IDinsight
DATA. DECISIONS. DEVELOPMENT.

STATE OF AADHAAR REPORT 2016-17

MAY 2017

Sponsored by ON OMIDYAR NETWORK

IDinsight
DATA. DECISIONS. DEVELOPMENT.

STATE OF AADHAAR REPORT 2016-17

MAY 2017

Ronald Abraham
Delhi

Elizabeth S. Bennett
Delhi

Noopur Sen
Delhi

Neil Buddy Shah
San Francisco

Sponsored by

OMIDYAR NETWORK

About IDinsight

IDinsight is an international development consulting organisation that helps policymakers and managers make socially impactful decisions using rigorous evidence. We carefully tailor a wide range of analytical and quantitative tools to enable our clients to design better policies, rigorously test those ideas, and take informed action at scale to improve lives.

Our advisory teams have led embedded cells within ministries of state-level governments—including Andhra Pradesh and Bihar—and have worked in a wide range of sectors, including agriculture, education, health, and digital identity. We strive to provide comprehensive support for clients who want to maximise their social impact through evidence-informed policymaking.

IDinsight has offices in Delhi, Lusaka, Manila, Nairobi, San Francisco and Vijayawada.
To learn more, visit www.IDinsight.org.

About Omidyar Network

Omidyar Network is a philanthropic investment firm. We create opportunity for people to improve their lives by investing in market-based efforts that catalyse economic and social change. In India, we focus our efforts on helping the 100's of millions of Indians in low-income and lower-middle-income populations, which we define as ranging from the poorest among us to the existing middle class.

Omidyar Network has committed more than $1 billion to for-profit companies and nonprofit organisations that foster economic advancement and encourage individual participation across multiple areas, including Digital Identity, Education, Emerging Tech, Financial Inclusion, Governance & Citizen Engagement, and Property Rights.

To learn more, visit www.omidyar.com, and follow on Twitter @omidyarnetwork #PositiveReturns.

Suggested citation

Abraham, Ronald, Elizabeth S. Bennett, Noopur Sen, and Neil Buddy Shah.
State of Aadhaar Report 2016-17. Report. IDinsight.

Contact us

We welcome your feedback on this report. Please write to us with your comments or questions to StateofAadhaar@IDinsight.org.

Disclaimer

The information contained in this report is prepared by IDinsight and commissioned by Omidyar Network. It is furnished to the recipient(s) for free distribution and use. The authors have made their best efforts to ensure the accuracy and completeness of the information in this report but make no representations or warranties therein and expressly disclaim any liabilities based on such information or on omissions. Each recipient should therefore conduct its own analysis of any information contained in this report.

Preface

IDinsight's work on Aadhaar and digital identity began with our partnership with Omidyar Network in the latter half of 2015. In this engagement, we spoke with a diverse range of leaders—in government, the private sector, civil society, academia, and think tanks—to gauge whether and how research on the Aadhaar landscape would be useful for practitioners. We were struck by the robust consensus on the general need for more research, data, and evidence, as well as specific concrete suggestions on particularly salient evidence gaps.

One of the frequent refrains we heard was that there is a vital need for a comprehensive, empirical, and structured review of the Aadhaar landscape: its architecture, governance, and various uses. Our interviewees consistently remarked that a foundational assessment of Aadhaar can promote a more fact-based understanding of the Aadhaar ecosystem. More critically, such an analysis could identify areas where more evidence is needed to understand whether and how Aadhaar can advance the welfare of India's residents. These conversations and consistent feedback sowed the seeds for the *State of Aadhaar Report 2016-17*, which we hope will adequately meet these objectives.

Our journey of carefully researching and compiling data from various sources, and bringing it together for this report would simply not have been possible without the excellent support of our wonderful research team: Akash Pattanayak and Rajesh Bhusal. In addition, we received tremendous technical and editorial support from our advisor, Heather Lanthorn. We also want to thank earlier members of our research team, Daniel Gastfriend and Suhani Jalota, whose contributions have been equally pivotal to this effort.

We also owe thanks to other members of IDinsight who reviewed this report and provided valuable feedback: Andrew Fraker, Doug Johnson, and Paul Wang. Another debt of gratitude is to our colleagues in the Delhi office, for the innumerable small and large ways in which they supported us.

This report also benefits from the expert review of many specialists in the Aadhaar or digital identity ecosystems. Their feedback tangibly improved the quality of this report and we are grateful for their time. The reviewers for this report included: Bhuvana Anand, Savita Bailur, Gautam Bhatia, Shrayana Bhattacharya, Alan Gelb, Anu Madgavkar, Anit Mukherjee, and Himanshu Nagpal.

