same biometrics. Accordingly, every Aadhaar entrolled person receives a unique 12-digit number linking to their biometric data in the database.

However, the visible and most-used piece of Aadhaar, the Aadhaar card, contains or offers no more information than other documents: name, address, and photograph, and is used in the same way as other IDs. Thus, the prima facie visual inspection of an Aadhaar card at any public place – airport, government office, hotel, etc. –is susceptible to the same human error as any other ID. The Aadhaar card does come with a 2-D Bar code which when read can display details in the letter, making it one of the checks for a fraudulent printed version of the letter or card. However, at a prima facie level of visual inspection as is common practice, the Aadhaar offers no additional utility to any other identity document. It was under these circumstances that the first signs of public or NGO anxiety emerged over its utility and purpose, considering the Aadhaar card or number was neither mandatory nor projected as a preferred or superseding identity device.

However, as subsequent events have demonstrated, Aadhaar's unique appeal to its proponents lay in its ability not to verify identity per se, but to identify genuine beneficiaries of government transfers. Issuance of biometric based identities is expected to reduce problems of identity frauds and ghost beneficiaries. Thus the intent behind Aadhaar is not so much to enable individuals to produce proof of their identity, but rather to enable the state to furnish proof of delivering its services rightfully.

Intent

The government's intent to use Aadhaar as an electronic identifier tool for delivering public services became clearer in 2013, with the announcement of the Direct Benefits Transfer programme and Aadhaar's central role in the same. Indeed, the thrust for Aadhaar enrolments came largely in the form of public offices and banks doubling up as enrolment camps, besides converting their audiences for enrolment.

Thus, the real evolution in Aadhaar has come to be its recognition as an enabler of financial benefits, a tracer for financial G2P transactions, to ensure error-free credits into the accounts of rightful beneficiaries. This role has become even stronger and the push even accelerated under the present government with the launch of the ambitious PMJDY and later the JAM trinity as the platform to drive financial inclusion, with the 'Your money in your hands' slogan for efficient, leakage free delivery of benefits. In all of this, the technological aspects became central: Aadhaar seeding of beneficiary databases, verification and de duplication of accounts, integration of bank accounts with beneficiary Aadhaar details; and the creation of Aadhaar Payments Bridge.

With the piloting of public services and benefits transfer, confusing signals began emerging in the landscape over the essentiality of Aadhaar to avail of services. Some state actors went overboard making Aadhaar mandatory for school admissions and even for purely private transactions such as transfer of property (e.g. in Maharashtra).

The Supreme Court, while still studying constitutionality of the right to privacy and whether Aadhaar is a violation of such a right, has prima facie allowed the government to continue

Aadhaar enrolments and use the same for identifying beneficiaries for PDS, LPG and MNREGA schemes, but clearly proscribed it as a mandated precondition to receive public services or benefits.

For now, a formidable nationwide architecture has been laid out. By March 2016, over 970 million Aadhaar cards have been issued (75.8% of the population) with the aim of universalization by end 2016. Digital mapping/seeding of beneficiary names with Aadhaar numbers and nominated bank accounts is well under way for over 30 Central DBT schemes. Finally, a bank-led last-mile agent assisted payments network is being set up in rural and remote areas, at the level of sub service areas (village clusters with population of 1500 households). In all of this, the Aadhaar piece is the king pin, the traceable identifier that authenticates every beneficiary and credits benefits or any rightful payments into the nominated Aadhaar-linked bank account.

Thus far, the core rationale for Aadhaar is its being in the class of 'public goods' for the provision of improved public services by the state. The Supreme Court's approval of the government's enrolment and seeding is also in large measure because at one end of these transactions is a state entity.

This intent is unambiguously captured in The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Bill, 2016, which narrows its purpose to the provision of state services funded out of the Consolidated Fund of India. The Bill does not make it mandatory for an individual to obtain an Aadhaar number as a condition to receiving subsidies, benefits and services, and although it seeks to facilitate obtaining one, viable alternative means of identification have been included as well.

