CASE STUDY

Aadhaar – India

Aadhaar – meaning "foundation" in several Indian languages – is the largest biometric identity programme in the world. Since its launch in 2009, Aadhaar has enrolled nearly 1.2 billion Indian citizens and residents (about 15% of the global population), including over 99% of all Indian adults. Each Aadhaar recipient receives a unique 12-digit ID number, and submits their photo and their biometric data in the form of fingerprints and iris scans. Originally designed to help mitigate fraud, waste and abuse in social benefit programmes by ensuring benefits went to the right person, the initiative has grown to encompass many parts of everyday life in India, such as bank transactions and activating a mobile phone. Use of Aadhaar is mandatory for a growing number of these programmes. As the programme has grown, so has the controversy surrounding it, including a landmark November 2017 Indian Supreme Court ruling that for the first time recognised privacy as a fundamental human right, which may have implications for the future of Aadhaar. As far as digital identities are concerned, all eyes are on India.

THE PROBLEM

India had major problems in identifying beneficiaries for social programmes. A significant proportion of residents lacked formal identity credentials, and many of those who had credentials possessed ones that were only recognised locally. Inadequate identity records and verification processes meant that government agencies frequently distributed social welfare benefits to the same people multiple times, or to people who did not qualify. Prior to Aadhaar, it was estimated that 58% of subsidised food grains and 38% of subsidised kerosene disbursed under government programmes did not reach their intended beneficiaries (Government of India, 2005). This resulted in tremendous waste of resources. Such issues also affected other social programmes including scholarships, healthcare, pensions and subsidised household goods. Significantly, some eligible households were denied social assistance for which they qualified because they could not easily prove their identity.

AN INNOVATIVE SOLUTION

To overcome these problems, the Indian government launched Aadhaar – an ambitious programme intended to provide every man, woman and child living in India with a unique digital identity based on their biometric information (thumbprints and iris scans). Unique identification through this biometric information makes it simpler for authorities to verify that subsidised goods are delivered to the right recipients and limits the scope of fraudulent activities.

The initial target of Aadhaar was the country's Public Distribution System (PDS), a government-subsidised programme designed to enhance food security and serve as a safety net for the 330 million Indians who are nutritionally at risk. The food is distributed at over 500 000 "fair price shops", making it the largest distribution network of its type in the world. The primary challenge for the government has been widespread pilferage and diversion of food grains meant for low-income beneficiaries. Prior to the introduction of Aadhaar, pilferage could occur in a number of ways:

- Sales records were manually recorded, making it impossible to know whether a sale actually took place, whether food was fraudulently diverted by FPS staff, or whether the staff overcharged for provisions.
- Individuals would secure bogus rations cards by creating fictitious families.
- Individuals would use genuine rations cards stolen or purchased from someone else.

By enabling end-to-end digitisation of distribution and sales processes, Aadhaar helps eliminate these issues. Diversion during transport and delivery to fair price shops is mitigated through Aadhaar-enabled automatic weighing of the rations, which is tied directly to the current handler's Aadhaar identity.[42] If the weight is not accurate, the transfer of goods cannot take place and the identity of the handler is known. To mitigate abuse at the beneficiary end, each fair price shop is equipped with digital point-of-sale devices used by shop employees to authenticate beneficiaries using their fingerprints or iris scans (see Figure 13). The device links to the Aadhaar database via a mobile, Wi-Fi or cabled internet connection, and then verifies the beneficiary's identity and eligibility. When payment is required, the benefits are paid for using cashless payments through Aadhaar, so no money physically changes hands, which prevents overcharging of customers. The rations are also weighed to ensure the appropriate amount is given to the beneficiary (see Figure 14). A shop is unable to dispense benefits to individuals who are not eligible or who have already received their ration, or if the weight is incorrect. In some states, disabled beneficiaries are authenticated and the rations provided directly to the home, while in other states, a relative or neighbour can be designated to collect the rations. Finally, Aadhaar has made the process more efficient by allowing the government to determine the inventories of each FPS in real-time, so they can replenish just the right amount of inventory when required. This mitigates the possibility of shops operating black markets using excess stock, as was frequently the case in the past.

