International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Exploratory Research On "AADHAR" And Its Impact on Digital Transformation of The Country

Deepanshu Shukla

Student, Galgotias University

INTRODUCTION

In many parts of the world, questions have multiplied on the idea of establishing national digital identity systems. These issues relate to privacy, the concentration of power in the hands of governments, and the role of technology in society. Similar questions have been raised in India with respect to Aadhaar, India's unique identity programme.

In September 2010, 10 people from Tembhli, Maharashtra received their Aadhaar numbers, the very first in the country. Present at the event were then Prime Minister Manmohan Singh and UPA Chairperson Sonia Gandhi, who gave a speech about how the Aadhaar will benefit those who are unable to establish their rights to government benefits.

Nearly a decade later, the Aadhaar programme has seen 1.2 billion enrolments, has been the subject of multiple Supreme Court orders, and given birth to some 252 Aadhaar-seeded schemes. India is not the only country to have adopted a multipurpose or foundational identity system; similar digital ID schemes are in place in countries such as Sweden, Argentina and Nigeria. Because of certain policy decisions taken in the adoption of Aadhaar, an assessment of the programme becomes a worthwhile exercise. While India can draw some lessons from countries such as Estonia and Peru, its own experience looms larger in debates and strategies on digital identity in other parts of the developing world.

Aadhaar: The Rationale for Foundational Identity

The Government of India had considered implementing a national identity project for many years. In 2002, based on the recommendations of the Review Committee set up after the Kargil War three years earlier, a Group of Ministers introduced the concept of a "Multipurpose National Identity Card" to serve as a record of citizenship.

The most common justification for a national identity project was "better inclusion". While various identity documents (IDs) already existed—e.g. the electoral identity card, the income-tax PAN card, the ration card, the birth certificate and the driving licence—none of them could serve the entirety of the billion-strong population, due to their limited coverage and focus on a single use case. No single identity card was accepted across the board for public and private services, with different service providers demanding different sets of documents and verification processes. For example, the 'Know Your Customer' (KYC) rules for banking (to prevent money laundering) required a person to have a government-issued ID card (e.g. ration card or driving licence) as identity proof and a different document for address proof (e.g. utility bills or bank account statements). In the absence of these documents, the person would need a government officer (known as a Gazetted Officer) to issue a letter on their behalf, with an attested photograph. Thus, services—such as social

welfare programmes, banking or aid—were often denied to those who required them the most.An identity programme was proposed to be particularly beneficial for interstate migrant workers: over 139 million people who move to cities either seasonally or permanently and, in the process, find it difficult to establish their entitlements in their home state.

Another reason for introducing a national digital-identity system was to help improve the delivery of government services as well as reduce fraud and corruption. In 2008, a Planning Commission Report indicated that over one-third of the grain intended for poor households was ending up being sold elsewhere, and over half of the subsidised grain did not reach their intended recipients. Being able to accurately determine the identities of beneficiaries would thus reduce leakage and streamline the movement of welfare resources.

Early debates on a national identity card included issues of national security, particularly in border states. However, the Aadhaar programme delinked the question of nationality from that of identity and, therefore, failed to address these concerns.

Across the developing world, the arguments in favour of a national identity system are broadly the same: without it, welfare programmes do not reach their intended beneficiaries effectively; the lack of established identity prevents the most underprivileged from accessing a host of critical services; and governments remain concerned with being able to identify nationals and non-nationals accurately, which is crucial for holding free and fair elections.

Establishing an individual's identity is a complex task in the developing world. While the countries of the OECD (Organisation for Economic Cooperation and Development), for instance, have near-100-percent birth-registration rates, over a billion people across the world lack legal identity due to incomplete coverage of civil registry and functional identity systems. In countries without nationally accepted IDs, affidavits from local government officials are a common demand. However, the process for obtaining these is ridden with the potential for arbitrariness and exclusion.