Portent

In its new form and as a money bill, The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Bill, 2016 held a much greater chance of being passed in the Parliament, thus paving the way for government to accelerate its DBT programmes for all such expenditures covered under by the Consolidated Fund of India. In doing so, the government has repositioned Aadhaar as a governance tool for delivery of benefits and transfers to rightful beneficiaries through improved targeting and identification.

Salient provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Bill, 2016.

- The Bill seeks to provide for a good governance efficient, transparent and targeted delivery of subsidies, benefits and services (the expenditure of the services shall be incurred from the Consolidated Fund of India) to individuals residing in India, through assigning of unique identity numbers. This is to be done through a Unique Identification Authority of India.
- Every person residing in India shall be entitled to obtain an Aadhaar number by submitting relevant demographic and biometric information by undergoing the process of enrolment. Aadhaar number holders may be required to update the information from time to time to ensure continued accuracy of their information in the Central Identities Data Repository.
- The Central or state government may require an individual to undergo authentication or furnish proof of possession of Aadhaar number as a condition for receipt of a subsidy benefit or service, for which the expenditure is incurred from the CFI. If an Aadhaar number had not been assigned, the individual can apply for enrolment, or alternate and viable means of identification shall be used for delivery of the benefit, subsidy or service.
- The information collected shall be stored in the Central Identities Data Repository and shall be used to provide authentication services. The UIDAI may engage one or more entities to establish and maintain the Central Identities Data Repository and to perform any other functions as specified by regulations.
- The security and confidentiality of identity information and authentication records of individuals are to be ensured by the UIDAI. No core biometric information shall be shared with anyone for any reason, or used for any purpose other than generation of Aadhaar numbers and authentication (except when pursuant to an order of court not inferior to a district judge) However, identity information other than core biometric information may be shared in a manner specified by regulations.
- Unauthorised disclosure or copying or tampering of identity information is punishable with a three-year imprisonment or a fine of ten thousand rupees (one lakh rupees in case of a company).

However, there are grey areas in terms of potential use of the Aadhaar database and its authentication features by actors other than the state. These could be banks pinging to verify e-KYC, payment banks providing cash payment/ acceptance services through retail networks, or other private service providers offering goods/ services of commercial value against mobile payment transfers. Aadhaar authentication is also a highly monetisable commercial service, and has been provided through Aadhaar User Agencies, which are third parties licensed with the UIDAI to interface with the central database.

In the bill, a Requesting Entity has been defined as an agency or person that submits the Aadhaar number and demographic or biometric information, of an individual to the UIDAI for authentication. While the bill's intent is specific to the provision of benefits and transfers, the full potential of Aadhaar can be attained if requesting entities are not restricted to only the central government or state government bodies that seek to provide subsidies, benefits and (public) services but also banks and other commercial financial service providers as well. This will have major implications for the business models of banks and other payment service providers using Aadhar-based transactions and services.

The implications need to be understood and assessed more carefully, for they involve several issues: privacy, data security, accountability and liability of the parties involved, and the government as the

holder of the database. For optimal use of Aadhaar, it is therefore important to delineate the major issues that need to be deliberated, as follows.

Private party access: A fundamental question that has not been clarified in policy circles is whether the Aadhaar database can be a full-scale public good accessible for a broad range of service providers under commercial license terms. There is considerable potential for private parties to build services based on Aadhaar verification services as an underlying layer. here can be a wide diversity of views on this, and indeed the Supreme Court's deliberations would throw more light on these in times to come. However, there also needs to be clear articulation on how Aadhaar's potential as a unique identifier can be expanded, beyond the purposes implied in the bill (transfer and payment of benefits funded out of the Consolidated Fund of India).

