Aadhaar: Giving an Identity to India (A)

Appearing on The Daily Show in 2009, comedian Jon Stewart told Nandan Nilekani, the entrepreneur and politician often referred to as the Michael Bloomberg of India, "You're a very kind and lovely man. I welcome you as my new overlord."[1] A few years before, Nilekani had stepped down as CEO of Infosys, the giant Indian software and outsourcing company that he co-founded in 1981. He had had begun working on a book, "Imagining India," which made a deeply optimistic case for India's future and advocated for government reforms. According to Pratap Bhanu Mehta, the head of a Delhi think tank, the book showed "an odd romance about state-building that we haven't seen since the 1950s." In India, most contemporary ideas about government reform were "about getting the government out of where it doesn't belong. But here is a guy who's saying, 'Look, I'm going to build a state,'" said Mehta.[2] Among the key ideas in the book was that India should adopt national ID numbers for citizens, which would make it easier to claim entitlements and gain access to private services.

The book became a bestseller, and caught the attention not only of The Daily Show viewers, but also of leaders in Nilekani's own government. In 2009, the party of Prime Minister Manmohan Singh was re-elected, and Nilekani was offered to lead a newly created agency within the federal government responsible for issuing IDs to every Indian.[3]

For the next five years, Nilekani led that identity effort, known as Aadhaar, and built it very purposefully as a 21st-century institution. Although several small attempts to provide national IDs had been attempted in the past, none were nearly so ambitious. To ensure that no citizen registered for more than one ID number, Aadhaar used biometric scans of all ten fingers and two irises. To allow government as well as private corporations to easily verify any citizen's identity, Aadhaar was built with public APIs. Aadhaar enrolled its first citizen in 2010, and within 5 years had enrolled 600 million people; by early 2017, approximately 1.16 billion people had Aadhaar numbers.[4]

To many, Aadhaar represented the best of government infrastructure projects: big, ambitious, modern, and with the potential to significantly improve the lives of many Indians. However, a small group of vocal critics were also raising questions about the privacy implications of Aadhaar, as well as the wisdom of a system centralized so much power in the hands of the government. When Aadhaar reached scale, every Indian's biometrics would be stored in a central database; that database not only risked being hacked by criminals, but could also be misused by the government itself, facilitating mass surveillance. As Aadhaar began to roll out, these critics grew louder: "In 2009, there was a great deal of

This case was written by Lecturer David Eaves and Daniel Goldberg (Harvard MPP & MBA, 2019) at the Harvard Kennedy School (HKS). HKS cases are developed solely as the basis for class discussion. Cases are not intended to serve as endorsements, sources of primary data, or illustrations of effective or ineffective management.

excitement in India that [Aadhaar] would help reduce [customer verification costs] for banks and ease to financial inclusion. Verification of documents is particularly tricky in a country with a large migratory population. But along the way, we noticed the government was acting a bit funny," said Nikhil Pahwa, the founder of medianama.com, a technology news website. As time went on, critics contended that they saw a consistent pattern of false justifications for Aadhaar, inflated savings figures, and unfair political maneuvering.

In early 2017, these competing narratives had only become starker: was Aadhaar a bold and commendable project to bring hundreds of millions of impoverished Indians into the modern world, or was it an ill-considered scheme to centralize power at the expense of Indians' long-term security? Looking forward, government officials were preparing to expand Aadhaar to reach more citizens and to cover many more services, both public and private. Could that expansion be justified without making major changes to the nation's privacy laws or Aadhaar's technology infrastructure? Could delaying the expansion be justified in light of the tremendous short-term needs of Indians in poverty?

Background

The need for Identity Verification

Although easy to overlook in many countries, having simple ways to verify one's identity is an essential feature of modern public and private life. In the government, identity verification is sometimes needed to ensure that services reach only intended participants (e.g. welfare benefits should disburse to all citizens who qualify, and none should disburse to citizens who do not qualify), and is sometimes needed to track citizen participation in key programs (e.g. to ensure each person votes no more than once; to ensure all eligible citizens participate in military drafts). In the private sector as well, activities from banking to online dating typically require some way to verify that you are who you say you are.

When identity verification systems are weak, fraud and deceit become much easier. This makes routine interactions more costly and cumbersome, as multiple documents must be collected and processed to prove a citizen's identity. For this reason, Nilekani characterizes identity among the most fundamental features of modern society: "Even before we have property rights, you need identity rights. Because unless a person can identify himself or herself and have some sort of proof of existence, you can't even talk about him owning property or owning a car or whatever."[5] Based on similar reasoning, the United Nations set a Sustainable Development Goal to achieve "legal identity for all" by 2030, and several organizations (including the World Bank, the Gates Foundation, and Mastercard) developed a set of guidelines for reaching that goal.[6]

Identity verification is a task sometimes undertaken by government, and sometimes undertaken by the private sector. Private identity verification systems are particularly common on the internet, where companies like Facebook and Google offer services allowing users to log into other websites using their Facebook and Google profiles, essentially turning their accounts into a virtual identity card. However, because of the ease of creating fake and duplicate accounts, these solutions are typically not sufficient in instances where greater security is required.