We would like to extend a special thanks to Ajay Bhushan Pandey, the CEO of the Unique Identification Authority of India (UIDAI), for his inputs on our report and approach. We also want to thank Vijay Madan, former CEO of the UIDAI, who helped provide an in-depth understanding of the Aadhaar landscape.

We would like to thank Rajendra Srivastava, the Dean of the Indian School of Business (ISB), for his thoughtful advice on how to improve the report. In addition, we would like to thank Padmanabhan Balasubramanian and Prasanna Tantri, who are working closely on ISB's digital identity research initiative, for their detailed review of our work. We presented a version of this report to professors at ISB in a seminar and thank the participants for their constructive input.

We are thankful to Allan R. Gold, our editor, who significantly improved the report through his detailed review. We would also like to thank Studio Subu, our design firm. Both Allan and Studio Subu have been a pleasure to work with and provided excellent support despite demanding timelines.

And last, but certainly not least, we would like to sincerely thank Omidyar Network's digital identity team. CV Madhukar's advice on our approach and detailed feedback on the content have tremendously enriched the report's quality. It has been an absolute pleasure to work with Madhukar, Mike Kubzansky, Anamitra Deb, Subhashish Bhadra, Himanshu Jain and their colleagues. We thank you all for your in-depth support, critical thinking, and intellectual engagement throughout this process.

Of course, any shortcomings in the report are our own. It is our hope that this report facilitates meaningful dialogue and vital, policy-relevant research on digital identity systems across the globe.

Ronald, Elizabeth, Noopur, and Buddy

Letter from Dr. Pandey, CEO of UIDAI

Aadhaar has increasingly become an essential part of the everyday life of Indians across the country. The Unique Identification Authority of India believes that there is great potential within this identification platform to provide a legal identity for all residents as well as to improve the efficiency of government service delivery.

I am glad to note that the Indian School of Business is setting up a research initiative around the important topic of digital identity in India. An evidence informed debate on the salient issues around digital identity, specifically Aadhaar, will go a long way in strengthening the efforts of the government.

The *State of Aadhaar Report 2016-17* is a useful step in providing an organised overview of the Aadhaar landscape. A full understanding of the state of Aadhaar—and its current uses and challenges—is an important starting point for all those interested in realising the potential of Aadhaar as a tool for furthering public good.

Regards,

Dr. Ajay Bhushan Pandey
CEO, UIDAI

Letter from the Dean of Indian School of Business, Dr. R. Srivastava

I would like to thank and congratulate IDinsight on the *State of Aadhaar Report 2016-17*. This report provides a holistic overview of Aadhaar and its technical and operational nuances; anyone interested in this topic will find the report a useful starting point.

We at the Indian School of Business are making a significant commitment to the topic by embarking on an ambitious project to set up the Digital Identity Research Initiative. Through this project we plan to build an ecosystem of researchers and resources on Aadhaar to generate independent, multi-disciplinary, high quality research on digital identity and its applications. We hope that the findings generated by this effort will be translated into knowledge with immediate application for policymakers, educators, service providers, and entrepreneurs.

Regards,

Rajendra Srivastava
Dean and Novartis Professor of Marketing Strategy and Innovation
Indian School of Business

EXECUTIVE SUMMARY

Introduction

One-seventh of the world's population—more than 1.14 billion people—has an Aadhaar number, a biometrically enabled unique digital identity. This makes Aadhaar the world's largest digital identity programme implemented by a national government. With a handful of exceptions, most Indian states have enrolled more than 80 percent of their residents. Aadhaar's scale has caught the attention of policy-makers globally.

According to the Unique Identification Authority of India (UIDAI), which issues Aadhaar numbers, Aadhaar represents a potentially transformative way for citizens, governments, and businesses to interact with each other. Aadhaar's uses have already achieved significant reach in some areas, as shown in Figure ES.1 below.

Yet, for an identity programme that is increasingly central to India's economy and development efforts, there are gaps in our understanding of Aadhaar's coverage and performance in key areas. There is little publicly available data on Aadhaar's use-cases. As a starting point, a comprehensive catalogue of Aadhaar's public and private sector use-cases did not previously exist. To try and address this data gap, we have compiled an initial list of nearly 600 use-cases available on our website, **StateofAadhaar.in**. Furthermore, there are important open questions on the reach of these use-cases and their performance in improving public service delivery and socioeconomic outcomes. A systematic, multi-disciplinary, and large-scale research effort is critical to build a meaningful understanding of whether, where, and how Aadhaar might advance the public good.