In addition to reducing fraud in PDS, Aadhaar's streamlined and automated system means that beneficiaries:

- Receive SMS messages to alert them to the existence of new supplies, rather than having to physically check the shop repeatedly.
- Can view a map of all stores and their current inventory level via a mobile app.
- Authenticate their identity instantly to collect their benefits, reducing in-store wait times from half a day to a matter of minutes.

42. When supplies change hands from one person to another (e.g. when a deliverer drops off supplies at a fair price shop), both the deliverer and recipient must authenticate simultaneously to validate the transaction, which also involves an automated weighting. This ensures clear lines of accountability without the potential for either party to divert supplies.

Figure 13: **Obtaining rice using fingerprints**

Figure 14: **Weighing rice at a fair price shop**

- Select the shop where they prefer to receive their benefits. A central database manages the benefits and permits authentication of a beneficiary at any location, thereby promoting choice and mobility.

In addition to social services such as PDS, Aadhaar also now encompasses over 3 500 government and non-government services in India, ranging from opening bank accounts to making digital payments, enrolling in school, activating a mobile phone, receiving pension payments, filing taxes, voting and making e-signatures.[43,44] The government has also launched DigiLocker,[45] a platform for issuing, sharing and verifying documents and certificates, in an effort to move towards a paperless society.

Government officials believe that the full potential of Aadhaar is not yet apparent,[46] and that the next wave of innovation will come from the private sector with businesses using Aadhaar as a platform. The system includes an open application programming interface (API), which allows the programme to serve as a platform for private sector companies to build services using Aadhaar identity management as a foundation, which has the potential to enable a whole ecosystem of apps. For example, Google's Tez app allows people to send instant digital payments to friends, relatives and businesses. Tez gained 7.5 million users in its first five weeks, drastically increasing the number of Aadhaar transactions (see Figure 15) (Pahwa, 2017). Given the open nature of its interface, the architect of Aadhaar believes that in the future people will use Aadhaar in ways that are unimaginable today (Mirchandani, 2017).

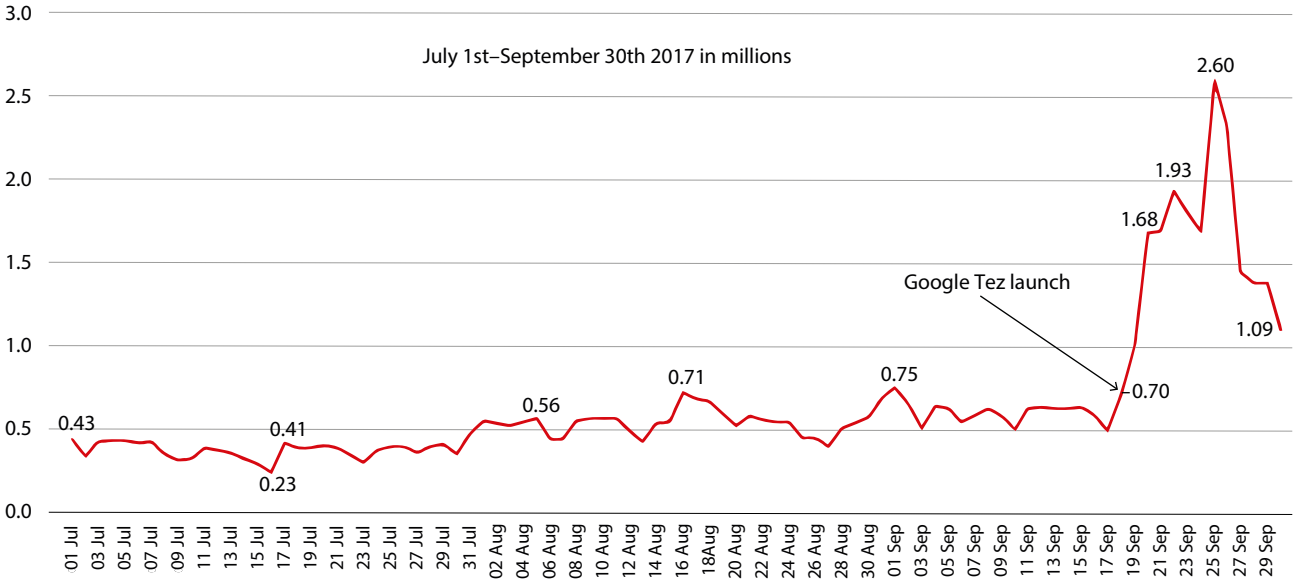
43. See https://economictimes.indiatimes.com/tdmc/your-money/7-benefits-of-aadhaar-card/tomorrowmakersshow/58412087.cms.