To fill this gap, governments have typically provided an authoritative identity for every citizen. However, the approaches governments take toward identity verification vary significantly around the world. For instance:

- In the United States, the most common government identifier is the Social Security Number (SSN), a 9-digit number assigned to citizens and residents. However, the SSN originally had a much narrower purpose: created in 1936, it was originally intended only to help the government to maintain accurate records of individuals' earnings in jobs covered under the Social Security program. Over time, the simplicity and near-universality of SSNs has led them to be used for a variety of other functions; today, it is common to need to submit a SSN when applying for mortgages, opening bank accounts, filing taxes, applying for jobs, and elsewhere.[7]

- In the UK, an attempt to create a centralized national identity card was scrapped in 2011, leading to the creation of a federated system of identity management, known as UK Verify. With UK Verify, citizens choose from a list of companies certified to verify their identity. (In 2017, the certified companies included the Post Office, the bank Barclays, the credit checker Experian, and others.) The company asks users a series of questions, may require documentation (such as a driver's license or bank account details), and performs other checks to verify the user's identity. Once a user has been verified, they can access a variety of government services online.[8]

- In Estonia, a small Baltic country that built most of its national infrastructure after gaining independence from the Soviet Union in 1991, every citizen is required to have a photo ID card, which is embedded with an electronic chip, similar to that of a credit card. The chip is programmed with the person's name, national ID number, and gender. Much like a credit card, the chip is also programmed with PIN codes. When a citizen wants to access a public or private service, they can use their card and enter their PIN code, and the government will verify that they match.[9] PIN codes can easily be changed, and lost cards can be replaced.[10]

India: An Unidentifiable Country

India, often referred to as a mosaic of different cultures, faces several unique challenges for identity verification, chief among them its enormous size and significant diversity. At more than 1.2 billion people, India is the world's second most populous country, and the world's most populous democracy. The country spans nearly 1.3 million square miles, making it the seventh largest in the world. India is also a particularly fragmented country: 461 languages (22 of which are recognized as official languages in the Constitution), differing official languages in each of its 29 states, and relatively high degree of illiteracy.[11] India has more than 1,000 political parties, with six major national parties, and a long history of political division based on caste and religion.[12]

Poverty and lack of connection pose a second challenge to establishing firm legal identity in India. Although India's economy has grown rapidly in recent decades, the World Bank estimates that more than 400 million Indians still live in poverty, and that the poverty rates in India's poorest states are 3-4x higher than in more prosperous states.[13] Especially in these poorer and more remote areas, the registration of births is relatively rare: despite a 1969 law requiring the recording of all Indian births and deaths, it was estimated that only slightly greater than 50% are registered, and only a small percentage of these registrations have birth certificates.[14] The result is a lack of formal records to verify that hundreds of millions of citizens exist.

As India has rapidly developed, these challenges have, in many ways, become more acute, as the demand for reliable and authoritative identity has increased. As Nilekani explains, Indians are becoming much more mobile: "People are moving from villages to cities, from north to south, from central India to coastal India. And all of them are finding that when they make that transition—they go to a new state and new city—they have to prove to the local establishment who they are, or they can't open a bank account, they can't get a mobile connection, they can't get their entitlements."[15] Not only has India become a more mobile society, but it has also become a more virtual society. In November 2016, Prime Minister Narendra Modi declared that nearly all cash in India would be voided (known as "demonetization"), forcing a massive increase in online payments. The Indian government has also aggressively pursued digitizing government services, increasing internet access, and other digital initiatives. While decades ago informal networks in smaller towns and villages could function as an ad-hoc identity verification, a more mobile and more digital society has made the need for formal identity much starker.

The Founding of Aadhaar

By the mid-2000s, India had already seen several efforts to provide identity to residents, such as the issuance of photo ID cards by the Election Commission in 1993 and the approval of the Multipurpose National Identity Card in 2003. However, the push for a unique identity truly began in 2009, when the Indian Planning Commission issued a notification creating the Unique Identity Authority of India (UIDAI).[16] In June of that year, Nandan Nilekani was appointed chairman of UIDAI, on the condition that he be given a cabinet-level appointment, reporting directly to the Prime Minister.[17]

To the Indian government, the primary reason for establishing residents' identity was to simplify the distribution of welfare benefits. Less than 5% of Indians pay income tax, less than 10% have salaried jobs, and 75% earn less than 5,000 rupees (or approximately $78) each month. The result is that a substantial portion of Indians depend on the state for welfare benefits (including direct cash transfers, subsidized food, cooking gas, and other benefits).[18] However, the government feared that a substantial portion of those benefits were being wasted due to fraud and corruption. As Pramod Varma, another Aadhaar co-founder responsible for the system's engineering architecture, explained to an audience at the UN, "India spends a huge amount of money on direct subsidies—about $50 billion every year…[However,] leakages on subsidies are very, very high [20-40%]. This is a very conservative number. So about $10 billion dollars every year going from the government is not going to the people it's supposed to reach."[19] For instance, a family entitled to 5kg of rice on one ration card has a strong incentive to create multiple ration cards by claiming multiple identities, or by claiming the identity of a dead or nonexistent person. To prevent this, the first task of UIDAI was to create an identity system where everybody could claim an identity, but nobody could claim multiple identities.

This focus on welfare benefits was odd, according to some observers, and did not nearly justify such a costly system. In fact, according to Pranesh Prakash, policy director at the Centre for Internet and Society, it may not have even required an identity verification system at all: "Aadhaar assumes that most fraud is identity fraud… [However,] there's not even any estimate of how much identity fraud there is." Instead of verifying identity to reduce fraud, Prakash suggests other less intrusive solutions: "One example is adding GPS to food ration delivery trucks and tracking them to make sure they don't make unwarranted stops." As Usha Ramanathan, a civil liberties lawyer, put it, "This is a solution in search of a problem."[20]

To provide unique identities to any Indian, the team at UIDAI decided the system would need to be based on biometrics. When registering for their 12-digit Aadhaar number, a citizen would need to scan all 10 fingerprints and both irises. (Both fingerprints and irises are scanned because many citizens, particularly manual laborers, don't have readable fingerprints, and many citizens, such as those with cataracts, don't have readable irises.) The government would then query its database to ensure that nobody with matching biometrics had already registered, a process known as de-duplication. To protect privacy, the Aadhaar asks for only four other data points: name, date of birth, gender, and address.

