Lessons from Aadhaar: Analog aspects of digital governance shouldn't be overlooked

Background Paper

Prakhar Misra

BLAVATNIK SCHOOL OF GOVERNMENT
UNIVERSITY OF OXFORD

Pathways for Prosperity Commission
Technology & Inclusive Development

Prakhar Misra works with a think-tank in Mumbai, India. He holds a Master in Public Policy from the Blavatnik School of Government, University of Oxford where he was a Chevening Scholar and a Postgraduate Diploma in Economics and Finance from the Meghnad Desai Academy of Economics where he was a Chanakya Scholar.

Background Paper 19
January 2019

The Pathways for Prosperity Commission on Technology and Inclusive Development is proud to work with a talented and diverse group of commissioners who are global leaders from government, the private sector and academia. Hosted and managed by Oxford University's Blavatnik School of Government, the Commission collaborates with international development partners, developing country governments, private sector leaders, emerging entrepreneurs and civil society. It aims to catalyse new conversations and to encourage the co-design of country-level solutions aimed at making frontier technologies work for the benefit of the world's poorest and most marginalised men and women.

This paper is part of a series of background papers on technological change and inclusive development, bringing together evidence, ideas and research to feed into the commission's thinking. The views and positions expressed in this paper are those of the author and do not represent the commission.

Citation:
Misra, P. 2019. *Lesson from Aadhaar: Analog aspects of digital governance shouldn't be overlooked.* Pathways for Prosperity Commission Background Paper Series; no. 19. Oxford, United Kingdom.

www.pathwayscommission.bsg.ox.ac.uk
@P4PCommission
#PathwaysCommission

Blavatnik School of Government
University of Oxford

Pathways for Prosperity Commission
Technology & Inclusive Development

Abstract

Aadhaar is the world's largest biometric identity programme covering about 16% of the world's population. While digital identity projects hold immense potential in improving public service deliveries, the respective governments need to pay attention to and invest enough resources in gaining the trust of the people on the digital ID systems. Overlooking this aspect will not bode well for long-term sustenance of such reforms.

This paper takes an objective approach in highlighting the successes of Aadhaar elucidating (a) its institutional structure, (b) branding and messaging, (c) the strong checks and balances in its design, and (d) the future possibility that it opens up. At the same time, the paper elaborates on the shortcomings of this process explaining how India tackled, albeit inadequately, (a) the dual question of security and privacy of citizen data, (b) fear of surveillance from the state, (c) making the programme optional vs. mandatory, and (d) having clear cut legal backing for the ID system. Overall, the paper looks at the Aadhaar as an example to illuminate non-salient aspects of the political economy of such reforms and tries to explain why governments shouldn't overlook 'analog' complements to digital systems if they wish to reap digital dividends in their countries.

Table of Contents

1. Introduction

The focus around digital ID systems across the world has sharpened in the last decade. Increasingly, governments are realising that harnessing newer technologies can help improve efficiency by reducing informational gaps and minimising transaction and co-ordination costs of governance. The 2016 World Development Report (WDR) noted that growth, jobs and investments are the three most important returns from digital investments. Such investments promote inclusion and innovation, allowing developing economies to 'leapfrog' stages of devising efficient service delivery mechanisms.

Technology has played a crucial role in intensifying the interaction between citizens and governments. Twitter, Facebook and government portals (for example, mygov.in for India) have allowed citizens to learn more about their government and vice versa. While technology has enabled a closer interaction between the government and its people, some citizens remain hidden. In sub-Saharan Africa, for example, 55% of people still have no official identification record, but 67% have a mobile phone subscription. The World Bank, in its World Development Report, noted that, while technology has spread rapidly, its benefits for development have lagged behind. 'Digital dividends' are yet to be harnessed.

To fill that gap, the logical next step for governments would be to build public infrastructure, using technology to deal with identity and reap such dividends. This should be a particular priority in countries where existing identification (ID) systems are less effective in identifying citizens because they are either exclusive, expensive, disconnected to services, or there are too many of them, and so on. Apart from being a fundamental human right, official identity can unlock formal services and give people a legitimate voice in the system. Voting, legal action, banking and government services are all denied without this formal recognition. Private services such as loan applications, business registrations, school enrolment and land titling can be more readily accessed when citizens have an official identity. USAID, in its report *Identity in a Digital Age: Infrastructure for Inclusive Development*, also notes: "Robust identity systems can help protect against human trafficking or child marriage. In many ways, the roughly 1.1 billion people who lack official identity are invisible, discounted, and left behind."

National identity systems are being studied all around the world. Insights from ID systems in Armenia, Moldova, Vietnam and the Organisation of Eastern Caribbean States point towards ease of service delivery in their respective countries. Similarly, evidence from Botswana's biometric enrolment of pensions and social grants resulted in a savings of 25%. In Nigeria, biometric audits reduced the pension roll by 40% (World Bank, 2016). Many low and middle-income countries, such as Peru, Thailand, Rwanda and Pakistan, have pioneered ID systems that have wide coverage and usability. However, other countries are facing problems – for example, Nigeria and the Philippines have multiple disconnected identity programmes, and conflict-affected countries, including Somalia, Liberia, South Sudan and the Democratic Republic of Congo, are struggling to build theirs (Gelb and Metz, 2017).

There are some successful models of digital ID systems that can be adapted depending on the context of the country. Syndicated models, such as the one in Estonia, are used for a variety of services. The system issues an electronic ID card with a chip using 2048-bit public encryption (which ensures that only the intended recipient can access the information). The UK's Gov.uk Verify is an example of a centralised ID system, where a citizen's digital ID is set up once and then verified every time they use the service.

India's biometric identity programme, Aadhaar (meaning: 'foundation'), is a recent development and has made tremendous progress since it started in 2010. With approximately 1.2 billion people enrolled, 16% of the world's population holds an Aadhaar number. This makes Aadhaar the world's largest biometric ID programme. Since September 2010, when the world's first Aadhaar number was issued, India has covered 99% of its total adult population over the age of 18.

While there is reliable literature around the digital parts of such ID systems, it is the "analog complements", to use the World Bank's term, that require more deliberation and research. The issues that need more exploration and control include:

- Legal frameworks around data safety
- Business environment to prevent monopolistic behaviour
- Interaction between regulation and technology
- Accountability and grievance and redress mechanisms
- Impact on labour market disruptions
- Effects of a more networked citizenry

There is much to learn from India's biometric programme – from the digital and the analogue components of the digital ID system. As a recent endeavour, Aadhaar certainly has lessons on how to balance the analogue and digital components of new ID systems. India's experience holds key lessons for governments across the world to incorporate certain 'best practices' – including fighting legal battles, emotive political speeches, dealing with issues around data leaks and state surveillance. There are also lessons in the mistakes that Aadhaar inadvertently committed which led to a loss of trust and, in some cases, may have contributed to loss of lives in India.

2. Aadhaar: a primer

2.1 The need for an ID system

Subsidies are the backbone of India's political economy. From Rs.1.22 billion in 1991, the food, fuel and fertiliser subsidy increased to Rs. 1.73 trillion in 2010. The scale of these outlays, however, did not always translate into accordant outcomes (Aiyar, 2017). Inadequate targeting, rampant corruption and funding leakages crippled the system and prevented the poor from claiming what was legitimately theirs. Official estimates indicate that in 2011–12, 41% of the kerosene subsidy, 15% of rice, 54% of wheat and 48% of sugar subsidies, respectively, were lost as leakage in India (Economic Survey 2014-15, Government of India).

At the turn of the millennium, the government started discussions around a national identity card. This was primarily driven by national security issues (Kargil War of 1999) and efforts to prevent money laundering, which hastened after the US created the Financial Action Task Force post the 9/11 attacks. While previous ID cards existed, they were problematic, each having a number of fake entities and countless ghost registrations. The transaction costs to redress those issues would be very high. Besides, some states in India had more ration cards than households and correcting for that would require high economic and political investments, making it a difficult task to execute. Therefore, a Multipurpose National Identity card (MNIC) project was proposed. A pilot was conducted, providing the first set of ID cards in 2007. However, they soon realised the circular problem: 'to get a document you needed to prove identity and to prove identity you needed some document' (Aiyar, 2007). This led to many groups being excluded and fell short of meeting the MNIC's original aims. Also, MNIC had a political appeal to it, leading opposition politicians to refuse to implement the project in the states that they had control over. The first problem with the MNIC pilot could be resolved by introducing technology in the process. The second problem, however, required building a new system which would be apolitical in its branding.

In 2004, a new government came into power with a mandate of targeting subsidies for the poor. The government did increase spending towards the marginalised sections of the society. The central government's share of expenditure on social services increased from 10.46% in 2003–04 to 19.46% in 2009–10. This resolve intensified the need for a better system to deliver the required services to the target recipients. In 2006, a unique ID for families below the poverty line (BPL) was proposed. The plan was to link the ID database with election rolls in India for speedy enrolment. But demarcation issues within the government caused much deliberation and a separate authority was created in 2008 called the Unique Identification Authority of India (UIDAI), with Nandan Nilekani as its chairperson. UIDAI gave birth to Aadhaar and chose it among other competing proposals, both at the union and state levels. It was clear that this system should have a twofold mandate: first, it would have to identify the needy accurately to reduce inclusion/exclusion errors; and second, it would make sure that, when claims are made, the person seeking benefits is in fact who they say they are.