44. See http://etaal.gov.in/etaal/auth/Login.aspx.

45. See https://digilocker.gov.in.

46. Interviews with J. Sathyanarayana, Indian Administrative Service (IAS), Chairman of the Unique Identification Authority of India (UIDAI) and Advisor to the Chief Minister of Andhra Pradesh, and Ajay Sawhney, IAS, Secretary to the Government of India for the Ministry of Electronics and Information Technology, 12 December 2017.

Figure 15: **Count of Aadhaar transactions**



Source: National Payments Corporation of India (NPCI) via Reserve Bank of India (RBI); Pahwa (2017).

Undoubtedly, Aadhaar has been as controversial as it has been innovative. As more services become integrated through Aadhaar, it becomes possible to piece together data to create a detailed profile of an individual. Over time, such profiles could even be used to predict future behaviours in ways impossible with traditional methods of identity. Privacy advocates argue that this can limit social mobility, as people could be trapped by their class, past actions or any associated stigma. Some also argue this could constitute a step towards a surveillance state, or misuse by the private sector, as businesses continue to enable Aadhaar authentication on their services (Kolachalam, 2017). Some also raise security concerns about the potential for privacy leaks or hacks of the Aadhaar database, which could potentially result in fraudulent use of an individual's identity. This concern is not without merit, as sensitive Aadhaar data have already been breached on several occasions. In July 2017, the names, addresses, Aadhaar numbers and bank account details of 1.4 million pensioners were accidentally leaked by a state Social Security office (Sethi, Bansal and Roy, 2017). Most recently, Indian newspaper The Tribune reported that they were able to purchase access to Aadhaar details for every registered Aadhaar number – including names, addresses, postal codes, phone numbers and email addresses (but not biometrics) – from anonymous sellers on WhatsApp. The transaction took 10 minutes and cost EUR 7. For an additional EUR 4, the newspaper was able to obtain software that would allow them to print their own Aadhaar cards with the obtained information (Khaira, 2018). The source of the stolen information was one of tens of thousands of private Aadhaar registration providers licensed to process new Aadhaar registrations, who thus had access to the Aadhaar database (*The Economist,* 2018). The government responded by giving users the ability to generate and use virtual IDs instead of their Aadhaar number. This extra layer of privacy can help mask the identities of users even if their data is compromised (Singhl, 2018). They also restricted the number of Aadhaar registration providers with access to the Aadhaar database (*The Economist,* 2018). However, it is too early to determine the extent to which these actions will address security concerns.

In interviews with the OECD, senior officials in the Indian government countered privacy and security concerns, stating that Aadhaar data operations are founded on three core principles:

1. ***Minimal data:*** the government collects only the data needed to prove identity. Other information, such as race, religion, education and profession, are not collected.

2. ***Optimal ignorance:*** although the Aadhaar database authenticates individuals, no data are sent to the government regarding the usage of the Aadhaar account. This limits the ability of the government to accumulate data on an individual's habits. In addition, no information from the Aadhaar database is shared

with a service provider. The Aadhaar system only provides the servicer with a yes or no (authenticated or not). Finally, by law, anyone who collects Aadhaar data is mandated to use them only for the purpose for which they are needed. Even if a large business has many different Aadhaar-enabled services, they cannot share Aadhaar data among themselves without the consent of the identity holder.