The use of biometrics alarmed many privacy advocates, who worried about the consequences if biometric data were stolen. However, UIDAI saw little alternative: as Nilekani explains, "in a society where every birth is registered, everybody has a unique root document that can be used for subsequent IDs. But in a society, where in some states, more than half of births are not registered, you have a lot of people with no ID or inadequate ID. And the only way we could solve the problem of establishing uniqueness was through biometric de-duplication." Without biometrics, it would have been nearly impossible to ensure all identities are unique.

Although Aadhaar was publicly marketed as a system for disbursing welfare benefits, the founders actually had a much more ambitious vision. The founders make a point of distinguishing between "foundational" and "functional" IDs. (Aadhaar means "foundation" in Hindi.) As Varma explains, a foundational ID is "minimalistic, context-free, unique, and verifiable." Functional IDs may then be built "on top of" the foundational ID, and include more specific information: "It could be a digital social network identifier or an ATM card or a passport or a driver's license. They are all identifiers, functional in nature, that can be used in a specific domain," explains Varma. In Varma's eyes, Aadhaar was a foundational ID; disbursing welfare benefits was merely a functional use case.

This platform-like vision for Aadhaar was inspired by government investments in the US. As Nilekani explains:

> We were inspired by the internet and GPS. In both cases, the design and investment was

> done by the US government. The internet is 40 years old, but it was only about 20 years ago that the private usage of the internet began with Netscape in 1995, which then led to Facebook and Google and all the great innovation we have since seen. Similarly, GPS was a US government investment for military purposes, but sometime around 2000, the commercial use of GPS was allowed and a few years later you had Google Maps and Uber. So, the Aadhaar system is designed for both government and commercial use. For the government, it is primarily used for eliminating corruption and fraud, and that itself justifies the investment. But over time there will also be a lot of innovative [private] uses that will be built on top of this infrastructure.

Actually rolling out Aadhaar to India's citizens represented a massive operational challenge. Operating as a "startup" within government, UIDAI never had more than a few hundred employees, and moved quickly to develop the software and database structures that would undergird Aadhaar. Given the size of India's population, the software had to be immensely scalable. The database would be an order of magnitude larger than what was then the world's largest biometric database, the US visa database, which included biometrics from about 100 million people.[21] When the billionth Indian registered for his or her Aadhaar number, the system would need to search for duplicates among each of nearly 10 billion fingerprints and 2 billion irises within a few seconds.

To reduce costs and increase speed, UIDAI relied on private contractors to handle most of the citizen enrollment. This, too, was not without controversy: according to Nikhil Pahwa, a technology commentator, "There are instances of dogs getting Aadhaar numbers, gods and goddesses getting Aadhaar numbers. These things happened because of how fast it was rolled out without enough checks and balances, and an outsourced enrolment program which incentivised speed of enrollment over accuracy. Vendors were paid per enrollment." However, the result was that enrollment was accomplished with remarkable speed and efficiency: according to Nilekani, the total cost was less than $1 per citizen. Within 5 years, Aadhaar had enrolled 600 million people; by 2017, approximately 1.16 billion people had Aadhaar numbers.[22] (See **Exhibit 2** for Aadhaar's enrollment growth.) To Nilekani, "Just making Aadhaar happen was my biggest success. It's a big, complex, and bureaucratic environment. And in that environment, to start from scratch and build a platform which today has 1.1 billion people on it and has become central to the governments' reform program is the biggest achievement."

One reason for Nilekani's pride in growing Aadhaar was that its expansion coincided with a dramatic political transition in India. In 2014, the nation held general elections that swept the Bharatiya Janata party (BJP), led by Narendra Modi, into power. Modi's BJP won a total of 282 out of 543 seats in the lower house (the first time in 30 years one party had won enough seats to govern without a coalition); the Congress party, previously in power and in power for all but 18 of the prior 67 years, won a meager 60 seats. The election results were surprising to many observers, and disturbing to some given Modi's reputation as a controversial Hindu nationalist.[23] However, the results were likely especially nerve-wracking to Nilekani and other Aadhaar advocates, as Modi had been a vocal critic of Aadhaar during the campaign. Approximately 2 months after the election, Modi and Nilekani met; a few days later, plans to merge UIDAI with other agencies were scrapped, and Modi's government began expanding Aadhaar in increasingly aggressive fashion.[24]

By 2016, Aadhaar had outgrown its relatively informal beginnings. Since its founding in 2009, UIDAI had been operating based on administrative rules issued by the government, but without firm legislative backing. Thus, in 2016, a bill was introduced to give UIDAI clearer legislative authority. To much criticism, the bill was introduced as a "money bill," a type of bill that needs to only pass in the lower house of parliament, on the grounds that it primarily concerned disbursing welfare benefits. To critics, the enormous number of potential uses for Aadhaar made it much broader than a money bill; moreover, they saw the tactic as politically motivated, as the ruling party lacked a majority in the upper house of parliament. Despite protests, the bill went forward as a money bill, and on March 11th, 2016 the "Aadhaar Act" was passed by the lower house of parliament and became law.[25]

Aadhaar Today

Aadhaar to Users

To a user, registering for Aadhaar is relatively simple. After waiting in line at a registration center, the citizen places his or her hands on a fingerprint scanner, peers into an iris scanner, and enters their name, date of birth, gender, and address into the computer database. If there are no matches for the same biometrics, a 12-digit Aadhaar number can be assigned on the spot, and a card will arrive in the mail a few weeks later.