In 2012, the National Institute of Public Finance and Policy (NIPFP), a research institution focused on public economies and policies did a cost-benefit analysis of Aadhaar. They concluded that Aadhaar would yield a substantial benefit when integrated with a variety of welfare schemes across India. "Even after taking all costs into account, and making modest assumptions about leakages, of about 7–12% of the value of the transfer/subsidy, we find that the Aadhaar project would yield an internal rate of return in real terms of 52.85% to the government" (NIPFP, 2012). In theory, Aadhar sounded like a great idea, but rolling out the programme for more than a billion people was a huge challenge.

2.2 What is Aadhaar?

Aadhaar is a 12-digit number linked to the biometric and demographic identity of an individual. Out of the 12 digits, 11 digits are randomly generated while the twelfth digit is used to check for data entry errors. Many ID systems in the world have information encoded in the number itself, with a particular digit for gender, birthday or the birthplace of the person, and so on. But, given Aadhaar's random number, no one can tell anything about a person by just looking at the number.

For the first time in India, an ID system existed that was designed to be portable and adaptable. Previously, other identification numbers issued were limited by purpose and issuing authority. For example, a driver's licence would be valid only while driving/riding and a Permanent Account Number (PAN) card would be valid only for taxation purposes in India. Different identity systems could not identify individuals across government services. This lack of interchangeability led to confusion and red tape, increasing systemic inefficiencies.

Aadhaar is unique for two reasons. Firstly, it is a number, not a card. The proof of an Aadhaar number, is the number itself which can be verified by any authorised body, be it a government or private entity. No other physical identification proof is required. Secondly, for the first time in India, biometrics have been used to uniquely identify a person. Fingerprints and iris scans were used to enrol a billion people under this system. As the biometric data of an individual is linked to Aadhaar, a fingerprint scan or iris scan would prove the real identity of the Aadhaar holder. This reduces the chances of duplicates and of unknown persons claiming benefits from the system – something common in former identification and targeting mechanisms.

2.3 Organisation structure

UIDAI is the body that enrols people on the Aadhaar system. It was established by an executive order (2009) and then by statutory backing through legislation in the Parliament (2016). It is housed under the Ministry of Electronics and Information Technology (MeitY), Government of India. UIDAI manages eight regional offices and two data centres across India, with a chairperson, CEO and two part-time members.

Enrolment is completed through registrars and enrolment agencies. The UIDAI website says: "Registrars are typically departments or agencies of the State Government/Union territory, public sector undertakings and other agencies and organisations who interact with residents, in the normal course of implementation of some of their programmes, activities or operations. Examples of such Registrars are Rural Development Department (for NREGS) or Civil Supplies and Consumer Affairs Department (for TPDS), insurance companies such as Life Insurance Corporation and Banks" (UIDAI, 2019).

The enrolment agencies are enlisted by UIDAI and paid for the successful generation of Aadhaar numbers. These agencies set up enrolment centres with the necessary equipment, following the technical standards specified by UIDAI.

Notes:

- The outsourcing of such processes did cause some problems. In one instance, the captain of the Indian Cricket team, MS Dhoni's biometric details were allegedly leaked. In another instance, a journalist obtained two enrolment IDs from an enrolment centre, raising questions about the safety of collected data by private companies.

- UIDAI has been cognisant of such problems and has taken care to monitor the quality of enrolments. In one case, all enrolment operations in the state of Karnataka were halted until the genuine ones were verified. UIDAI also said: "...All Aadhaar enrolment centres functioning from private buildings will be directed to move into government-owned buildings..."

- UIDAI has also changed its laws regarding the norms for such empanelling. For example, UIDAI relaxed Aadhaar enrolment policies so that banks could also act as enrolment agencies.

- In 2017, the Supreme Court took the stance that biometric data collection by private agencies was not a good idea (Firstpost, 2017).

2.4 Enrolment, generation and storage of Aadhaar numbers

An Aadhaar number is generated as follows:

a) An individual goes to an enrolment centre and provides the necessary demographic and biometric details. The mandatory information that has to be provided includes name, date of birth, gender, residential address, photograph of the face, fingerprints for all fingers and iris scans of both eyes. UIDAI has specified the proof required for all data provided during enrolment. Providing a mobile phone number and email ID is optional.

b) The collected information is encrypted and transferred to the Central Identities Data Repository (CIDR) within 20 days. Either a Secure File Transfer Protocol is used or, in case of infrastructural difficulties, the encrypted data is transferred on portable hard disks by post to the CIDR.

c) At the CIDR, the new incoming data is compared with the existing database to check for duplicates. This process is called deduplication. All identified duplicates are manually assessed to check for processing errors.

d) After deduplication, a randomly generated 12-digit Aadhaar number is assigned to the individual, if the enrolment is successful. If not, the registrar and the individual are informed of any corrections and next steps to take.

e) Once the individual is enrolled, the Aadhaar number is sent to their address by post and an e-Aadhaar is also made available for download.

Notes:

• The data is decrypted at the CIDR for deduplication purposes but it is not held in storage in its decrypted form. It is also essential to highlight that the final deduplication check is done by a human, and only then is the Aadhaar number generated.

• Even if an individual doesn't have an existing ID to prove any of their demographic information, they obtain an Aadhaar number through the 'introducer' system. The introducer could be the head of the family or someone from the locality who could vouch for the individual. The introducer must have an Aadhaar number. UIDAI also enrols people who don't have the requisite biometrics by using their photo as a primary identifier, with markers to determine uniqueness.

• An Aadhaar card is for all residents of India, not citizens of India. Once an Aadhaar number is issued, it can't be used again. If a person dies, UIDAI will not use their number for another person.

• Getting an Aadhaar number is free of cost.

2.5 The Aadhaar authentication process

After enrolment, an individual's identity can be cross-checked at any time and from any place by any authorised body. Depending on the purpose of authentication, UIDAI has set out five ways to authenticate:

• **Type 1:** Service delivery agencies can use Aadhaar Authentication system for matching Aadhaar number and the resident's demographic attributes (name, address, date of birth, and so on).

• **Type 2:** This allows service delivery agencies to authenticate residents through a one-time-password (OTP) delivered to resident's mobile number and/or email address present in CIDR.

• **Type 3:** Service delivery agencies can authenticate residents using one of the biometrics, either iris or fingerprint.

• **Type 4:** This is a two-factor authentication with an OTP combined with biometrics (either iris or fingerprint) for authenticating residents.

• **Type 5:** This allows service delivery agencies to use OTP, fingerprint and iris together for authenticating residents.

While the five types of authentication outline different *inputs* required, UIDAI also gives two broad types of *outputs*. The first is a 'yes/no authentication'. In this process, the demographic or biometric data of the individual is entered by the designated agencies and the CIDR checks it with the database and returns either a 'yes' or 'no' depending on the result. This merely verifies the identity of the concerned individual without giving any personal information.

Figure 1: Yes/No Authentication trend

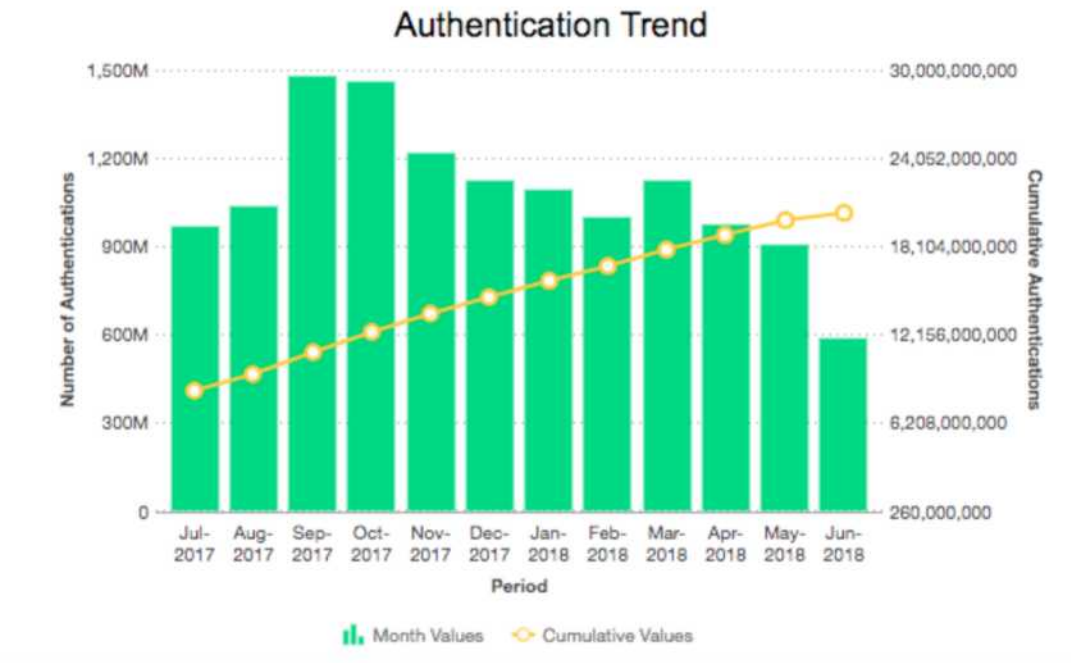

Chart from: uidai.gov.in

The other type is called 'e-KYC' (know your customer). On authentication via biometrics or OTP, the CIDR is authorised to return proof of identity for the individual, including address, date of birth and gender.