The lack of coherent and comprehensive evidence on the Aadhaar experience provides the motivation for the *State of Aadhaar Report 2016-17*.

The report is organised as follows: we start with an exploration of Aadhaar's technological architecture (Chapter 2) and its legal and governance structure (Chapter 3), both of which provide important context to understand the evolution of Aadhaar's use-cases. In Chapters 4 and 5, we explore two sectors with mature

Figure ES.1: Reach of Aadhaar's enrolment and uses

Aadhaar Enrolment	Authentication	e-KYC	Direct Benefit Transfer	Seeding
1.14 billion	**139 million**	**44.7 million**	**₹22,006 crore ($3.3 billion)**	**167 million**
People enrolled in Aadhaar as of Mar '17	Monthly average of people authenticating themselves using Aadhaar in the latter half of FY 2016-17	Number of bank accounts opened using Aadhaar e-KYC as of Mar '17	Total DBT payments sent using the Aadhaar Payment Bridge System in FY 2016-17	Number of PDS (food subsidy) beneficiary households with at least one member seeded to Aadhaar
85%	**12%**	**<16%**	**33%**	**72%**
of India's population in 2017	of Aadhaar enrollees	of Jan Dhan accounts opened as of Mar '17	of the total DBT expenditure in FY 2016-17	of total beneficiary households

Sources used in this summary include (but are not limited to): UIDAI, DBT portal, DigiLocker dashboard, Gazette of India, NPCI, NSAP, Parliament questions, PDS portals (central and state governments), PMJDY, RBI, Supreme Court archives, TSOnline, and APOnline. Refer to the main report for detailed references.

applications of Aadhaar—financial inclusion and social protection—before concluding with emerging uses in other sectors (Chapter 6). In Chapters 2 through 6, we also highlight policy-relevant research themes for future work. We conclude with thoughts on how policymakers and researchers can engage with this report and our online platform, StateofAadhaar.in (Chapter 7).

Against the backdrop of Aadhaar's rapid growth and evolution, we hope this report enables a holistic understanding of Aadhaar's complex ecosystem and provides a foundation for future research.

Aadhaar architecture

Aadhaar is a unique biometric form of identification, which consists of a 12-digit random number that is tied to an individual's biometric (finger print, iris scan and photograph) and demographic information. Since its inception in 2009, the UIDAI has created the technological and operational architecture to enrol Indian residents. This architecture enables digital authentication of individuals using their biometrics and Aadhaar number.

In Chapter 2, we provide a detailed description of Aadhaar's enrolment and authentication processes, and an overview of Aadhaar-enabled payment systems. We discuss data quality and security features of Aadhaar's technical processes, and how independent research can strengthen their design and implementation.

Legal and governance framework

The legal framework of Aadhaar has evolved significantly since its inception. In 2009, the UIDAI was created using an executive order. Today, the Aadhaar Act 2016 constitutes the legislative framework governing Aadhaar. Aspects of this Act were actively deliberated when the bill was debated in the Rajya Sabha of Parliament. The legal standing of the Act and important aspects of the Aadhaar project—especially its implications for individuals' privacy—are currently under challenge in the Supreme Court of India and await resolution. Research to inform important aspects of legislation—such as on questions of privacy and data security—will be valuable additions to policy, legislative, and judicial dialogue, benefitting Aadhaar and other digital services in India.

Financial inclusion

A growing body of evidence demonstrates the strong positive relationship between access to formal financial services and economic prospects for poor individuals and communities.

As part of the "JAM trinity" of Jan Dhan, Aadhaar, and Mobile, Aadhaar is increasingly integral to the Government of India's efforts to aggressively increase financial inclusion in the country. In the last two and a half years, more than 282 million bank accounts have been created under the Jan Dhan scheme. In roughly the same time period, Aadhaar e-KYC was used to open 44.7 million bank accounts, eliminating the need for other identity documents. In Figure ES.2, we show the growth in e-KYC verifications (to open bank accounts and for other uses).

Aadhaar also powers microATMs, portable point-of-sale devices that can be carried by business correspondents and used to provide banking services at or near one's home, potentially diminishing geographic barriers to financial services for the rural poor. The value of transactions conducted through microATMs, using Aadhaar authentication, grew by 26 times in the past year, from ₹86 crore ($12.8 million) in FY 2015-16 to ₹2,282 crore ($341 million) in FY 2016-17.