This relatively simple process for gaining a legal identity stands in sharp contrast to the tedious process that was previously required. According to Rahul Matthan, a technology lawyer, obtaining a passport was previously a nearly herculean task: "To get a passport, the police need to come to your house and verify that you live there. They will also interview two of your neighbors to confirm you've been there for some time… And each time you renew your passport, you have to go to a police station and accompany a cop to your house and show him where you stay." The process was both time consuming and expensive. Despite these inconveniences, many Indians did have some form of ID: as of 2015, more than 99.9% of all Aadhaar numbers were issued to people who already had at least two existing forms of identification.[26]

Using the Aadhaar number is likewise relatively simple. There are two key services offered by Aadhaar: authentication and electronic "Know Your Customer" (eKYC). Authentication allows Aadhaar holders to prove that they are who they say they are. For instance, at a government ration station, a user can place their thumb on a fingerprints scanner and input their Aadhaar number. The system then returns only a "Yes" or "No" answer to whether the thumbprint and number match. If they do, the rations are disbursed.[27] eKYC is a second service that sits on top of authentication, and allows users to share more demographic information. For example, when opening a bank account, an Aadhaar user may enable eKYC functionality, and thereby allow Aadhaar to share their name, date of birth, address, and mobile phone number, in addition to the simple Yes/No answer to their identity claim. The bank can then use this data to open an account for the user.

When the system works, it presents massive savings of time and money. According to Pramod Varma, the use of eKYC has reduced the time required to onboard a customer at a bank from 6 days to 1 hour, the customer onboarding at telecoms from 1 day to 4 minutes, and the transaction times at large asset management firms from 4 hours to 2 minutes. [28] The previous system "simply excluded hundreds of millions of people, simply because there was no effective way for them to establish their identity. With more and more things like money laundering and terrorism funding, these regulated domains like financial services only got more paperwork, and that actually meant more exclusion," explains Varma. With Aadhaar and eKYC, the costs of customer acquisition have fallen enough to both benefit corporations and allow more citizens to participate in the economy.

However, when the system doesn't work, it can be tremendously disruptive to a citizen's life. Because authenticating an identity via Aadhaar requires an internet connection and electricity, ration shops in remote areas are known to force their customers to move to the top of a hill or roof, where there is a phone signal, to verify their identity. Even more troubling are rumors of significant false negatives on identity claims: according to The Economist, in some areas as high as a third of authentications come back negative.[29] To many, this is a significant and unacceptable failure rate for a system on which people rely for basic necessities. Nikhil Pahwa, a technology writer, asks: "You look at some of these videos on YouTube of poor people, old people, people who've had to travel 10 kilometers to try to get their monthly rations [but are turned away], and you have to start thinking: is this worth it?" Some go even further in their critiques, arguing that the prevalence of false negatives represents an assault on poor Indians. According to Sowmya Kidambi, the government knew that the system was not reliable, and therefore did not implement it for teachers, hospital workers, or other professionals. "This is being done to the poor," she said, because "the assumption is that the poor are thieves."[30]

The problem of false negatives becomes even more pressing as a growing number of services require Aadhaar. Although Aadhaar was originally designed as a voluntary system, in which users had a choice of how to identify themselves while collecting welfare benefits, the 2016 Aadhaar Act allowed Aadhaar to be made mandatory for certain government benefits, while keeping it voluntary for more ancillary functions. Nonetheless, significant controversy continues as to whether Aadhaar is, in fact, voluntary: "There is quite a bit of confusion," says Arghya Sengupta, Director of the Vidhi Centre for Legal Policy. "I saw a meme that Aadhaar is like Schrodinger's Cat: it's mandatory and not mandatory at the same time." The Supreme Court has ruled that Aadhaar should be voluntary. However, in early 2017, the government made access to several services contingent on using Aadhaar and inserted a rule into a fast-tracked budget that required linking tax numbers with Aadhaar numbers. Rumors circulated about whether Aadhaar would soon be mandatory for things like school lunches and purchasing airline tickets.[31] "As a lawyer I can certainly see that it's essentially a mandatory scheme for many purposes," says Sengupta.

Aadhaar to Government Agencies

To the government, having citizens use Aadhaar makes the administration of public benefits simpler and more efficient, although there is disagreement about how much of an improvement

Aadhaar represents. World Bank Chief Economist Kaushik Basu estimated that Aadhaar saves the Indian government approximately $1 billion per year[32]; the Indian Finance secretary estimated in March 2017 that approximately $6 billion had been saved since Aadhaar's inception.[33] These savings are derived from a variety of different sources, including reduced corruption, reduced leakage, and improved efficiency. For instance, a large portion of the savings came from welfare programs in which, because of Aadhaar, money could be directly deposited into citizens' Aadhaar-linked bank accounts. According to Nilekani, "the government has said that the cumulative savings from eliminating fraud and corruption were about $9 billion, and the total project cost was about $1.5 billion. So Aadhaar has had a very high ROI."

However, some critics dispute these savings figures, arguing that the actual savings are in fact much lower. According to Nikhil Pahwa, "The savings are overhyped… A significant portion of the savings come from people being disenfranchised"—in other words, from not granting welfare benefits to people who deserve them. In addition to this, Pahwa claims that the government savings figures rely on overly optimistic estimates: one article on his website suggests that the actual savings in a particular program may be 200 times lower than the government claims.[34] Thus, many activists are distrustful of the government's claims about savings.