As of 2016, all but 12 of the world's low- and middle-income countries have launched a national identity programme, including every country in sub-Saharan Africa. While Kenya, Botswana, South Africa and Zimbabwe have relatively high coverage of its identity programmes, other countries have little to show despite substantial investments.[12] Ghana, Nigeria and Tanzania have shown uneven progress, while Somalia and the DRC have underdeveloped and fragmented systems. Regional variation is present in Asia as well. Countries such as Malaysia have a comprehensive multipurpose ID system, while the Philippines has only made several failed attempts at establishing a trusted national system.

Although there is consensus on the provision of "legal identity" as a policy imperative across the world, in the shape of the United Nations Sustainable Development Goal 16.9, "digital identity" continues to be debated, and rightly so. Digital foundational-identity systems involve implementing a 'single unique identifier' for every person, which has the capability to support multiple purposes and applications in the public and private sector.[14] However, without adequate institutional safeguards and well-established democratic practices, such a system can result in a greater concentration of power in the hands of a government, allowing scope for misuse.

India's Aadhaar is a 12-digit unique identity number (UID) issued to every resident of India by the UIDAI, the agency entrusted with this task. The UID is linked to their demographic (name, address, date of birth and gender) and biometric (photograph, 10 fingerprints and two iris scans) information, stored in centralised databases. A card is issued to enrollees, and the identification number, together with a means for authentication (biometric or mobile-linked), forms the basis for identification.

Aadhaar enrolment takes place through existing public and private infrastructure. While a Central Identities Data Repository (CIDR) is managed by the UIDAI, 'Registrars' are UIDAI partners[15] who handle enrolment through authorised connections to the CIDR. The Registrars usually outsource enrolment to UIDAI-certified agencies, which maintain enrolment centres or mobile camps. However, problems have arisen with agencies acting fraudulently, and by 2017, the UIDAI had blacklisted over 49,000 certified agents.

For authentication against the Aadhaar number, the UIDAI created a system under which an agency or company must be recognised as an Authentication User Agency (AUA). AUAs are then allowed to query the CIDR by submitting a person's Aadhaar number and biometric information. They receive a Yes-or-No answer on whether the two match, to establish if the person is who they claim to be. A registered Authentication Service Agency, such as the National Payments Corporation of India, acts as the digital intermediary in this process. For example, for the public distribution system (PDS), "fair price shops" that distribute rations have certified point-of-sale devices, where people must authenticate themselves before picking up their monthly rations.

Lessons from the Aadhaar Experience

Over 90 percent of Indian adults are now enrolled in the Aadhaar programme, making the total about 1.2 billion people. It has become one of the pillars around which Indians debate some of the most critical issues of our times, such as the role of government in our lives; the value of privacy and how we should safeguard it; how public policy should be shaped and implemented; and whether technology is being truly harnessed in the best interests of the citizens.

The following five lessons from India's experience can help other countries navigate the issues involved in the implementation of a national identity system.

1. Identity First

Aadhaar enrolment has been de-linked from a person's nationality and is instead available to all "residents." To be eligible for enrolment, an applicant does not have to prove their Indian citizenship; they must only supply proof of residence for at least 182 days in the previous year. This is a move away from one of the original motivations for issuing an identity card, i.e. establishing nationality, as that could cause significant delay and exclusion.

The Aadhaar has thus adopted an 'identity-first' approach. The number itself does not establish nationality or confer any rights or benefits; it merely establishes who a person is. By establishing their identity, people can claim their entitlements from the government and other programmes. The Aadhaar's minimal data-collection

approach, and the fact that it requires very little information from a person that needed to be verified, made rapid enrolment possible, with use cases and applications being developed subsequently.

In most other countries, IDs are usually either functional (e.g. election cards or driving licences) or issued to nationals for use in a variety of contexts. This stands in the way of comprehensive coverage if the government machinery is not well-placed to collect and verify numerous data points for each enrollee. While each country's context will vary, the Aadhaar, with its minimal data collection, is a good model to consider.

2. A Relentless Focus on Inclusion

A central debate in India over Aadhaar has been on its claims towards inclusion. Proponents point out that vulnerable sections of the population, who have previously been excluded from individual legal identity, now have access to a nationally and widely recognised form of identification, e.g. poor migrants, tribal populations in remote areas, transgender individuals and the homeless. Unfortunately, the Aadhaar's impact on the inclusion of marginalised populations has not been properly evaluated.