Figure 2: e-KYC Authentication trend

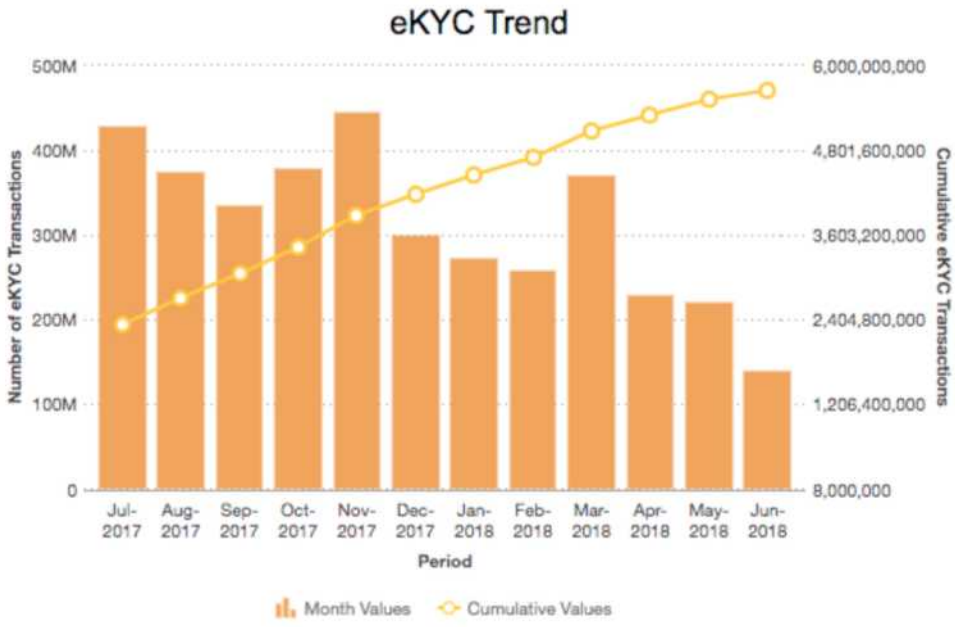

Chart from: uidai.gov.in

3. Aadhaar: a report card

People's trust of UIDAI varies. This is partly because of Aadhaar's technology-intensive nature which keeps some people sceptical of the safety and security of data. In *Rebooting India,* Nandan Nilekani and Viral Shah describe how people in rural India did not mind standing in line and registering for an additional identity number. They illustrate with an incident where a person compared an identity card to getting a buffalo. If the government was to give him another buffalo, there was no reason for him to refuse, and he would most definitely enrol in the project.

Contrast this to the urban centres, where the residents were thinking about opportunity cost of the time they spent standing in line at enrolment centres. They also questioned whether this exercise will reap any future benefits or if it would be more likely to fail like other similar endeavours. Questions about the fear of surveillance and the creation of a 'Big Brother' state are concentrated in specific parts of the country where people oppose the ubiquitous use of Aadhaar. Aadhaar's advocates support it on the grounds of increasing efficiency in service delivery mechanisms, which mostly benefits the poor. Even though Aadhaar was created as an optional system, it was made mandatory after it received legislative backing. While there was a lot of pushback to this in mainstream media debates, a recently conducted survey in 3 states across India shows that 87% of rural residents approved mandatory linking of Aadhaar to government services; and 77% approved the linking for private services (State of Aadhaar Report, 2017-18).

3.1 Aadhaar's achievements

3.1.1. Service delivery and the 'cascading effect'

The Aadhaar project's mandate was essentially to identify individuals. This goal of unique verification was mostly important to improve efficiency in targeting and delivering subsidies in India. However, Aadhaar's effect has moved beyond that original goal.

Year-on-year, the government has been consistently increasing the share of funds transferred directly to beneficiaries' bank accounts. In this regard, Aadhaar has been instrumental in two ways. The first is to help Indians open bank accounts. Financial inclusion was a big problem, with almost two in every three Indians not having a bank account in 2010. While there were many reasons for this, prominent was the lack of proof of identification. Therefore, people could now use Aadhaar to identify themselves and open a bank account. This, coupled with schemes like 'Pradhan Mantri Jan Dhan Yojana' (Prime Minister's People's Bank scheme), which allowed for zero-balance accounts, has led to 80% of Indians holding a bank account as of April 2018. Of the total number of bank accounts opened globally between 2014 and 2017, 55% were from India. Figure 3 shows the rise in use of Aadhaar as proof of identity to open a bank account.

Figure 3: Use of Aadhaar as proof of ID to open a bank account

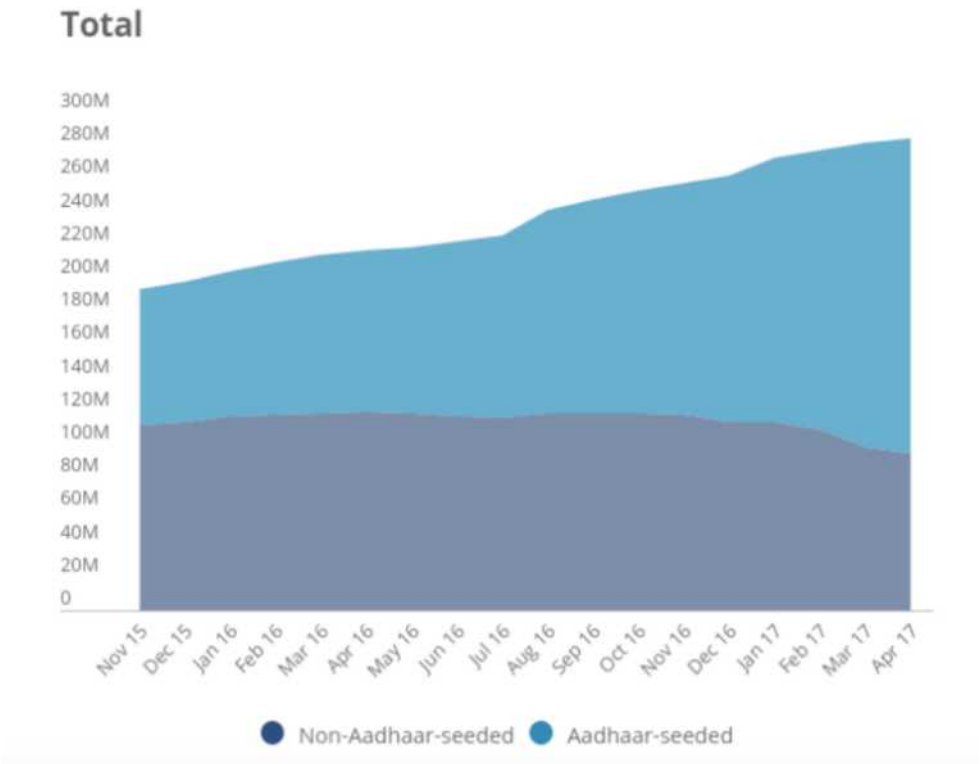

Chart from: Aadhaar as Payment Infrastructure: Current Implementation and Challenges

The second is the invention of the Aadhaar Payments Bridge System (APBS). The APBS allows the government to directly transfer subsidies to people's bank accounts, navigating rent seekers and improving efficiency in the process. The government estimates that, as of December 2017, Rs. 2.43 lakh crore (US$37.38 billion) has been disbursed through Aadhaar under 394 government schemes.

The government also claims that 23.3 million bogus ration cards and 30 million fake liquefied petroleum gas (LPG) connections were identified. Another scheme called 'Jeevan Pramaan', which is an Aadhaar-based platform for biometric authentication of pensioners and senior citizens, has seen tremendous growth. From 1.65 million people registered on it in 2016, the number has increased to 15.015 million pensioners to the end of 2017.

The APBS has had issues of its own. For example, if there are multiple accounts linked to an Aadhaar number, then the money is transferred to the last linked account, leaving people confused about when the money was deposited, if at all.

In 2017, the government claimed that Aadhaar has led to a savings of Rs. 57,000 crore (US$8.11 billion) between 2014 and 2017. Some analysts claim that the methodology used to calculate these numbers is flawed. Some even say that evidence around these figures is missing (Abraham and Dubey, 2018). Yet, the government continues to stand by its projected figures. As of July 2018,

the figure has increased to 90,000 crore (US$ 12.9 billion). Even if the government's statistics are flawed, there is little doubt that Aadhaar has had a cascading effect across public and private service delivery mechanisms. Its simple structure of identification has opened up possibilities for companies to innovate and increase the consumer surplus in the economy.