Beyond savings, Aadhaar also has advantages for governments in the realms of transparency and performance management. For instance, state governments in India have used Aadhaar to advance their financial inclusion goals (e.g. giving all citizens an Aadhaar-linked bank account) and enable digital payments (e.g. directly to another Aadhaar number, linked to a bank account). Some states post voluminous Aadhaar-related statistics online on government scorecards and performance management dashboards.

The drive for transparency can go too far. According to a May 2017 report, the websites for several government programs disclosed Aadhaar numbers and other personally identifiable information for between 100 million and 130 million people. According to the authors, this may be only a small portion of the data available on other websites. However, even this limited trove is significant, and increases the likelihood of fraud and theft.[35] According to Aadhaar defenders, this disclosure is more the result of a misunderstanding than a mishap. Government websites had long posted personal information of the recipients of welfare benefits (including information as specific as name, address, and date of birth), in an effort to reduce fraud and corruption. When Aadhaar numbers were added to government databases, it seemed only natural that this, too, should be published. As Varma explains, "two different purposes collided. The Right to Information Act people said, 'don't go back to hiding all the information, it was a mechanism to allow social audits of how governments use taxpayers money.' At the same time, privacy advocates were saying 'you can't put all this information online.' So India has to debate what information needs to be given out when it's taxpayers' money."

Criticisms of Aadhaar

Risks of Data Security and Identity Theft

To security advocates, it was concerning to learn that the government had published a large number of Aadhaar numbers; however, their concerns began long before those publications. Two fundamental features of Aadhaar that were required to uniquely identify and de-duplicate IDs—that it rely on biometrics as well as a central database—also make it uniquely vulnerable to hacks.

The fact that biometrics are unique and cannot be changed made them essential for ensuring that each ID issued by Aadhaar is unique, but it also causes concern to security advocates. As Nikhil Pahwa, the technology writer, explains: "The Aadhaar number is like your permanent username; biometrics are like your password. And biometrics can't be changed. So, you can't change your password if it gets leaked. That means Aadhaar is a system which makes people more vulnerable." Not only can biometrics not be changed, but many fear that stealing them from individuals is relatively easy. Recently, engineers have claimed to have developed technology that can capture iris scans discretely from distances of up to 40 feet; however, critics are skeptical that the granularity of such images is sufficient to make them useful.[36] The ability to steal fingerprints is much simpler, as Pahwa illustrates: "Imagine I go to authenticate my thumbprint somewhere and the teller puts out a fake machine and records my thumbprint. And then they say, 'Oh this machine didn't work, let me try another machine,' and they put out another machine that's real." Such schemes need not be high tech; they simply need to be well-executed.

Not only can biometrics be stolen from individuals, but they can also be stolen from the government. All biometrics are stored in a central database, making it a valuable, if difficult to breach, target for hackers. There have been no data breaches yet, but many Indians leerily recall the 2015 Office of Personnel Management hack in the US, which compromised 22 million personnel records and 5.6 million sets of fingerprints of government employees. "In the US, because everything is not tied to your fingerprints, the consequences of this massive data breach were still limited," says Pranesh Prakash of the Centre for Internet and Society. However, "in India, using the same data, you would be able to engage in bank transfers. People are proposing being able to vote remotely. Well, if you have peoples' fingerprints, some of the very foundations of democracy would be in question—not just all the money in your account." Critics worry that that the lack of data breaches in the past does not predict that there won't be any in the future.

Not all agree that these are serious threats. For one, even if the data of a person's fingerprint is stolen, using the data to impersonate that person is another matter. Actual fake fingerprints would need to be produced, an expensive and difficult undertaking. Furthermore, UIDAI has built significant data security into every aspect of its operations to prevent breaches in the first place. For instance, at the point of capturing the biometric, Nilekani explains that "We've done a lot of work on what are called 'registered devices,' so that the biometric is captured and encrypted at source from a recognized device during authentication and is safe and secure."

However, overall, Nilekani is somewhat unperturbed about the problems of data security: "Your biometrics are now actually being used everywhere—when you are on your smartphone and use the fingerprint or iris sensor, you are giving your biometric to the smartphone vendor. And with the advances happening in image and facial recognition, somebody can take your photograph and figure out who you are. So, biometrics has now become so pervasive, that we just have to deal with the challenges of privacy, security and surveillance in a very broad way." In other words, these data security issues are much larger than Aadhaar, even if they were accelerated by Aadhaar's development.

Risks of Privacy and Surveillance

Even when Aadhaar is kept secure and no identity theft takes place, critics have identified a second important risk: reduced privacy. This concern is particularly pressing because India's data privacy laws in early 2017 were notoriously weak. India has no nationally recognized right to privacy, and although there are a set of administrative rules define a framework for protecting personal digital data, experts fear that because there is no actual privacy law, the rules have no teeth. According to Rahul Matthan, a partner at the TriLegal law firm, "You have this set of rules that says what you can do, but there's nothing that says what happens if you don't do it. There is also nothing in the rules that says who's going to enforce all of this." Matthan laments:

> I think there are about 120 countries that have privacy laws in place…Not only do we have none of that, we have no inherent requirement for it. The way our society is set up, there is a certain freedom with parting with personal information that doesn't exist in other countries.

In some ways, Aadhaar anticipates citizens' concerns about privacy, and has designed its architecture to protect privacy. For instance, as Arghya Sengupta, director of Vidhi Center, explains, the drafters of the Aadhaar Act "hardwired data minimization into the statute by not allowing certain categories of data to be collected, such as caste, religion, and so on." In addition, the Aadhaar Act strictly regulates who can access biometric information, how that information can be shared, and gives strict penalties for breaking those laws.