Using the foundation of unique identification provided by Aadhaar, payment systems have emerged that attempt to solve different market frictions. The Aadhaar Payment Bridge System (APBS) is used for Direct Benefit Transfers (DBT) from the government to individuals. In FY 2016-17, ₹22,006 crore ($3.3 billion) was transferred using APBS, which was 33 percent of total DBT value in that year.

The Aadhaar Enabled Payment System (AEPS) allows those who live or work far from a bank branch to carry out banking transactions through trusted intermediaries (using microATMs).

Another payment system, Unified Payments Interface (UPI) is a platform that facilitates banking transactions

Figure ES.2: Monthly number of successful Aadhaar e-KYC verifications as per NPCI, Apr 2016 – Mar 2017

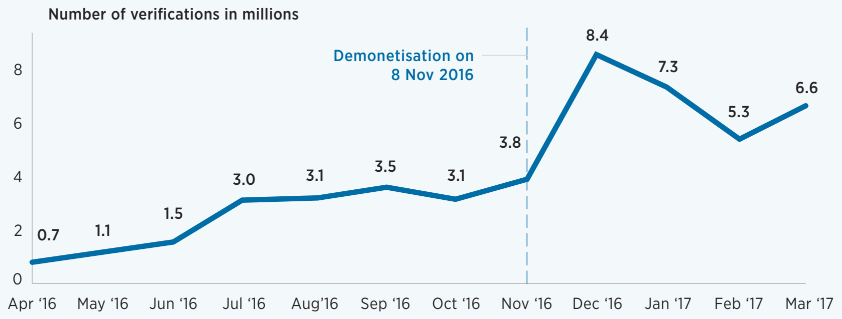
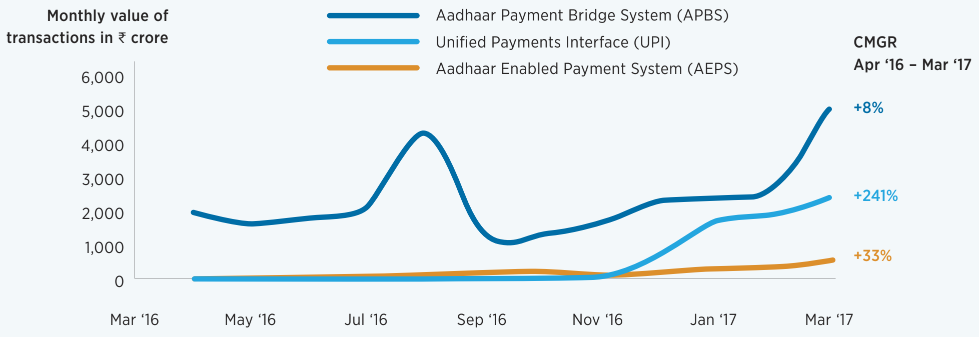


Figure ES.3: Monthly transactions of Aadhaar-enabled systems for payments and transfers, Apr 2016 - Mar 2017



through applications developed for both smart phones and feature phones. About 6.4 million transactions were conducted using UPI, totaling ₹2,425 crore ($362 million), in March 2017.

While growing fast, payments routed using Aadhaar-enabled systems formed only 6.67 percent and 0.06 percent of the total volume and value, respectively, of digital financial transactions in March 2017.

In addition, there are important gaps in our understanding of how Aadhaar is impacting financial inclusion in India. Two themes for research that can aid practitioners today are: a) how best to implement Aadhaar use-cases for financial inclusion, with a particular focus on take-up, efficiency, and infrastructure, and b) the impact of Aadhaar-enabled tools on access and usage of financial services, and consumer welfare.

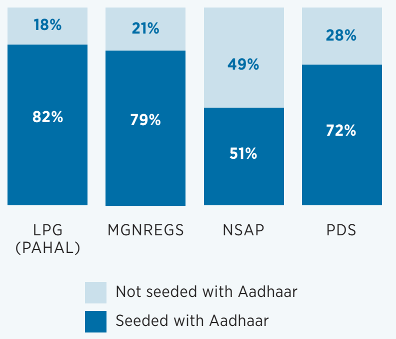
Social protection

We estimate that the Government of India spends more than ₹3 lakh crore ($47 billion) annually on social protection—more than one-sixth of its total budget. It aims to provide robust safety nets to India's poor, including food subsidies, employment guarantees, and direct cash transfers. However, the efficacy of these social protection programmes has been constrained by financial leakages and service delivery inefficiencies.