The Aadhaar Enabled Payment System (AEPS) fosters digital payments across banks, making the network interoperable. The United Payments Interface (UPI) was then rolled out, allowing instant payment and transfer of money between banks using the Aadhaar number linked to the bank account. This enabled Whatsapp to launch a payments feature in India. While it is beyond the scope of this report to go into detail of the UPI's functions, it is worth noting that UPI transactions increased from 4,000 per day in 2016 to 256,000 per day in 2017. The total AEPS transactions doubled from 6 million in April 2017 to 13.7 million in March 2018. Clearly, despite the availability of traditional financial transaction mechanisms, people in India are using these services, and finding real value in them.

The government also rolled out a digital locker. This is an online repository of documents that users can share with others. School and college mark sheets, drivers' licences, government health records and other documents are uploaded to the portal by the issuing authority, for access by registered users. This is also made possible by the seamless link with Aadhaar. Aadhaar allows unique mapping of each individual to his or her digital repository. The authentication feature prevents their documents from being misused.

Aadhaar authentication is already being used for multiple schemes involving public distribution of goods, rural employment, and in education. Government services such as driver's licences, passports and income tax returns are also linked to Aadhaar, making the process paperless.

In *Rebooting India*, Nandan Nilekani lists how Aadhaar is transforming governance in India today, and how it could be used in the future. Already in the early implementation stages, an e-signature feature will allow any individual with Aadhaar to digitally sign transactions and documents. Nilekani also highlights the creation of an Aadhaar-based voter-management system. Expanding the use of Aadhaar numbers to link to cars will allow seamless electronic tolls across the country, saving time and money on delivery of goods across the country. Other sectors such as justice, education, healthcare and energy would also be affected in the future.

3.1.2. UIDAI's institutional structure

To implement a project as novel as Aadhaar, a new institution had to be set up with clear aims and objectives. An early realisation was that a mix of people from both the public and the private sectors were needed to see the project through.

Aadhaar's founder Nandan Nilekani needed people who were well-versed with government functions. It was important to get the paperwork and the request-for-proposals right, as even a small mistake could significantly prolong timelines or completely derail the project. From the public sector, he recruited candidates who had been veteran bureaucrats but who also had an interest in technology. Ram Sewak Sharma, an Indian Administrative Service (IAS) officer with an interest in coding, was brought on board. Similarly, other officers like N. Ganga who had pioneered the use of technology in previous roles were asked to join the project. A balance was sought between knowledge of the government ecosystem and faith in technological adaptation and innovation.

Having co-founded Infosys, a technology giant in India, Nilekani knew the relevant people he could bring on board from the private sector. Domain and technology experts were brought in to build a robust backend of the technology system. It was the largest of its kind and was to store, and make available in real time, details of more than a billion citizens. Former Infosys employee, Pramod Varma, became Aadhaar's chief architect; Viral Shah, a PhD in Computer Science and co-inventor of Julia programming language; Shankar Maruwada, CEO of Marketics; Sanjay Swamy, CEO of mCheck among others joined in. A marketing team was needed to manage the optics and get the public and politicians invested in the idea. They were recruited from various private sector companies. As Shankkar Aiyar writes in his book *Aadhaar: A biometric history of India's 12-digit revolution*: "the procurement processes of UIDAI, the use of in-house trials for cost and proof of concept studies for outcomes, outsourcing the man-machine matrix and opting to pay for services, are among shared best practices within the Government of India."

Ram Sewak Sharma also said: "Creativity lies at the junction of different disciplines, not in a homogeneous group, but in heterogeneous groups." (Aiyar, 2017) The central principle while building the institution was to bring in diversity, irrespective of where people came from.

UIDAI's size was also key to its seamless functioning. A compact company enables efficient decision-making. UIDAI's original template had 1400 people, but it was trimmed down to 200–300, keeping efficiency in mind. A small team was dedicated to building Aadhaar's fundamentals, while a lot of work was outsourced and other state government departments chipped in to make it happen.

3.1.3. Aadhaar's design

While building an identity system from scratch, the kind of information collected is key to the project's success. The Aadhaar team faced a trade-off from the very beginning. The dominant thought process was to collect as much information as possible. The marginal cost of adding an additional question to the survey was nothing compared to doing the survey all over again to collect more information. However, there were constraints on the efficiency of the process and the quality of responses being affected by the addition of subsequent data points. In competition with Aadhaar was the National Population Register, with 16 fields of data being collected. There was pressure for Aadhaar to collect all possible data from people, including disability and blood group, even though they were not important to the central identity question that Aadhaar was trying to solve. UIDAI stood their ground and eventually, data collection was limited to basic information such as name, gender, age and address. Mobile phone number and email ID remained optional.

UIDAI also proposed collection of biometrics for the project. While fingerprint collection was undebatable, the question of 'how many fingers?' was raised. Given that much of India is engaged in direct labour, balding of fingerprints is a well-known phenomenon. Thus, they decided to record all 10 fingerprints. Some states in India were already using fingerprints to register and deliver services. Andhra Pradesh had issued biometric ID cards to ensure efficient service delivery. Bihar too had a biometric programme to ensure timely wage payments to beneficiaries of a rural employment scheme. The Union Government had also issued biometric ID cards in coastal villages across nine states after the 2008 Mumbai terror attacks, where the terrorists entered the country by boat. Following this, the UIDAI Biometrics Standards Committee was set up and collected more than 250,000 fingerprints from 25,000 people across all rural regions, using different devices, with different operational processes. The report that followed highlighted that the operational process and quality of devices used are essential to obtaining good-quality fingerprints.

Apart from fingerprints, the Aadhaar team also incorporated iris scan recognition. This was done in consultation with a variety of experts and after the biometrics committee concluded that iris scans would improve deduplication accuracy. There were two hurdles in incorporating iris scans. The first was that iris scans require high levels of computing to collect, encode and store the data. Thus, the technology process being designed needed to take this into account. Academics from various universities were consulted before designing the specifications. The second was that the technology was still under patent and thus expensive. The decision was made to go ahead because the scale of use would automatically bring prices down.

Another crucial question debated by UIDAI was whether to issue a card or a number. Keeping in mind the principle of portability, UIDAI wanted to only provide a 12-digit number, while the government was keen on issuing a physical card. After much debate, they settled on the middle ground by deciding to send a 12-digit number in a printed letter. The number on its own would be sufficient proof as it could be authenticated in real time, and so people were not required to present the letter to verify their Aadhaar number.

3.1.4. Strong checks and quality controls

UIDAI created a 'hub-and-spoke' architecture for Aadhaar as they realised they needed partners to help implement the project on such a large scale. State governments and private entities were involved in the process for this reason. UIDAI also recognised the need to use multiple equipment vendors to enrol people under Aadhaar. Over-reliance on any one vendor could have potentially derailed the project. The UIDAI team learnt from the US-VISIT programme that their software and hardware was 'locked-in' with only one vendor. However, US-VISIT handled around 100 million people and the number for Aadhaar was 10 times that. Diversifying risk with hardware and software was key to keeping the project going.

In their training manual on biometric devices, UIDAI outlined specifications for all devices (both biometric and non-biometric) to be used in the enrolment process. It gave guidelines on granular details such as the position of the fingerprints and the iris, and for the shutter speed and aperture of the camera. The document also provided details for the enrolment processes for senior citizens versus children, using graphical descriptions and comic strips. UIDAI has developed one of the most robust mechanisms while enlisting agencies to conduct the operation at such a large scale. The CEO of UIDAI once exclaimed that the universe's strength was needed to break Aadhaar's encryption.

Aadhaar had quality checks built in at every stage. Thus, aberrations could be detected and fixed early on in the enrolment process. One such incident was in January 2011 when the data packets for the left and right iris were reversed for a sizeable number of people during enrolment. But, because it was detected early, the team was able to write algorithms to identify the position of tear-glands on each of the scans and flip the images, thus correcting for the discrepancy (Nilekani and Shah, 2015).

3.1.5. Outreach and branding

The positioning of any idea is incredibly important to its success or failure, especially if it is radical and has the potential to be a 'game changer' in any domain, including governance. The complicated name of the issuing authority – UIDAI – was a deterrent in explaining the concept to politicians and the general public. The team took this challenge seriously and thought of hundreds of names for the project. They paid special attention to identifying exactly what people across India needed to know to understand and embrace this idea. Marketers from multinational firms joined the project to streamline the communication. They travelled across India to understand how the larger populace interpreted the project; they sat with writers to come up with names that could communicate the idea in a simple but effective manner; they used graphical representations and infographics to explain problems faced by individuals due to the lack of a unique identification mechanism. Finally, after a conversation with a rural resident of India, they came up with the name 'Aadhaar', which means 'foundation'. After this, extra efforts were undertaken which were crucial to successfully communicating the Aadhaar concept and benefits, and to encourage larger take-up and a more positive attitude to the Aadhaar number.

3.2. Aadhar's failures

3.2.1. Data security and privacy in India

Data security and privacy are two separate yet interlinked issues. When Aadhaar was being developed and launched, there was an animated debate around data leakage and the possible mechanisms for redress. As early as 2009, UIDAI had identified that privacy would be a hotly debated issue. In its Strategic Overview, it talked about how a balance between "privacy and purpose" is important and should be achieved. Their consultation paper, *Legal Framework for Data Protection and Security and Privacy Norms*, was released in July 2010. The paper argued that, while there were some existing laws regarding these issues, a new, broader law would be needed, with a mandate beyond Aadhaar, covering e-governance issues and data sharing and privacy from third parties. Yet, as the law was being debated, Aadhaar was rolled out in its entirety and many activists started opposing the move due to the lack of legislation governing UIDAI's existence and the privacy and security concerns around Aadhaar.