However, no matter how strong the protections in the Aadhaar Act may be, they exist in a broader environment that is largely unregulated. Organizations other than the UIDAI—including other government agencies and private corporations—are neither governed by the Aadhaar Act nor any other privacy law. Thus, although the Aadhaar Act limits the information that UIDAI can collect, other organizations can build robust databases of personal information and tie that information to an Aadhaar number. This was not a major issue prior to Aadhaar because, as Rahul Rahul Matthan of TriLegal puts it, India had "inherent privacy protection, because the data collected, even by government, [was] in siloes." Stitching together a comprehensive view of an individual was difficult (but not impossible) because each disconnected form of ID—a birth certificate, driver's license, passport, email address, account number, or other informal identity—would need to be linked together in a database. This complexity made some kinds of fraud much easier, but it also offered privacy protections. Adding Aadhaar numbers to data sets undermines this protection because it gives a unique key that can be much more easily linked between databases, effectively breaking down silos.

Reductions in privacy not only make it easier for corporations to build up databases of personal information, but also make it easier to conduct state surveillance. Many see this as the primary concern: Aadhaar "makes citizens particularly vulnerable to machinations of the state, and I'm particularly worried about a totalitarian regime coming in," says Nikhil Pahwa. Again, the Aadhaar architecture takes some precautions against these types of risks, such as maintaining limited logs of transactions. As Pramod Varma explains, "Aadhaar is like a GPS. GPS doesn't know whether you're taking Uber from home to your work. All it does is tell location. So Aadhaar is designed to be completely agnostic or unaware of the purpose of your authentication. All it tells you is whether your identity claim is right or not."[37] Despite this claim by Varma and others, some outside critics simply don't believe it. As Pranesh Prakash comments, "One of the big question marks that isn't clear is what's being logged by UIDAI when a transaction happens, for instance when somebody authenticates me or uses eKYC. How much information does UIDAI have about that, and how long is it stored?... The law tries to keep the logs minimal…But there's really no way of enforcing that."

Requests to surveil citizens are already common in law enforcement. As Narendra Bhooshan, the deputy director general of the Enrolment & Updation Division at UIDAI, recounts, "We sometimes receive requests that somebody is absconding, has taken lots of loans, has run away, and can you help us track him." UIDIA currently refuses these requests, but their legality is currently being adjudicated. Outside of law enforcement, many legal experts are less worried about the possibility of surveillance. As Rahul Matthan of TriLegal remarks, "There are many nefarious things the state could do, like classifying people by race, religion, and other irrelevant criteria…Having said that, the law is quite clear that the state cannot discriminate on these grounds…We have many decades of jurisprudence on that. If Aadhaar were to be used for something like that, the lack of a privacy law wouldn't come in the way of somebody taking the government to task."

While most agree that the lack of a privacy law is a risk for Aadhaar, there is widespread disagreement about the correct remedy. Although Varma acknowledges that "The ideal situation would have been to enact an umbrella privacy and data protection law in India," he argues that the most prudent sequence of events was to build Aadhaar first and worry about privacy laws later, rather than the reverse. This is in part because a primary goal of Aadhaar founders was simply to grow Aadhaar as quickly as possible: "One clear goal we had was to have wide adoption of Aadhaar, which required having close to the entire resident population enrolled on the platform." said Nilekani. A second reason that Varma and Nilekani believed privacy laws could come later is because they believed Aadhaar would actually create a demand for privacy where none previously existed. As Varma explains, "Interestingly, having Aadhaar is now making the civil society more interested in putting in the privacy law, because so much digitization is happening in India."

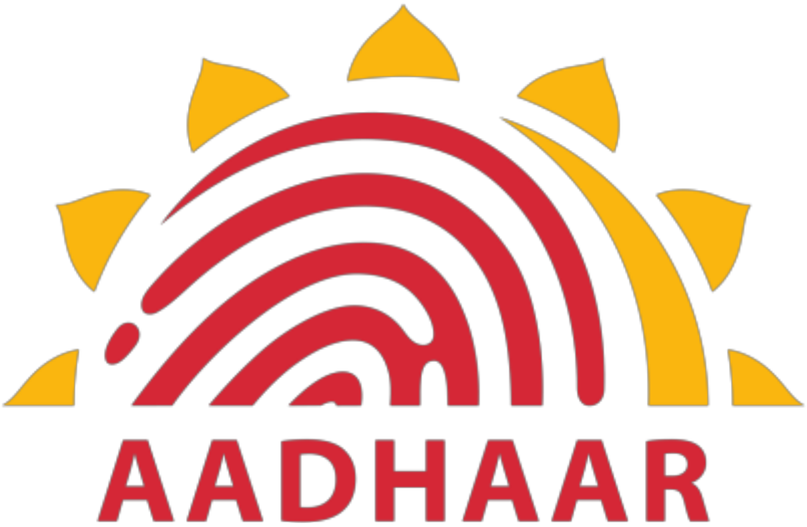
Moreover, Varma argues that there may be little need for a privacy law at all, as much of the problem could be solved through additional Aadhaar product features. In particular, Varma envisions a system in which "the technology allowed an Aadhaar holder to say, 'In this case, I'll use a temporary identifier.'…Imagine the system allowed me to create a virtual number, and then I can revoke it." Currently, Aadhaar can only verify somebody's identity if they use their full Aadhaar number, but if the system allowed Aadhaar holders to create temporary, revocable numbers, a separate number could sit in each database and make it much more difficult for them to be stitched together. "Federated databases are already happening, but federated identities are not happening," explains Varma. "More and more, [I'd like to enable] derived identifiers to be used within a domain, which are revocable and changeable."