An analysis by Kelkar, Nathan, Revathi and Gupta looks at the impact of the Aadhaar on women's lives. Before Aadhaar, the ration card was a common identification document issued at the household level. However, it was typically in the name of the male head. This provided household-level identity, but not an individual identity that could be used to access other services. The Aadhaar number allows women to directly receive transfers under the National Rural Employment Guarantee Scheme, and has helped many apply for SIM cards.

Special procedures were also developed as a response to disability- or occupation-related challenges in capturing biometric data. Certain occupations such as mining can lead to the erosion of fingerprints, and around 8.8 million people suffer from blindness in India. While exception-handling in the case of failure to enrol was built into the system, alternative approaches have also been suggested for improved inclusion.

While inclusion in enrolment is an important issue, an even more important and pressing one is whether the Aadhaar has paved the way for greater inclusion in the actual provision of services. The Aadhaar currently serves a host of identity-related needs: to prove entitlements after migrating from a home state, to open a bank account where one was formerly denied, or to directly receive benefits in bank accounts.

However, critics oppose Aadhaar-based authentication for access to government social-protection services such as the PDS, on the grounds that it introduces too many points of failure, resulting in a denial of benefits. In some states, to obtain monthly rations, a ration-card holder must authenticate themselves—usually through fingerprint verification—at the POS device at the "fair price shop." The 2017–18 ID Insight survey across three states found that Aadhaar-related failures led to 0.8–2.2 percent of PDS exclusion. This included the lack of Aadhaar seeding, authentication failures, connectivity or electricity issues, and the lack of physical presence of the beneficiary to authenticate themselves in the Aadhaar database. Thus, more than two million people in these three states alone faced Aadhaar-related exclusions. Exclusion due to non-Aadhaar reasons, such as the non-availability of rations and the absence of a dealer, was between 0.3 percent (Andhra Pradesh) and 6.6 percent (Rajasthan).

To address these issues, inclusion must be prioritised throughout the system, not only in the rollout of the identity programme but also in every public and private application where it is linked. The primary question must be whether it enhances, or has the potential to negatively impact, access to basic services. For social-welfare programmes to be effective, they must be viewed as entitlements that citizens can demand. Lack of a particular form of identity cannot be the basis for denial of entitlements, and this must be borne out not only in the laws but also in practice. It thus follows that enrolment in digital identity programmes must be truly voluntary, with a demonstration of its benefits being the lead cause for adoption.

The lack of clear evidence from the ground, coupled with an insistence on combating fraud and reducing the weight on the public exchequer, can result in an insistence on digital authentication, whether or not a region or service has the infrastructure and process to support the same. Since technology serves as an amplifier of badly designed policies as well as effective ones, if inclusion is not the primary goal, digital identity will not live up to its potential.

3. Make Privacy and User Consent a True Priority

One of the principal reasons why "legal identity for all" enjoys widespread acceptance, while "digital identity" creates debate, is the concern regarding privacy and information security. A paper-based system offers privacy by obscurity, and a move to a digital system can have irrevocable consequences if there is a lack of sufficient safeguards or holistic understanding of the issues involved.

The Aadhaar was implemented without a framework of data protection and privacy legislation in place, and it is missing in India even today. As a result, while the central repositories of UIDAI have not been breached, the demographic information collected for issuing Aadhaar cards, and the Aadhaar number itself, have been subject to multiple disclosures by government bodies as well as through fraudulent means. In 2018, a journalist for The Tribune was able to buy access, for INR 500 (approx. US$7), to a portal where she could enter any Aadhaar number and obtain the person's demographic details. There was a lack of clarity on the status of this information and the rules about how it was to be collected, handled and disclosed.

Privacy by design principles, such as limiting data collection for specified purposes and controls on the retention of data, must be incorporated into the programme, not only in the design of the technical system (as was done in the Aadhaar) but also in the rules and processes for every partner and agency (public or private) involved in handling identity-related data. It remains a significant challenge, however, for countries where data governance practices are not yet well established, while technologies are rapidly proliferating.