Justice KS Puttaswamy, a retired High Court judge brought a case challenging Aadhaar in light of the potential violations to individual privacy. The Supreme Court heard his case and a nine-judge bench recognised the Right to Privacy as a fundamental right emanating from Article 21 of the Indian Constitution. This was a landmark judgement in India's legal history.

However, before this judgement was passed and its effects felt, the government had made many errors, leading to a panic about data security and a subsequent privacy breach. There have been multiple instances of government websites revealing confidential Aadhaar data publicly. The first such display was in February 2017, but despite the knowledge, this problem has continued to persist. The leaked data was generally about subsidy beneficiaries – including the rural employment programme, pensions or the food subsidy programme in India. If the Aadhaar number alone is leaked, there may not be much damage caused. However, government websites often listed other confidential details such as bank account number, pay order amount, time and date of disbursement, number of days worked, gender, caste, age, religion and even the geo-location of the beneficiaries of these schemes.

They have further maintained that the UIDAI portal has never been breached and it is safe and secure. Despite this, a security researcher in India has revealed details of leaks from the government. While this may not come from a direct breach of the Aadhaar database, it is still worrying for people to find their Aadhaar number and details vulnerable to a breach. Many claim that not much can be done with the 'leaked' data as Aadhaar inherently requires authentication – either biometric, through an OTP, or a combination of those. This, however, does not absolve the government from such practices. Between February 2017 and April 2018, there have been more than 220 cases of data leakage or wilful revelation of information.

A French Security researcher Robert Baptiste, going by the pseudonym of Elliot Alderson, has been testing the security of websites maintained by the Indian government (Medianama, 2018). He has been consistently able to find and identify citizens' Aadhaar numbers. He was also able to retrieve the biometrics of certain Aadhaar cardholders. UIDAI continues to maintain that there has been no data breach.

Also, in January 2018, a newspaper journalist from *The Tribune* broke a story that revealed she could get a billion Aadhaar numbers for as low as INR 500 (Khaira, 2018). 'Agents' had software that could allow access to all information related to the Aadhaar number as well as enable the printing of an Aadhaar card. There were also reports of spurious Aadhaar cards being generated under a dog's name (Indian Express, 2015). In another incident, 100 farmers in the state of Maharashtra were found to be linked to the same Aadhaar number (NDTV, 2017). The veracity of UIDAI's claims about Aadhaar's safety and security was now under scrutiny. The broader question and fear continues to remain that the law is ineffective and is falling short in protecting India's citizens.

These incidents have led to three major problems. The first is the lack of a redress mechanism for citizens. While there is a toll-free number and a provision to establish contact centres in the law, the exact procedure isn't clearly communicated to the population. The wider problem is a legal one. People were left wondering what they would do if their data became publicly available, how safe their data was, how such a leak would be justiciable, and who would be prosecuted, under what law? There are no clear-cut guidelines for this and this certainly creates unease among the citizens of India. This is mostly due to the lack of a data protection law. While India does have certain laws governing the internet, these do not keep the government accountable on citizen's data. Moreover, the powers of the UIDAI were quite wide-ranging and many felt a threat from that too. Regulations gave UIDAI authority to deactivate Aadhaar numbers and control the publication of the minutes of the meeting whenever the members met - holding the power to censor and publish the minutes of the meeting, reducing transparency in the process.

The second problem is the lack of a bug-reporting mechanism. There is no formal way to reach out to the authorities and tell them the issues of security that the UIDAI portal faces. Ethical hackers and security researchers have often found instances when the Aadhaar database fell short of protecting citizens' data. This further leads to non-reporting of vulnerabilities and leaves the database open for potential breaches. The bigger problem is that, time and again, the government counsel has mentioned that citizens, researchers and Aadhaar users are welcome to provide input and give feedback to make sure the system works well. Yet, such mechanisms have been largely absent or, where they have been implemented, have not been efficient enough.

Third, it is UIDAI's response and its mismanagement of such issues that is problematic. In *The Tribune* incident, they responded by saying that there was no data breach, but it was a case of "unauthorised access", yet they filed a first information report (FIR) against the journalist. Similarly, in a series of tweets, UIDAI dismissed all of the information that Elliot Alderson was releasing, finally compelling him to disclose a folder with biometric data for some Indian citizens.

Under Justice BN Srikrishna, a committee was set up to draft a data privacy law and establish a data controller for India. A white paper was circulated for comments from civil society in December 2017, and, in August 2018 a draft law titled 'The Personal Data Protection Bill 2018' was released. The bill is yet to be tabled in the parliament.

3.2.2. Aadhaar's constitutionality

India follows a parliamentary style of democracy with a bicameral legislature, the parliament being divided into the Lok Sabha and the Rajya Sabha – the lower and upper houses of Parliament, respectively. The Constitution of India allows various types of bills to be tabled in Parliament – ordinary, constitutional amendment, financial and money bills. Aadhaar was tabled and passed as a 'money bill' in Parliament. There are seven grounds for this, broadly to do with government borrowings, withdrawals, taxation – essentially anything to do with the Consolidated Fund of India. The key question is whether the Aadhaar Bill, officially titled the Targeted Delivery of Financial and other Subsidies, Benefits and Services Act, 2016 qualifies as a money bill or not.

To pass a money bill, only the Lok Sabha needs to have a majority. The Rajya Sabha can merely send comments on the bill to the Lok Sabha, which includes or rejects those comments. This practice is mostly borrowed from the Commonwealth system due to India's colonial past. A similar practice continues in the UK today. A money bill can be passed if there is majority in only one of the two Houses of Parliament, which is unique to this category of bills. The current government has a simple majority in Lok Sabha, but not in the Rajya Sabha. Thus, there are allegations that it was easier for the current government to pass the Aadhaar Act as a money bill, and so they tabled it that way in Parliament. This is a challenge to its very constitutionality.

The government's defence is that Aadhaar is primarily a targeted delivery of subsidies which are withdrawn from the Consolidated Fund of India, thus making this a legitimate money bill in Parliament. The Rajya Sabha suggested multiple amendments to the Aadhaar money bill. The two most important related to the fear of government mass surveillance, and making Aadhaar mandatory rather than optional (we discuss this issue later). But the Lok Sabha overlooked both of these concerns and passed the bill.

Legal experts argue that only one section of the Aadhaar Act (section 7) has anything to do with the Consolidated Fund of India. In fact, in the whole bill, the Consolidated Fund of India is only mentioned three times. The government lawyers dismiss these concerns by turning to a different argument. They cite procedural norms such as the Speaker of the house having a final say in the categorisation of the bill, and that such Acts are protected from Judicial Review, making the challenge itself void. Such defences do not serve to uphold Aadhaar's legitimacy and do not encourage positive public perceptions about this biometric project.

From February 2018 onwards, the Supreme Court decided to take 27 writ petitions challenging the constitutionality of Aadhaar as a money bill. In September 2018, the Supreme Court upheld the constitutional validity of Aadhaar with certain caveats. There was a 4-1 split among the 5 judge bench. The judges said "In the present case as well, we have come to the conclusion that Aadhaar Act is a beneficial legislation, which is aimed at empowering millions of people in this country", while the sole dissenting judge went on to say, "passing it as a money bill is a fraud on the Constitution and it violates its basic structure."

3.2.3. Mandatory or optional?

Aadhaar was designed as a voluntary, opt-in programme. Many voiced their concerns, but the government always took the stance that Aadhaar was optional and the residents of India would not be forced to register. In 2013, the Supreme Court said that Aadhaar could not be cited as grounds for denial of any service. In 2015, the Supreme Court again echoed that Aadhaar could be used for six government schemes, as long as it was voluntary.

However, in 2017, the government made it mandatory to link Aadhaar to receive benefits under 252 welfare schemes. They also made Aadhaar mandatory for receiving private services such as getting a telephone connection or opening a bank account. Also, if this did not happen, there was a threat of disabling those bank accounts and mobile connections. The deadlines for linking these services was first set to December 2017, then extended to February 2018, and then to March 2018.

The mandatory use of Aadhaar slowly became ubiquitous. Passport renewals, board exam registrations, PAN cards and other government documents required Aadhaar linkage to be mandatory. In some cases, petitioners argued that HIV-positive patients were being denied treatment if they didn't have an Aadhaar number. There were other cases of disabled citizens getting scholarships and women rescued from sex trafficking seeking job training who also had to produce an Aadhaar number, which was in violation of an earlier Supreme Court ruling. In March 2018, the Supreme Court finally cancelled any mandatory linking of Aadhaar and indefinitely extended any previously announced deadlines, while the matter is under judicial consideration. This applied to all services and schemes, with the exception of state-run welfare schemes and subsidies. It asked the government: "How can you make the Aadhaar card mandatory, when we have passed an order to make it optional?"