Undergirding Varma's and Nilekani's relative lack of concern about enacting strict privacy protections quickly is a focus on serving more people. "There is always a fine balance between a theoretically perfect solution versus 800 million people having nothing," says Varma. To Varma, the privacy advocates are losing sight of the very pressing short term needs of poor Indians: "A huge portion of people depend on the state to provide for them. Lots of us who travel around the world have a very evolved view of [privacy], saying 'We won't trust the state to do the right thing, and there will be temptations to do bad things.' And there will be. But sometimes [we must] solve short term problems that are affecting people every day." Instead of developing a stronger solution, with more privacy protections up front, UIDAI has focused on serving as many people as possible as quickly as possible, and evolving Aadhaar as time goes on. By focusing on evolution rather than perfection, they believe that UIDAI can continuously improve Aadhaar, reducing error rates and building more privacy protections into the architecture.

Moving forward

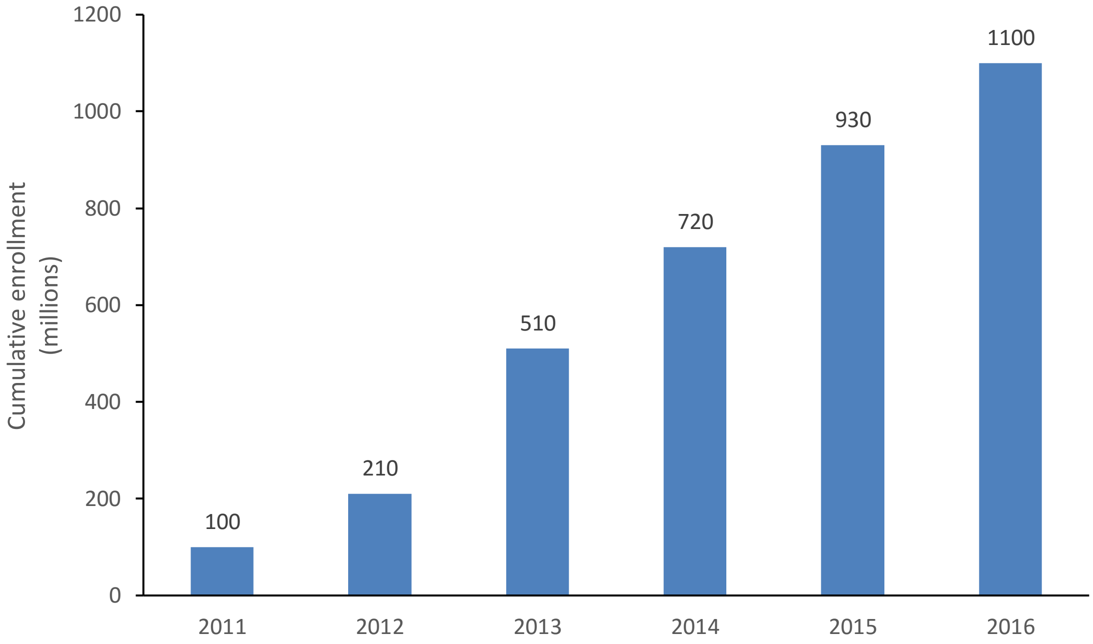
As India continues to rapidly digitize, the role of Aadhaar in society promises only to grow. However, how Aadhaar should grow with India is a matter of fierce debate. Could critics' complaints about Aadhaar be best addressed with policy changes (such as enacting or privacy law or other regulations about data use), product improvements (such as developing temporary identifiers), governance reforms, or something else? And perhaps most fundamentally: is it finally time for Aadhaar to stop prioritizing expansion and begin focusing more on privacy and security; or, with limited adoption by the private sector and still significant potential to impact the lives of poor Indians, should expansion still take priority above all else?

Exhibit 1: Aadhaar Logo



Source: Wikipedia

Exhibit 2: Aadhaar Enrollment Growth Over Time



Source: "State of Aadhaar Report, 2016-17", IDinsight. http://stateofaadhaar.in/wp-content/uploads/State-of-Aadhaar-Full-Report-2016-17-IDinsight.pdf