Introducing framework laws and regulations is a necessary step, but it is not sufficient. The system as a whole, including its administrators, processes and technology must prioritise data privacy and data sovereignty; enforcement mechanisms must also be as robust. One approach that addresses these issues in a holistic fashion is the formulation of a 'National Digital Identity Framework' to define clear and effective privacy and data-protection regulatory measures. Such a framework can articulate the rights of individuals enrolled in a digital-identity system, allowing for a strong regulator with adequate enforcement powers, while also ensuring consequences for government agencies that violate the framework. Specific restrictions, institutional checks and balances should be introduced on unlawful surveillance, interception of communications and unauthorised processing of data.[27]

The data-protection and privacy laws that hindered the Aadhaar implementation process also affect the legislative and institutional framework as a whole. The Aadhaar Act did not come into force until 2016, and the Supreme Court had to make several interventions on the status of the Aadhaar, since various government bodies had differing views on how the Aadhaar was to be used. Of central concern was whether the Aadhaar number was mandatory or voluntary and whether the lack of an Aadhaar number could be grounds for the denial of benefits.

The most challenging task in any developing country looking to establish an effective and inclusive identity system is to ensure that laws, policy, technology and logistics move in tandem, particularly because, at the outset, the consequences of adopting far-reaching technological systems are not clear to policymakers. For an ID system to work for the citizens of a country, accountability and transparency must also be built into the system through meaningful consultations, independent audits and effective grievance redressal. Above all, identity systems must operate in a way that centralises user agency and informed consent and provides deeply embedded safeguards against government misuse.

The Government of India has drafted a "Data Protection Bill," which addresses some of these issues. For example, the Bill places data-processing obligations on both the government and private entities, mandates the setting up of a "Data Protection Authority," and categorises biometric data and the Aadhaar number as "sensitive personal data," which has a higher standard for processing. However, substantial categories of government data, including any data that is required to provide a service, are exempted from consent requirements under the Bill, as long as the data is "strictly necessary" for the exercise of that function.[28] The standard, and how it is to be implemented, is yet to be formulated. This, and other concerns regarding the independence and degree of discretion ceded to enforcing authorities under the Act,[29] cast doubts on the Bill's ability to effectively curb government misuse of its citizens' information.

4. Technology Choices and Their Consequences

The Aadhaar programme costs US$1.16 per enrolment, the lowest of any identification programmes in the world. In other parts of the world, costs run up to US$6 for enrolment and up to US$5 per identity card, a burden that low-income countries cannot afford.[30]

The Aadhaar's low costs are achieved through a number of factors, primarily the absence of a smart card, one of the main drivers of cost. However, this makes the system dependent on connectivity for authentication and enrolment, which is difficult to adopt for countries with lower mobile and internet penetration. In India, one of the most contentious points (discussed above) has been the exclusion from entitlements due to connectivity-related authentication failures, particularly in the provision of affordable foodgrains through the PDS.[31]

In response to this concern, the UIDAI introduced offline verification in 2018, through a digitally signed copy of demographic information on a QR code on the Aadhaar card. It enabled local authentication without connecting to the centralised database and also addressed the issue of fraudulent Aadhaar cards. An IDInsight Survey, however, indicates that the paper-based use of the Aadhaar card as identity remains the most common form of verification.[32]

Rapid enrolment was one of the hallmarks of the Aadhaar programme, made possible through a standards-based approach. As briefly outlined above, enrolment and authentication in the Aadhaar system are carried out through agencies that have to be certified by the "Standardisation Testing and Quality Certification Directorate of the Ministry of Electronics and Information Technology." Standards were implemented or devised for testing, which allowed for competitive, off-the-shelf products in all cases, except for the ABIS software for deduplication at enrolment, where only three providers compete. This, too, helped to bring down costs.