Between June 2017 and March 2018, there was chaos regarding this issue. *Should Aahaar be linked to private services or should it not?* There were debates on how or what changed the nature of Aadhaar from optional to mandatory. Was this the right move on part of the government? And what options did citizens have? The government was compelling its residents to take up Aadhaar, and in a low-trust environment like India, such measures do not work well.

During the debate around Aadhaar's mandatory nature, the government was constantly revealing statistics of Aadhaar's success. For example, until October 2017, they said that around 500 million Indians had linked their Aadhaar numbers with telecoms operators. This led to a series of questions: if Aadhaar's take up was indeed successful, why was it being made mandatory? A bigger question was that, if Aadhaar was being envisioned as a subsidy and delivery medium, why were people being asked to link their numbers and bank accounts which are services provided by private entities? There were further concerns around security and privacy, including the question of who was accountable in cases of data breach.

The bigger problem was that poorer people, whom the scheme was supposed to help, were themselves losing out. Since 2016, after the passage of the Aadhaar Act, Aadhaar authentication was made mandatory to receive subsidies under certain government schemes. Two primary problems were associated with this: (a) seeding (the process by which Aadhaar numbers of residents are included in the service delivery database of the service providers); and (b) authentication.

The seeding problem occurs when the Aadhaar number has to be linked with the subsidy scheme. People are often unaware of how to do this, or go great lengths as the process can extend to several months. Until the link is in place, they do not receive the due benefits. This is claimed to have conributed to the death of an 11-year-old girl in Jharkhand whose family's ration card was cancelled as it wasn't linked to the Aadhaar, denying them food subsidies. The girl died due to starvation. This problem occurred many times, resulting in death in multiple cases.

The second problem is around authentication failures. Poor people who are dependent on subsidies went to the designated shops and authenticated themselves using their fingerprints, but the system rejected them incorrectly. There was no other way they could establish their identities because Aadhaar was made mandatory to receive subsidies. This meant that the poor were denied what they were entitled to. UIDAI has officially said that Aadhaar authentication failure rates are at 12% for government services (Sachdev, 2018). This is quite a jump from the 0.04% statistic given in 2012. At a national level, the failure rate for iris scan authentication is at 8.54%, while for fingerprint scans, it is 6%. At the level of individual states in India, UIDAI was unable to provide data on authentication failure rates.

In a presentation to the Supreme Court, UIDAI's CEO revealed that his authentication failure rate stood at 19.2% (five out of 26 attempts failed). The statistics around authentication failures seem small as a percentage, but considering that 1.2 billion people are enrolled in Aadhaar, even a 6% failure would mean a number of people equivalent to the population of many countries being denied subsidies that they are entitled to. It must also be noted that these authentication failure rates include impostors and it is difficult to tell how many of these were legitimate failures and how many were false negatives.

In April 2018, the Supreme Court made it amply clear that, "authentication failures do not mean exclusion or denial from subsidies, benefits or services since the Requesting Entities are obliged under the law to provide for exception handling mechanisms".

The combination of making Aadhaar mandatory and not providing alternatives for establishing identity worsened the situation of those it had actually set out to make better off. However, the issue has been realised and the judiciary has sided with the people, forcing the government to move forward on this issue constructively.

3.2.4. The 'Big Brother' problem

There is legitimate fear that the State will use Aadhaar data as a means to identify and single out individuals who are opposed to the norms of the State. The current government is perceived to be more authoritarian and so this issue has become more serious. The three issues outlined above highlight this idea. The absence of a data protection law, the misuse or leakage of individual data, and Aadhaar's mandatory status – combined with subverting the legislative process to pass the law – all compound the fear of the government wanting to potentially misuse Aadhaar data for its own ends. The absence of data protection regulation further exacerbates these concerns.

This position was tested in 2014 when a Goa court ordered UIDAI to share the biometric data of all of Goa's residents with the Central Bureau of Investigation in order to identify the perpetrators in a case involving a gang-rape of a 7-year old girl. UIDAI refused this and argued with the Bombay High Court and then the Supreme Court of India, saying that such a condition once fulfilled will lead to a slippery slope. Further, it compromises Indian citizens' right to privacy. The Supreme Court sided with UIDAI and the database wasn't shared. What the future holds is hard to tell but this precedent sends a strong message about protecting the privacy of Indian residents.

4. Conclusion: Analog is as important as digital

There is overwhelming evidence that digital systems strengthen governance structures, primarily by furthering service delivery mechanisms. Aadhaar's birth was based on the same promise of improving targeting and efficiency for subsidy transfers in India. There isn't a definitive answer to whether Aadhaar is a success or a failure. Instead, Aadhaar should be looked at as a work in progress: it has some things right, some horribly wrong, and others where there is room for improvement. But, the question is: *Would no Aadhaar be more desirable than Aadhaar in its current form?* While there is no simple answer to this question, if we broadly break down Aadhaar's 'digital' and 'analog' components, it may shed more light and outline key lessons for the 'transition phase' of digital ID systems – from initial instigation to achieving a high degree of enrolment and finally to seamless usage and delivery of services, the last of which Aadhaar still needs to accomplish.

The digital components are the backbone of the ID system because the primary goal is identification of an individual. If the system can correctly verify that I am who I claim to be, then it is a success. While Aadhaar does well for most part, it does fail sometimes. At this point, however, it is hard to tell unambiguously whether Aadhaar has done well or not. But, it is important to note two primary lessons from the institutional mechanisms around digital components. The first is that the composition of the team is crucial in building an ID system such as Aadhaar. As noted, the team should be diverse with domain-specific competency. The traditional tendency to see a distinction between government and private sector needs to be avoided. While the private sector brings with it knowledge around processes, technology and safeguards, the public sector has the skills to navigate the complex government maze where often one single word can change the nature of policy for years to come. The second is the quality checks and institutional processes that are put in place. Enlisting external agencies to do the work increased speed of enrolment and introduced inclusivity. The process of encrypting and decrypting the data was also important. The technological processes were robust in catching any errors and the team was agile in fixing them. Thus, Aadhaar fares well on the backend processes and its functioning.

However, Aadhaar's analog components took longer to evolve and meet the project's needs. There were two important elements that Aadhaar got right: the first is timing, and the second is securing the necessary political backing.

Timing is crucial to any political process. All governments have a limited time frame to act on an idea and make it happen before it is subsumed by other problems. All background work, planning, processes should be in place before it becomes politically viable to launch such a programme. There is no merit in waiting for the window of opportunity to begin planning the evolution of such a project. As early as 2010, UIDAI had identified that Aadhaar needed legislative backing. They also pre-empted questions around data privacy and security from the public. It took six years before Aadhaar had any legislative process and a couple more for the debate around data privacy to get serious. At the time of writing this report, in June 2018, 1.2 billion people have already been enrolled, a data regulator is still being talked about, and a draft law is yet to be finalised. While this may not be the ideal outcome, if UIDAI had waited for a draft law, Aadhaar may not have 1.2 billion people on its roll. The counterfactuals are hard to imagine and it is further difficult to pass a value judgement on them, but the central lesson stands – if there is a window of opportunity to make the change and the project can't be rallied, then it might take a long time for it to gain traction in the future.

Political backing is also essential. The political establishment needs to be invested in the idea to bring about reform from the ground up. Incentives need to be aligned to the process to prevent any Principal-Agent mismatches. In Aadhaar's case, Nandan Nilekani had a meeting with the President and the Prime Minister who, despite facing challenges and backlash from within the government and political parties, made a great effort to back Aadhaar. A separate empowered group of ministers was constituted to legitimise Aadhaar against its opponents. After the 2014 general elections, the previous opposition party became incumbent as the single largest party in India. They too backed Aadhaar when in government, despite opposing it earlier. Without political legitimacy, it is difficult to instigate reform. Thus, gaining buy-in from the political class is crucial to the success of such reforms.

There were other analogue components where Aadhaar could have performed better. The passing of a Data Protection Act or the establishment of a data protection regulator was not achieved on time. This was important for getting procedures right and to have the necessary grievance redress mechanisms in place, and also to maintain the faith of the citizens of India in the project. Legal systems are the balancing mechanisms as they form one-third of the legislative, executive, judiciary triad in India. The absence of one certainly tips the scales of power in the favour of the others, leading to a loss of public trust. The passing of Aadhaar as a money bill and the ad-hoc decision to make Aadhaar mandatory added fuel to the fire. Governments should be wary of this. It is important to follow due process and not subvert the rule of law to gain a favourable policy outcome, let alone for a substantial game-changer such as this one. A sound legal basis is important to keep projects like Aadhaar afloat, especially in low-trust environments such as India.

Another important lesson would be to have valid identification mechanisms in case the new one fails. It is expected that technology will take its time and improve its functioning; while that transition phase is being realised, public services should not be affected. This is especially the case for services that are aimed at poorer people who fundamentally depend on these subsidy transfers for their lives. Therefore, it is critical that there is a timeline of a gradual phase-out and takeover of the new identity mechanism.

Aadhaar has added tremendous value to the lives of Indians, yet in many cases it has taken a lot away from them too. While some would say that this is not Aadhaar's fault, it does fall on incumbent authorities to think through the whole process of enrolment, authentication and service delivery and leave room to make changes and plug any gaps as needed.