3. ***Federated databases:*** all services that use Aadhaar (e.g. PDS, scholarships, pensions, businesses) maintain their own database containing the data of relevance to them. This lack of centralisation protects privacy by helping to prevent data from multiple sources being combined to enable profiling. It also protects security, as there is no central knowledge base, and thus no central host for attacks or leaks.[47] In addition, informed consent by the Aadhaar identity owner is required for one service to share information with another.

Officials further stated that the need for physical biometrics to authenticate a user largely precludes the possibility of fraudulent transactions in the event of a data breach. To further mitigate privacy and security risks, the government has assembled a data protection committee comprising privacy and security experts, headed by a former member of the Supreme Court. This committee can make recommendations on policy and legislation to ensure the protection of privacy and security going forward. One of their first acts was to develop a data protection framework, which is currently in draft form.[48] Government leaders expect the framework to be launched in the first half of 2018.[49]

In spite of the above core principles, the controversies surrounding Aadhaar have played out in the Indian judicial system. In August 2017, in response to a case brought about by a series of petitions by privacy advocates challenging the constitutionality of Aadhaar, the Indian Supreme Court unanimously issued a landmark ruling that the constitution of India provides that all Indians have a fundamental right to privacy (see Box 6). In so doing, the court overruled two previous rulings.[50] While this judgement has set a major new precedent for Indian society, it makes no formal ruling on whether Aadhaar violates privacy. However, it clears the way for a future court hearing to proceed, using this new precedent as an argument (Mirchandani, 2017).[51] According to the Aadhaar CEO,[52] and the original architect of Aadhaar (Mirchandani, 2017), this should have no bearing on the programme, as the system is premised on the belief that there is a right to privacy and is said to collect minimal data. The ruling also provides that, under certain instances, such as social welfare and public safety, the government can circumscribe this right, although this would need to be tested on a case-by-case basis. It is not clear what the ruling could mean for the future of Aadhaar, but numerous parties, from proponents of biometric and national identities to privacy advocates, are watching closely.

Box 6: SUPREME COURT RULING ON THE RIGHT TO PRIVACY

"The right to privacy is an element of human dignity. The sanctity of privacy lies in its functional relationship with dignity. Privacy ensures that a human being can lead a life of dignity by securing the inner recesses of the human personality from unwanted intrusion. Privacy recognises the autonomy of the individual and the right of every person to make essential choices which affect the course of life. In doing so privacy recognises that living a life of dignity is essential for a human being to fulfil the liberties and freedoms which are the cornerstone of the Constitution."

Source: www.countercurrents.org/2017/08/24/right-to-privacy-judgement-highlights-and-full-judgement.

NOVELTY

Aadhaar is the largest identity programme ever created and has resulted in the biggest repository of biometric data in existence. The scale of its current system and the potential for its use as a platform is unprecedented.

RESULTS AND IMPACT

In just a few years, Aadhaar has given almost 1.2 billion Indians a nationally recognised identity that unlocks a wide variety of government and private sector services.

47. Interview with Ajay Bhushan Pandey, CEO of the Unique Identification Authority of India (UIDAI) and Secretary for IT, 11 December 2017.

48. See http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf.

49. Interviews with J. Sathyanarayana, Indian Administrative Service (IAS), Chairman of the Unique Identification Authority of India (UIDAI) and Advisor to the Chief Minister of Andhra Pradesh, and Ajay Sawhney, IAS, Secretary to the Government of India for the Ministry of Electronics and Information Technology, 12 December 2017.

50. See http://indianexpress.com/article/india/right-to-privacy-judgment-a-fundamental-right-here-are-the-two-judgments-supreme-court-overruled-4811117/ for information on the two previous rulings.