Another critical, but often overlooked, aspect of the Aadhaar is that authentication services were built into its design, something legacy systems are not set up to do. The UIDAI established structures and protocols for authentication services to connect with the central ID repository for identity verification, making identity "digital" in the true sense of the word.[33]

In most of the developing world where national IDs have been rolled out, biometric-based enrolment is most commonly used, since it helps establish uniqueness in large populations. Previous identity programmes suffered from duplicate and fraudulent enrolments, eroding trust. However, the collection of biometrics has also been one of the primary grounds for opposition to the Aadhaar programme, and biometric authentication does not guarantee immunity from fraud. Moreover, while biometric-based enrolment is deemed necessary to ensure uniqueness, the requirement of biometric authentication has been opposed on the grounds that it leads to exclusion from entitlements. An overall framework must be established to decide when and why authentication is required for a service, as well as the process for the same, e.g. human verification, biometrics or mobile OTP based.

5. Financial Inclusion

While trying to assess the impact of the Aadhaar system, two instances are most significant: the PDS, where the benefits are disputable; and financial services, where its role in accelerating the KYC process in opening bank accounts has been successful.

Due to increasing complexity in anti-money laundering rules in the banking sector, KYC rules had become cumbersome, in a way that weighed heavily on the most underprivileged. In response, the Reserve Bank of India in 2011 recommended the use of the Aadhaar-based eKYC process for opening small bank accounts. This received a boost in 2014 with the launch of the Jan Dhan Yojana, through which over 300 million accounts were opened using eKYC. However, these accounts remained largely dormant. An uptick in account usage was observed once cash benefits were directly transferred to these accounts, suggesting that the lack of an initial balance might be a deterrent.

What is the lesson for other countries looking to develop multipurpose identity programmes? Even when the ID itself is delinked from any particular function, early applications are crucial in encouraging adoption. Currently, 1.7 billion people worldwide are unbanked. The design of the identity programme, therefore, must take into account the enormous potential for financial inclusion that a foundational identity system can provide.

OBJECTIVES

WhatsApp, Instagram and Facebook were incidentally obstructed in Sri Lanka in mid 2018 for their abuses which assumed a job in fanning the flashes of hostile to Muslim savagery. This time, in any case, it appears to be no phony news was spread – it was somewhat that Facebook and WhatsApp were being utilized to spread recordings impelling individuals to assault the adherents of Islam. Counterfeit news has turned out to be such an enormous issue in India that there the two media and private individuals have taken to the assignment of confirming and countering them.

WhatsApp understands the gravity of the issue. In June this year, the application included a component that educates the beneficiary a the message has been sent (and, along these lines, has not been made by the quick sender). In July, the organization guaranteed liberal research awards for specialists who might think about the field of falsehood. That month, it reported that it restrains the quantity of offers – the greatest number of concurrent talks, through which one can share news and different things – to 20, and to five in India. WhatsApp additionally pulled back the brisk offer alternative for Indian clients. While the declaration, made through a blog entry, considered the progressions a "test," and did not make any reference to counterfeit news or impelled viciousness, a comment significant is that the organization communicated plan to "keep WhatsApp the manner in which it was intended to be: a private informing application." It was likewise evident that India emerged in the message. The declaration considered India a nation "where individuals forward more messages, photographs, and recordings than some other nation on the planet" and the points of confinement WhatsApp has presented explicitly for Indian clients are clearly stricter than the ones forced wherever else.

REVIEW

In any case, is WhatsApp to fault for the phony news and the viciousness they impel and ought to be it singled out from different methods for present day correspondence?

To begin with, it isn't simply WhatsApp. As referenced above, counterfeit news, doctored pictures and recordings speaking to inconsequential occasions were additionally shared on Facebook, Twitter, Instagram and through different strategies. Lawmakers, their turn specialists, and radical hatemongers utilize every one of the devices they can. The conventional media may have more systems to separate phony news from certainty, however a few papers and TV channels assume their own job in spreading falsehood or sheer publicity, and on an a lot bigger scale than WhatsApp's shared messages. As only one of the numerous examples in the Indian setting, one could recollect how preceding the Babri masjid's annihilation in 1992 – the mosque's decimation prompted far reaching Hindu-Muslim brutality – certain Hindi-language papers spread "counterfeit news" that instigated radical Hindus against Muslims. The issue is likewise not constrained to India. WhatsApp has been abused in Sri Lanka, as referenced above, and in Myanmar, Brazil and Mexico, as well.