References

1. Abraham, R., & Dubey, S. (2018). 'Did Aadhaar really save Rs. 57,000 crores? Simply put, no.' | State of Aadhaar. Retrieved from https://stateofaadhaar.in/did-aadhaar-really-save-rs-57000-crores-simply-put-no/

2. Abraham, R., Bennett, E., Bhusal, R., Dubey, S., Li, Q., Pattanayak, A., & Shah, N. (2018). State of Aadhaar Report 2017-18 [Ebook]. IDInsight. Retrieved from https://stateofaadhaar.in/wp-content/uploads/State-of-Aadhaar-Report_2017-18.pdf

3. Abraham, R., Bennett, E., Sen, N., & Shah, N. (2017). State of Aadhaar Report 2016-17 [Ebook]. IDInsight. Retrieved from https://stateofaadhaar.in/wp-content/uploads/State-of-Aadhaar-Full-Report-2016-17-IDinsight.pdf

4. Abraham, R., & Pattanayak, A. (2018). 'Clearing the air on Aadhaar data breach'. Retrieved from https://www.livemint.com/Opinion/MUPJK28VMeoICzl1whSBrJ/Clearing-the-air-on-Aadhaar-data-breach.html

5. AccessNow. (2018). National Digital Identity Programmes: What's Next? [Ebook]. Retrieved from https://www.accessnow.org/cms/assets/uploads/2018/03/Digital-Identity-Paper-digital-version-Mar20.pdf

6. Aiyar, S. (2017). Aadhaar: A Biometric History of India's 12-Digit Revolution. Westland.

7. Bhakta, P. (2018). 'Aadhaar enabled payments double to 13.7M in March'. Retrieved from https://tech.economictimes.indiatimes.com/news/mobile/aadhaar-enabled-payments-double-to-13-7m-in-march/63874951

8. Bhushan, K. (2018). 'Know the man behind Elliot Alderson, who exposed flaws in Aadhaar, OnePlus & Paytm'. Retrieved from https://www.hindustantimes.com/tech/know-the-man-behind-elliot-alderson-who-exposed-flaws-in-aadhaar-oneplus-paytm/story-v2fC1MhdpScxYq6VkmzPzN.html

9. Business Today (2017). 'Supreme Court extends Aadhaar linking deadline: Here's a five-year timeline'. Retrieved from https://www.businesstoday.in/current/economy-politics/aadhaar-linking-deadline-supreme-court-timeline-pan-card-bank-account/story/266066.html

10. Business Today (2018). 'India accounts for 55% of new bank accounts opened globally: World Bank'. Retrieved from https://www.businesstoday.in/current/economy-politics/india-accounts-for-55-per-cent-of-new-bank-accounts-opened-globally-world-bank/story/275348.html

11. Chari, M., Yadav, A., & Chowdhury, S. (2017). 'Not just mid-day meals: Aadhaar made mandatory for 11 more schemes, violating Supreme Court ruling'. Retrieved from https://scroll.in/article/830946/not-just-mid-day-meals-aadhaar-made-mandatory-for-11-more-schemes-violating-supreme-court-ruling

12. Dahan, M. (2015). 'Digital IDs: A powerful platform for enhanced service delivery across all sectors'. Retrieved from https://blogs.worldbank.org/ic4d/digital-ids-powerful-platform-enhanced-service-delivery-across-all-sectors

13. Deccan Chronicle (2017). 'We said Aadhaar is optional, how can you make it compulsory: SC to Govt'. Retrieved from https://www.deccanchronicle.com/nation/current-affairs/210417/how-can-you-make-aadhaar-compulsory-when-we-said-its-optional-sc-to-govt.html

14. Deepalakshmi, K. (2017). 'The long list of Aadhaar-linked schemes'. Retrieved from https://www.thehindu.com/news/national/the-long-list-of-aadhaar-linked-schemes/article17641068.ece

15. Deloitte (2016). Picture Perfect: A Blueprint for Digital Identity [Ebook]. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/gx-fsi-digital-identity-online.pdf

16. Divan, S. (2014). 'The Aadhaar trap: Why you should be really, really worried'. Retrieved from https://www.firstpost.com/business/economy/you-should-be-worried-with-aadhaar-you-are-at-govts-mercy-1315823.html

17. Drèze, J. & Khera, R (2018). 'Aadhaar's $11-bn question: The numbers being touted by govt have no solid basis'. Retrieved from https://economictimes.indiatimes.com/news/economy/policy/aadhaars-11-bn-question-the-numbers-being-touted-by-govt-have-no-solid-basis/articleshow/62830705.cms

18. Economic Times (2017). 'Government saved Rs 57,000 crore through DBT scheme, says Ravi Shankar Prasad'. Retrieved from https://economictimes.indiatimes.com/industry/banking/finance/government-saved-rs-57000-crore-through-dbt-scheme-says-ravi-shankar-prasad/articleshow/60530667.cms

19. Economic Times (2018a). 'Aadhaar-enabled DBT savings estimated over Rs 90,000 crore'. Retrieved from https://economictimes.indiatimes.com/news/economy/finance/aadhaar-enabled-dbt-savings-estimated-over-rs-90000-crore/articleshow/64949101.cms

20. Economic Times (2018b). 'Number of adult Indians with bank accounts rises to 80%'. Retrieved from https://economictimes.indiatimes.com/industry/banking/finance/banking/number-of-adult-indians-with-bank-accounts-rises-to-80/articleshow/63838930.cms

21. Financial Express (2018a). '80% adult Indians now have bank accounts, thanks to Aadhaar, Jan Dhan Yojna, says World Bank'. Retrieved from https://www.financialexpress.com/economy/80-adult-indians-now-have-bank-accounts-thanks-to-aadhaar-jan-dhan-yojna-says-world-bank/1140545/

22. Financial Express (2018b). 'Can't provide state-level authentication failure rates: UIDAI'. Retrieved from https://www.financialexpress.com/aadhar-card/cant-provide-state-level-authentication-failure-rates-uidai/1120573/

23. Financial Express (2018c). 'SC hearing: Government told to justify passing of Aadhaar Act as money Bill.' Retrieved from https://www.financialexpress.com/economy/sc-hearing-government-told-to-justify-passing-of-aadhaar-act-as-money-bill/1153754/

24. Firstpost (2017). 'Aadhar data collection by private agencies not good idea, says Supreme Court'. Retrieved from https://www.firstpost.com/india/aadhar-data-collection-by-private-agencies-not-good-idea-says-supreme-court-3189590.html

25. Gelb, A., & Metz, A. (2017). Identification Revolution: Can Digital ID Be Harnessed for Development? [Ebook]. Centre for Global Development. Retrieved from https://www.cgdev.org/sites/default/files/identification-revolution-can-digital-id-be-harnessed-development-brief.pdf

26. Gopakumar, G. (2017). 'UIDAI eases norms on enrolment centres after bankers' opposition'. Retrieved from https://www.livemint.com/Industry/YrKhcSpN8rjKfgoG23B2RL/UIDAI-eases-norms-on-enrolment-centres-after-bankers-opposi.html

27. India Today (2017). 'Aadhaar now mandatory for bank accounts, link it by Dec 31 or lose access to banking'. Retrieved from https://www.indiatoday.in/technology/news/story/aadhaar-made-mandatory-for-bank-accounts-existing-accounts-will-be-invalid-without-aadhar-linking-983116-2017-06-16

28. Indian Express (2015). 'Man makes Aadhar card for dog 'Tommy Singh', arrested'. Retrieved from https://indianexpress.com/article/trending/man-arrested-for-getting-aadhar-card-made-for-dog/

29. Jain, M. (2018). 'Universe's strength needed to break Aadhaar encryption: UIDAI CEO to SC'. Retrieved from https://www.business-standard.com/article/current-affairs/universe-s-strength-needed-to-break-aadhaar-encryption-uidai-ceo-to-sc-118032200794_1.html

30. Jean, D., Khalid, N., Reetika, K., & Anmol, S. (2017). 'Aadhaar and Food Security in Jharkhand', Economic & Political Weekly, LII (50), 50-60.