Privacy and informed consent: In a basic sense, Aadhaar authentication services concern the status of an actual individual. Key questions in this regard are: Who owns the customer data? What part of the data residing in the central repository can be shared at all with service providers or parties requesting authentication services? To what extent does non-biometric information exchanged constitute sensitive, personal information proprietary to the person? What are the time and limits to the prior consent for use of the identity information? These questions can be comprehensively settled only under a Privacy Law, which does not yet exist in India, although a draft bill has been languishing for over two years. With the rising debate over the use of personal information, it is imperative that a national Privacy Act be in place at the earliest. Meanwhile, until a law comes into force, there should be clear procedural frameworks that safeguard customer data linked to any use of Aadhaar by licensed users and subscribers to the authentication services.

Data protection and security: Another aspect raised by petitioners is whether the Aadhaar architecture is secure, robust and hack-proof enough, given that it is the world's largest human database. The selection of vendors and technology platforms to build Aadhaar, inadequate public consultation of the system's features, risks and safeguards and most of all the centralized single-point storage of the data repository have attracted some criticism in the past. However, technical experts hold that sufficient safeguards are in place including 2048-bit encryption, distributed and redundant storage, etc., that defend the integrity and security of the database. The 2016 Bill does not refer to any guidance on the levels of safety standards to be used in the maintenance and use of the information depository.

Accountability: The Aadhaar Bill 2016 affixes the primary custodianship of the identity information with the UIDAI. Even though the Bill requires all persons with access to Aadhaar related information to keep it secure and confidential and prescribes penalties for unauthorized access or intentional disclosure of information, the penalties are meagre in relation to the significance of the underlying information. The ten thousand rupee fine (one lakh for company) is much more dilute than under the Information Technology Act, 2000, which prescribes for a transacting party compensation up to Rs. 5 crores for mishandling 'sensitive personal data'.

Further, the absence of strong liability provisions in the Aadhaar User Agency agreements do not provide sufficient comfort to big-ticket users, especially public sector banks, when it comes to insuring against liabilities arising from 'false positive' authentication. This has been a major deterrent to large-scale adoption of Aadhaar even for KYC purposes, and banks continued to rely on their own closed-loop KYC systems.

Given the swell of public concerns over privacy, accountability and liability provisions need to be strengthened to serious deterrent levels. This can be best addressed under a Privacy law besides administrative procedures under the Aadhaar Act.

Conclusion

That the public debate on Aadhaar is now over fundamentals is a testimony to India's healthy democratic firmament.

The intent and content aspects are addressed to a large extent explicitly in the Aadhaar Bill 2016. However, more clarity needs to emerge on the government's intent as to the commercial utilization of the UID database beyond the provision of public services, and especially in the sharing or licensing of the information to private parties for providing financial and other services. For that is where the 'public good' character of Aadhaar will squarely be tested. It is important to establish whether the UID data base is a broader 'public good' to be shared and utilized to its full commercial potential by all actors (much like a national highway) or is it to remain an 'e-governance' enabler and exclusive to the state in providing essential public services.

The direction of this discussion will have far reaching implications not only for the state agencies, but also for the huge digital payments market that India can become in the medium term.

More specificity would be needed as to the portent. The thrust of the 2016 Bill seems to be on empowering the state to collect and use personal information for 'national interest' purposes; whereas the coverage of security, privacy and data security safeguards and the direct liabilities of the proposed UIDAI as a statutory body appear prima facie to be diluted and ambiguous, compared to the formulations in the erstwhile NIAI bill.

It is also important to have the dialogue going between the proponents and managers of the Aadhaar and stakeholders who may have legitimate concerns over the potential, if not actual, limitations and risks arising from design or operation of the databases in the various intended services. For this, the government should be more proactive and open to engage and demonstrate how the Aadhaar systems actually work and the safeguards already addressed in the system architecture. Also, the government should ensure use of appropriate best in class technology to maintain and continually strengthen the integrity of the world's largest human database.

Finally, the need for a comprehensive Privacy Bill is becoming ever more important given the potential of the Aadhaar database to serve as an effective 'public good', although with the much required checks and balances which a Privacy legislation can provide as to the sweep of its use by a variety of public and private actors.