A majority of the central government's social protection expenditure—more than ₹2.4 lakh crore ($36 billion)—uses Aadhaar in one or more ways. According to UIDAI reports, Aadhaar has the potential to enhance the effectiveness of India's social protection programmes in three ways.

First, fake beneficiaries and duplicates can be removed by linking a person's (unique) Aadhaar number to her or his identity record in each programme's database. About three quarters of the beneficiary names across four major social protection programmes have now been linked to their Aadhaar numbers. See Figure ES.4 for a programme-wise breakdown of Aadhaar seeding. According to the DBT portal, ₹14,000 crore ($2.1 billion) in food subsidies and ₹26,000 crore ($3.9 billion) in cooking gas subsidies were saved, by removing 23 million and 35 million duplicates, respectively. However, the role of Aadhaar in these savings needs to be studied further.

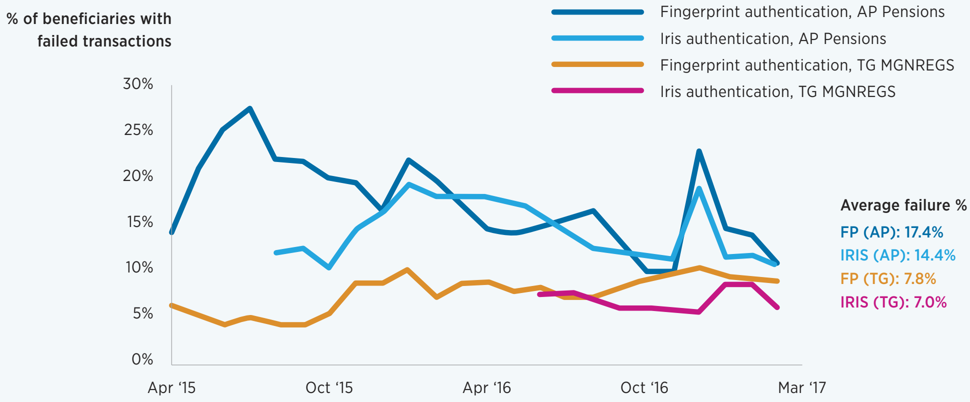
Figure ES.4: Percentage of Aadhaar seeding in four social protection programmes, as of Dec 2016



Second, Aadhaar-enabled electronic transactions can authenticate each beneficiary using her or his biometrics, thus reducing the potential for fraudulent transactions. For example, the Government's largest subsidy programme, the Public Distribution System (PDS), has equipped 186,726 (35 percent) of its shops with electronic point-of-sale (ePoS) machines that are used to authenticate each transaction. Despite this potential, authentication failure rates reported by Andhra Pradesh and Telangana highlight the need for more research to understand and ensure adequate coverage. From April 2015 to March 2017, the pension programme in Andhra Pradesh reported fingerprint authentication failure for 17.4 percent individuals, despite three attempts. Similarly, the failure rate averaged 7.8 percent for the Mahatma Gandhi National Rural Employment Guarantee Scheme in Telangana. We illustrate the failure rate over time in Figure ES.5.

This "failure rate" may include those who were trying to fraudulently access benefits (which is the purpose of authentication). These numbers do not necessarily indicate exclusion as shop owners can use an override facility over Aadhaar's authentication results. However, investigating the true rates of exclusion with and without Aadhaar, and contributing factors, are an important area of future research.

Figure ES.5: Percentage of beneficiaries with failed transactions, after multiple attempts, using fingerprint and iris in Andhra Pradesh and Telangana, Apr 2015 – Mar 2017



Third, Aadhaar enables Direct Benefit Transfers (DBTs) to beneficiary bank accounts, which can reduce siphoning by middlemen as well as payment delays. About 33 percent of all DBTs in FY 2016-17 were made using APBS with the rest relying on older systems such as National Electronic Funds Transfer (NEFT). However, rigorous evaluations are needed to determine whether and to what extent Aadhaar-enabled DBT reduces financial leakages and payment delays.

Despite the growing number of applications of Aadhaar for social protection, there remain key gaps in our understanding of whether and under what conditions Aadhaar can best be utilised to improve social protection in India. Three important themes for future research are: a) representative estimates of whether and how genuine beneficiaries are excluded, in order to design strategies that reduce exclusion, b) research to strengthen implementation (for example, technological preparedness, beneficiary time-use and experience, and connectivity infrastructure), and c) evaluations that examine the impact of Aadhaar use-cases on financial leakages and service delivery, in order to inform decisions on which use-cases to expand.