Endnotes

[1] Ian Parker, “The I.D. Man,” *The New Yorker*, September 26, 2011, http://www.newyorker.com/magazine/2011/10/03/the-i-d-man.
[2] Ibid.
[3] Ibid.
[4] “Public Data Portal,” *UIDAI Dashboard Summary*, accessed July 9, 2017, https://portal.uidai.gov.in/uidwebportal/dashboard.do.
[5] Eric Braverman and Mary Kuntz, “An Interview with Nandan Nilekani,” *McKinsey*, October 2012, http://www.mckinsey.com/industries/public-sector/our-insights/an-interview-with-nandan-nilekani.
[6] Neil Hughes, “15 Global Organizations Issue New Principles for Inclusive, Secure Identification in the Developing World,” *One World Identity*, February 8, 2017, https://oneworldidentity.com/2017/02/08/world-bank-issues-10-principles-inclusive-secure-identification-developing-world/.
[7] Carolyn Puckett, “The Story of the Social Security Number,” *Social Security Bulletin*, 2009, https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html.
[8] “GOV.UK Verify - GOV.UK,” accessed May 30, 2017, https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify.
[9] Keith Duffy, Pasha Goudovitch, and Pavel Fedorov, “The Application of Digital Identity in the United States,” May 10, 2016, http://dci.mit.edu/assets/papers/15.998_identity.pdf.
[10] “Estonia Takes the Plunge,” *The Economist*, accessed May 23, 2017, http://www.economist.com/news/international/21605923-national-identity-scheme-goes-global-estonia-takes-plunge.
[11] “Languages in India - Map, Scheduled Languages, States Official Languages and Dialects,” accessed July 8, 2017, http://www.mapsofindia.com/culture/indian-languages.html.
[12] Konstantinos Antonopoulos and Nadine Cheaib, “India’s Political Parties and Their Symbols,” *Al Jazeera English*, April 6, 2014, http://www.aljazeera.com/indepth/interactive/2014/04/india-political-parties-their-symbols-201446115541946199.html.
[13] “The World Bank in India: Overview,” *The World Bank*, accessed July 8, 2017, http://www.worldbank.org/en/country/india/overview.
[14] Arun Serrao and Sujatha B.R., “Birth Registration, a Background Note” (UN Knowledge Base: Civil Registration and Vital Statistics, October 23, 2004), https://unstats.un.org/unsd/vitalstatkb/KnowledgebaseArticle50113.aspx.
[15] Braverman and Kuntz, “An Interview with Nandan Nilekani.”
[16] “About UIDAI: Background,” *Unique Identity Authority of India*, accessed July 8, 2017, https://uidai.gov.in/about-uidai/about-uidai/background.html.
[17] Mitu Jayashankar and N.S. Ramnath, “UIDAI: Inside the World’s Largest Data Management Project,” *Forbes India*, November 29, 2010, http://www.forbesindia.com/article/big-bet/uidai-inside-the-worlds-largest-data-management-project/19632/1.
[18] Ritika Katyal, “India Census Shows Extent of Poverty,” *CNN*, August 2, 2015, http://www.cnn.com/2015/08/02/asia/india-poor-census-secc/index.html.
[19] Pramod Varma, “2017 ID2020 ‘Platform for Change’ Summit” (2017), http://webtv.un.org/search/2017-id2020-platform-for-change-summit/5476783692001?term=2017%20ID2020%20Platform%20for%20Change%20Summit.
[20] Lydia Polgreen, “With National Database, India Tries to Reach the Poor,” *The New York Times*, September 1, 2011, sec. Asia Pacific, https://www.nytimes.com/2011/09/02/world/asia/02india.html.
[21] Ibid.
[22] “Public Data Portal.”
[23] Jason Burke, “Narendra Modi’s Landslide Victory Shatters Congress’s Grip on India,” *The Guardian*, May 16, 2014, sec. World news, http://www.theguardian.com/world/2014/may/16/narendra-modi-victory-congress-india-election.
[24] Shankkar Aiyari, “How Aadhaar Scheme Got a Second Life under PM Modi - Times of India,” *The Times of India*, July 6, 2017, http://timesofindia.indiatimes.com/india/how-aadhaar-scheme-got-a-second-life-under-pm-modi/articleshow/59464487.cms.

[25] "Aadhaar Bill Passed in Lok Sabha," *Livemint*, March 11, 2016, http://www.livemint.com/Politics/UgblAmPPHetk71sjQUqcvN/Aadhaar-bill-passed-in-Lok-Sabha-the-story-so-far.html.

[26] The Wire, "'Most Aadhar Cards Issued to Those Who Already Have IDs,'" *The Wire*, June 3, 2015, https://thewire.in/3108/most-aadhar-cards-issued-to-those-who-already-have-ids/.

[27] "India's ID System Is Reshaping Ties between State and Citizens," *The Economist*, April 12, 2017, https://www.economist.com/news/asia/21720609-long-they-have-mobile-signal-indias-id-system-reshaping-ties-between-state-and-citizens.

[28] Varma, 2017 ID2020 "Platform for Change" Summit.

[29] "India's ID System Is Reshaping Ties between State and Citizens."

[30] "(Big) Hopes and Hazards of Big Data | School of Public Policy," accessed June 14, 2017, https://spp.ceu.edu/article/2017-05-15/big-hopes-and-hazards-big-data.

[31] "India's Biometric Identity Scheme Should Not Be Compulsory," *The Economist*, April 15, 2017, https://www.economist.com/news/leaders/21720599-bjp-government-should-listen-peoples-qualms-about-snooping-indias-biometric-identity.

[32] "Aadhaar ID Saving Indian Govt about USD 1 Bln per Annum: World Bank | The Indian Express," accessed July 12, 2017, http://indianexpress.com/article/india/india-news-india/aadhaar-id-saving-indian-govt-about-usd-1-bln-per-annum-kaushik-basu/.

[33] ET Bureau, "Aadhaar Scheme Helped Government Save Rs 34,000 Crore: Finance Secy," *The Economic Times*, March 30, 2017, http://economictimes.indiatimes.com/news/economy/finance/dbt-leads-to-rs-34000-crore-savings-for-government-finmin/articleshow/57894751.cms.

[34] Anand Venkatanarayanan, "Government's Claims of Aadhaar Savings for the LPG Scheme Are Overstated," *MediaNama*, June 8, 2017, http://www.medianama.com/2017/06/223-aadhaar-lpg-scheme/.

[35] Amber Sinha and Srinivas Kodali, "Information Security Practices of Aadhaar (or Lack Thereof)" (The Centre for Internet and Society), accessed July 13, 2017, https://cis-india.org/internet-governance/information-security-practices-of-aadhaar-or-lack-thereof/view.

[36] Robinson Meyer, "Long-Range Iris Scanning Is Here," *The Atlantic*, May 13, 2015, https://www.theatlantic.com/technology/archive/2015/05/long-range-iris-scanning-is-here/393065/.

[37] Converge - ThoughtWorks, *Pramod Varma : Building Country Scale Systems (Aadhaar & India Stack Experience)*, n.d., https://www.youtube.com/watch?v=lvZSXjB_04s.