Second, what isolates WhatsApp from different methods is the innovation. As a straightforward informing application, it was structured as substantially less meddling on individuals' security than the profoundly entering Facebook. WhatsApp's overseers supposedly have no entrance to the substance of messages – they are scrambled except if explicitly revealed. Since Facebook (WhatsApp's proprietor), discovers considerably more about its clients, it has more prominent capacity to battle counterfeit news and more intends to deal with the issue. It appears this is one of the issues of the cutting edge, electronic world: The more a social medium

or an informing application thinks about its clients, the more it can do to confine malignant conduct, yet the more it knows, the more it very well may be utilized to keep an eye on individuals' lives (and hence be abused in similarly fiendish ways).

In a streamlined sense, it is a decision between utilizing devices like WhatsApp and being presented to counterfeit news or utilizing devices like Facebook and furthermore being presented to counterfeit news, having somewhat greater opportunity to report it and battle it, however taking a chance with that our own information can be mined, for instance, to control a race crusade. There is a third decision – not to utilize any of it whatsoever. The center route is to be both cautious about one's protection and about confiding in news (any news: originating from companions, conventional media or online networking). By and by, it comes down to individuals, not their devices.

Third, it is about a chain of trust. I may not confide in the media – particularly in the light of what was composed above – however I confide in my companions. The individual that had sent me the data about "no Islam in Japan" is an individual I trust and know to be straightforward. It is conceivable that this individual gotten the message from another companion, whom that individual trusts. Somewhere in that chain someone abused the trust of other individuals to sell his plan. All things considered, I would not anticipate that anyone should confide in media more than his companions. Maybe it is progressively about depending on companions for data on what they should find out about than us, for example, their own lives or expert skill, however not really on general news.

METHODOLOGY

There are solid individuals to fault for such brutality impelling phony news, and WhatsApp is only one of their numerous instruments. Individuals have been hawking dishonest incriminations against others for a very long time, some time before the Internet, yet even before print media. When finding out about late instances of phony news actuating brutality in the Indian province of Assam, it rung a bell that they look somewhat like how Jews were seen and treated in medieval Europe. In Assam, some outside (for example non-Assamese Indians) people were beaten or lynched on dishonest complaint that they needed to hijack kids. On a general level, it looks somewhat like an old European legend about Jews grabbing Christian youngsters. In the two cases, a dubious thought of the little-referred to "Other" as leading the most terrible demonstration of kidnapping youngsters is utilized to briefly bring together the network in a demonstration of viciousness.

In this way, humankind has a long history of censuring others for anecdotal wrongdoings. Present day apparatuses, for example, online life and informing applications can strengthen the old generalizations that a few gatherings harbor about others. Be that as it may, WhatsApp or the whole Internet ought to barely be accused. Why this might be an unsafe hypothesis, I don't think the Internet has raised the issue higher than ever (and, as an unbiased apparatus, it tends to be utilized as a lot to handle it). Savagery against others was much more regrettable and boundless during the pre-Internet period. Given an opportunity, the Nazis would have definitely utilized the Internet to hawk their loathe, in any case, luckily, the web showed up in our life when instruction and urban obligation turned out to be a lot more grounded, at any rate in certain social orders.

The size of data with which we bomb our brains is past our ability to similarly investigate every last bit of it. What is required is an acknowledgment of which training devices and awareness creation.

CONCLUSION

digital identity systems have the potential for both good and harm. A well-designed system, with adequate safeguards in place, can facilitate civic empowerment and inclusion, unlocking significant economic value.[38] However, issues of privacy, user consent, biometrics and inclusion are still open for debate in countries considering the implementation of such systems.

A common thread connecting the issues regarding the Aadhaar is that the users of digital-identity programmes must be kept central to the design of the system, i.e. to be effective, digital identity must empower people, not governments. The solutions can only take effect within a larger institutional framework that prioritises the rights of the users above other considerations.

BIBLIOGRAPHY

1. www.timesofindia.in
2. www.wikipedia.com
3. www.thehindu.com
4. www.hindustantimes.com