31. Johari, A. (2017). 'Denied food because she did not have Aadhaar-linked ration card, Jharkhand girl dies of starvation'. Retrieved from https://scroll.in/article/854225/denied-food-because-she-did-not-have-aadhaar-linked-ration-card-jharkhand-girl-dies-of-starvation

32. Johari, A. (2018). 'Yet another Aadhaar-linked death? Denied rations for 4 months, Jharkhand woman dies of hunger'. Retrieved from https://scroll.in/article/867352/yet-another-aadhaar-linked-death-jharkhand-woman-dies-of-hunger-after-denial-of-rations

33. Khaira, R. (2018). 'Rs 500, 10 minutes, and you have access to billion Aadhaar details'. Retrieved from http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html

34. Khera, R. (2017a). 'Impact of Aadhaar on Welfare Programmes'. Economic & Political Weekly, LII (50), 61-70.

35. Khera, R. (2017b). 'The Different Ways in Which Aadhaar Infringes on Privacy'. Retrieved from https://thewire.in/featured/privacy-aadhaar-supreme-court

36. Khera, R. (2017c). 'Opinion: It is time for judiciary to call out the Indian government's lie on 'voluntary Aadhaar''. Retrieved from https://scroll.in/article/860572/opinion-why-it-is-time-for-judiciary-to-call-out-the-indian-states-lie-on-voluntary-aadhaar

37. Madanapalle, A. (2017). 'How Aadhaar compares to other biometric national identification systems around the world'. Technology News, Firstpost. Retrieved from https://www.firstpost.com/tech/news-analysis/how-aadhaar-compares-to-other-biometric-national-identification-systems-around-the-world-3700543.html

38. Madhavan, M. (2016). 'The power to certify'. Retrieved from http://www.thehindu.com/opinion/op-ed/aadhar-bill-the-power-tocertify/article8604009.ece

39. Manzar, O. (2018). 'The questionable foundation of Aadhaar'. Retrieved from https://www.livemint.com/Opinion/N4giOeHMkcl5QiK6VGTpAL/The-questionable-foundation-of-Aadhaar.html

40. Medianama (2018a). 'A continuously updated list of all Aadhaar data leaks'. Retrieved from https://www.medianama.com/2018/05/223-aadhaar-leaks-list/

41. Medianama (2018b). French security researcher reveals series of security issues in Indian sites. Retrieved from https://www.medianama.com/2018/03/223-french-security-researcher-reveals-series-of-security-issues-in-indian-sites/

42. Ministry of Electronics and IT, Government of India. (2017). Key Achievements: 2017. Retrieved from http://pib.nic.in/PressReleaseIframePage.aspx?PRID=1514598

43. Mittal, P. (2018a). 'Aadhaar authentication failure doesn't mean denial of benefits, UIDAI tells SC'. Retrieved from https://www.livemint.com/Politics/the2brDHqCcWztKlpLLeuK/Aadhaar-authentication-failure-doesnt-mean-denial-of-benefi.html

44. Mittal, P. (2018b). 'SC upholds constitutional validity of Aadhaar, strikes down certain provisions.' Retrieved from https://www.livemint.com/Politics/eUH1dl06ly9otiDHqGNCfM/Aadhaar-verdict-Supreme-Court-upholds-constitutional-validi.html

45. Nambiar, N. (2018). 'People protest after denial of ration over Aadhaar seeding'. Retrieved from https://timesofindia.indiatimes.com/city/pune/people-protest-after-denial-of-ration-over-aadhaar-seeding/articleshow/63765943.cms

46. National Institute of Public Finance and Policy. (2012). A cost-benefit analysis of Aadhaar. Retrieved from http://planningcommission.nic.in/reports/genrep/rep_uid_cba_paper.pdf

47. NDTV (2017a). 'After 100 Farmers Found With Same Aadhaar, Devendra Fadnavis Steps In'. Retrieved from https://www.ndtv.com/india-news/after-100-farmers-found-with-same-aadhaar-devendra-fadnavis-steps-in-1766839

48. NDTV (2017b). ''You Cleared Aadhaar For 6 Schemes, Centre Made It 139': Court Told'. Retrieved from https://www.ndtv.com/india-news/you-cleared-aadhaar-for-6-schemes-centre-made-it-139-supreme-court-told-1787744

49. Nilekani, N., & Shah, V. (2015). Rebooting India: Realizing a Billion Aspirations. Penguin Random House India.

50. Nilekani, N. (2017). 'Building On Aadhaar'. Retrieved from https://indianexpress.com/article/opinion/columns/building-on-aadhaar-4692193/

51. Peermohamed, A. (2017). 'Justice K S Puttaswamy: The 92-yr-old who fired the 1st shot in privacy war'. Retrieved from https://www.business-standard.com/article/current-affairs/justice-k-s-puttaswamy-the-92-yr-old-who-fired-the-1st-shot-in-privacy-war-117082401108_1.html

52. PricewaterhouseCoopers. (2018). An overview of the changing data privacy landscape in India [Ebook]. Retrieved from https://www.pwc.in/assets/pdfs/publications/2018/an-overview-of-the-changing-data-privacy-landscape-in-india.pdf

53. The Quint (2017). 'Aadhaar Is Optional, How Can You Make It Mandatory? SC Blasts Govt'. Retrieved from https://www.thequint.com/news/india/aadhaar-card-mandatory-supreme-court-questions-government

54. Radhakrishnan, S. (2016). 'Is the Aadhaar Bill a Money Bill?'. Retrieved from https://www.thehindu.com/news/national/is-the-aadhaar-bill-a-money-bill/article14311812.ece

55. Rajagopal, K. (2018). 'SC questions government's justification for passing Aadhaar Act as Money Bill'. Retrieved from http://www.thehindu.com/news/national/sc-questions-governments-justification-for-passing-aadhaar-act-as-money-bill/article23749005.ece

56. Rao, P. (2015). 'Explainer: The rights and wrongs of using Money Bills to bypass the Rajya Sabha'. Retrieved from https://scroll.in/article/777862/explainer-the-rights-and-wrongs-of-using-money-bills-to-bypass-the-rajya-sabha

57. Rautray, S. (2018). 'Aadhaar linking extended indefinitely, SC says govt can't insist Aadhaar till the matter is subjudice'. Retrieved from https://economictimes.indiatimes.com/news/politics-and-nation/sc-indefinitely-extends-march-31-deadline-for-mandatory-aadhaar-linking/articleshow/63284996.cms

58. Regidi, A. (2018). 'The passing of Aadhaar as a Money Bill and its immunity from judicial review needs a thorough re-examination by the Supreme Court'. Firstpost. Retrieved from https://www.firstpost.com/india/the-passing-of-aadhaar-as-a-money-bill-and-its-immunity-from-judicial-review-needs-a-thorough-re-examination-by-the-supreme-court-4460247.html

59. Sachdev, V. (2018). 'Aadhaar Authentication for Govt Services Fails 12% of Time: UIDAI'. Retrieved from https://www.thequint.com/news/india/uidai-ceo-admits-aadhaar-authentication-failure-rate-12

60. Sekhose, M. (2018). 'How to send money to any UPI ID via WhatsApp payments feature'. Retrieved from https://www.hindustantimes.com/tech/how-to-send-money-to-any-upi-id-via-whatsapp-payments-feature/story-T2pjmdhC7yvqxk9N4YPcsL.html

61. Sharma, M., Giri, A., & Chadha, S. (2017). Aadhaar as a payment infrastructure: current implementation and challenges [Ebook]. Retrieved from https://stateofaadhaar.in/wp-content/uploads/Aadhaar_as_a_payment_infrastructure.pdf

62. Srinivas, A. (2018). 'Aadhaar row: UIDAI snaps ties with enrolment agency; millions at risk'. Retrieved from https://www.business-standard.com/article/economy-policy/aadhaar-row-uidai-snaps-ties-with-enrolment-agency-millions-at-risk-118021001206_1.html

63. Srivastava, P. (2018). 'Jean Dreze Exclusive: 'MGNREGA workers have become guinea-pigs for Aadhaar Payments System''. Retrieved from https://www.financialexpress.com/economy/jean-dreze-exclusive-mgnrega-workers-have-become-guinea-pigs-for-aadhaar-payments-system/1246759/

64. Unique Identification Authority of India (UIDAI), Planning Commission, Government of India. (2010). UIDAI Strategy Overview [Ebook]. Retrieved from http://www.prsindia.org/uploads/media/UID/UIDAI%20STRATEGY%20OVERVIEW.pdf

65. Unique Identification Authority of India (UIDAI) (2012). Working with Biometric Devices and Data Quality. Retrieved from http://www.nictcsc.com/images/Aadhaar%20Project%20Training%20Module/English%20Training%20Module/module4_working_with_biometric_devices_and_data_quality_17122012.pdf

66. Unique Identification Authority of India (UIDAI) (n.d.), Aadhaar Dashboard. Retrieved from https://www.uidai.gov.in/aadhaar_dashboard/

67. Unique Identification Authority of India (UIDAI) (2019). 'Registrars'. Retrieved from https://uidai.gov.in/enrolment-update/ecosystem-partners/registrars.html

68. USAID (2017). Identity in a Digital Age: Infrastructure for Inclusive Development [Ebook]. Retrieved from https://www.usaid.gov/sites/default/files/documents/15396/IDENTITY_IN_A_DIGITAL_AGE.pdf

69. World Bank. (2016). World Development Report 2016: Digital Dividends Retrieved from http://www.worldbank.org/en/publication/wdr2016

70. World Bank (n.d.). Brief on Digital Identity [Ebook]. Retrieved from http://pubdocs.worldbank.org/en/413731434485267151/BriefonDigitalIdentity.pdf

71. Yadav, U. (2017a). 'Aadhaar enrolment by private operators stopped all over Karnataka'. Retrieved from https://tech.economictimes.indiatimes.com/news/technology/aadhaar-enrolment-by-private-operators-stopped-all-over-karnataka/59521753

72. Yadav, A. (2017b). 'It isn't just Dhoni: UIDAI received 1,390 complaints about Aadhaar agents – but took no legal action'. Retrieved from https://scroll.in/article/826089/it-isnt-just-dhoni-uidai-received-1390-complaints-about-aadhaar-agents-but-took-no-legal-action

Pathways
for Prosperity
Commission
Technology &
Inclusive Development