51. See https://thewire.in/170700/right-to-privacy-aadhaar-supreme-court.

52. Interview with Ajay Bhushan Pandey, CEO of the Unique Identification Authority of India (UIDAI), 11 December 2017.

Connection of services to Aadhaar is completely changing sectors across India. Over USD 12 billion in financial transactions have taken place (Mirchandani, 2017), and over a billion bank accounts and mobile phones have been linked to Aadhaar.[53]

Aadhaar has also simplified and made more efficient many processes, resulting in better services for citizens and residents and significant cost-savings for the government. By mitigating fraud and abuse, the initiative has saved the government an estimated USD 10 billion over the last 2.5 years, according to the Aadhaar CEO.[54] Pilferage of food benefits, for example, has been drastically reduced.[55]

New data also show that Aadhaar has promoted financial inclusiveness and gender equity. The Centre for Global Development conducted a survey of Aadhaar users in the state of Rajasthan to learn more about their experience (Gelb et al., 2017).[56] It found that nearly all households now have at least one bank account, and a significant proportion of them are held by women. Before the introduction of Aadhaar, only 44% of women had bank accounts; this proportion has now grown to 90%. It also found that women tend to do the most banking for the family.

Aadhaar has fundamentally changed bargaining power from supplier to consumer, according to Nandan Nilekani, the original architect of Aadhaar and the cofounder of the major tech company InfoSys (Mirchandani, 2017). For PDS alone, customer wait times have fallen from hours to minutes. Enhanced mobility allows customers to receive their rations at any shop they like. If a shop provides bad service, keeps irregular hours or tries to scam customers (e.g. overcharging or putting stones in the rice to manipulate weighing), customers have the ability to vote with their feet and go instead to another of the many shops. The government tracks usage data and shuts down underperforming shops, thus providing them with an incentive for good customer service.

The function and functionality of Aadhaar has had a perceptible influence on citizens' trust in their government and each other, according to Aadhaar government officials. Receiving their payments and benefits on time and knowing that the government is protecting them against corruption and diversion helps to increase citizens' trust in government (Mirchandani, 2017). It increases trust among communities, as beneficiaries no longer fear that others may take what is rightfully theirs. It also increases trust among servicers and businesses in clients and users, as their visibility means they cannot defraud them. For example, Aadhaar helps to increase banks' trust in clients, increasing the likelihood that they will lend to them. According to the Aadhaar CEO, the Aadhaar identity and the trust it inspires will help to unleash the full potential of each Indian,[57] although critics may not agree.

The results and impact of Aadhaar are poised to expand beyond the borders of India. Despite the ongoing controversies, over 20 other countries are interested in potentially implementing similar identity programmes and the underlying technology, according to reports (Jayadevan, 2018).

USER PERSPECTIVE

Feedback on Aadhaar-enabled services, such as PDS and pensions, was generally positive in the Centre for Global Development survey. Most respondents found that Aadhaar services were at least as good as the previous systems, with many stating they were better and only a few believing they were worse. Users generally found the services to be faster and more convenient, and appreciated that no one else could steal goods meant for them. There were some challenges, however, with 25% of users reporting having to authenticate three or four times before being accepted by the system, and some saying that the system has not worked for them at all (Gelb et al., 2017).

CHALLENGES AND LESSONS LEARNED

Aadhaar's main challenges stem from the privacy and security concerns of people and advocacy groups. Strong political support on the part of the Congress and the Prime Minister, as well as the Finance Ministry, was crucial to the success of Aadhaar in terms of programme implementation and subsequent interactions. Collaboration across many divisions and levels of government has also been critical, according to the original Aadhaar architect (Mirchandani, 2017).

53. Interviews with J. Sathyanarayana, Indian Administrative Service (IAS), Chairman of the Unique Identification Authority of India (UIDAI) and Advisor to the Chief Minister of Andhra Pradesh, and Ajay Sawhney, IAS, Secretary to the Government of India for the Ministry of Electronics and Information Technology, 12 December 2017

54. Interview with Ajay Bhushan Pandey, CEO of the Unique Identification Authority of India (UIDAI) , 11 December 2017.

55. Interview with Guru Prasad, National Informatics Centre, India, 12 December 2017.

56. The survey interviewed 633 households from both urban and rural areas, with a mix of incomes and land-owning statuses. Sixty-three percent of the respondents were women.

57. Interview with Ajay Bhushan Pandey, CEO of the Unique Identification Authority of India (UIDAI), 11 December 2017.