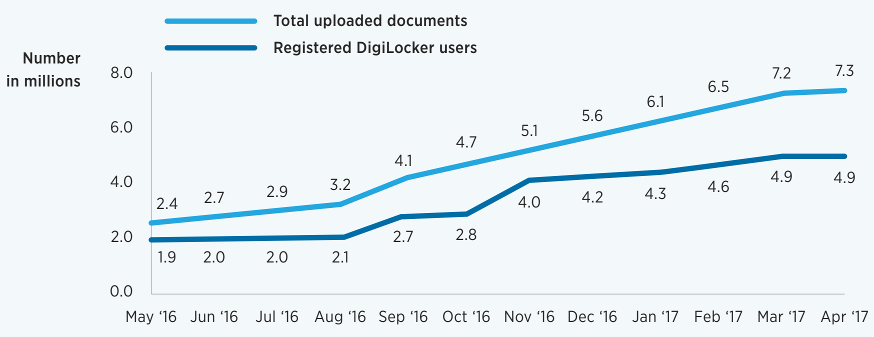
Emerging uses

Along with financial inclusion and social protection, newer uses of Aadhaar are emerging in a diverse set of sectors, including health and education. Several Application Programming Interfaces (APIs) have been developed building off the identity verification provided by Aadhaar. These include DigiLocker ("a platform for digital issuance and verification of documents and certificates") and Electronic Signature (e-Sign). These crosscutting APIs are often referred to as the "India Stack."

As of April 2017, there are about 5 million users of DigiLocker who have uploaded more than 7 million documents (see Figure ES.6). The Central Board of Secondary Education (CBSE) uses DigiLocker to issue students' mark sheets, migration certificates, and passing certificates, and has uploaded more than 11 million documents. E-Sign is also used across many sectors. As of April 2017, nearly 400,000 documents on DigiLocker were signed using e-Sign.

Aadhaar's uses are increasingly being taken up in other sectors as well. In healthcare, Aadhaar is being linked to a Unique Health Identity (UHID), a digital identity issued by healthcare providers to track patients and help secure relevant health documents. The government is trying to improve governance through initiatives like monitoring staff attendance using Aadhaar authentication. In the telecommunications sector, Aadhaar-based e-KYC is being used for real-time and digital verification of subscribers. Private sector start-ups are also beginning to use India Stack elements for uses such as background verification of prospective employees. A more complete list of applications in various sectors is provided in Chapter 6.

Figure ES.6: Cumulative number of registered users and uploaded documents on DigiLocker, May 2016 – Apr 2017



As these new use-cases proliferate, two important themes for future research arise: a) research on the implementation quality of use-cases, especially take-up, efficiency, and infrastructure, and b) evaluations on the impact of Aadhaar-linked uses compared to the counterfactual of non-Aadhaar alternatives.

Looking ahead

Aadhaar enrolment has reached near-universal coverage in most parts of the country, and use-cases continue to evolve and mature. Rigorous empirical evidence is required to develop a more nuanced understanding of Aadhaar's uses and impacts and to provide policy inputs. We hope that the government will proactively share more information, and researchers will work in active collaboration with practitioners. Such a collaborative effort on policy-relevant research can facilitate a clearer understanding of what is working well and what needs to be improved in the Aadhaar space. We hope that such efforts will enable Aadhaar to achieve its stated objective of empowering India's residents.

Table of Contents

Figures

Abbreviations

ABIS	Automatic Biometric Information Systems
AEBAS	Aadhaar Enabled Biometric Attendance System
AEPS	Aadhaar Enabled Payment System
AIIMS	All India Institute of Medical Sciences
APBS	Aadhaar Payment Bridge System
API	Application Program Interface
ASA	Authentication Service Agency
AUA	Authentication User Agency
BC	Business Correspondent
BHIM	Bharat Interface for Money
BSBDA	Basic Savings Bank Deposit Account
CAF	Customer Acquisition Form
CAG	Comptroller and Auditor General of India
CBSE	Central Board of Secondary Education
CIDR	Central Identities Data Repository
CVC	Central Vigilance Commissioner
DBT	Direct Benefit Transfer
EGoM	Empowered Group of Ministers
e-KYC	Electronic Know Your Customer
e-Sign	Electronic Signature
GDP	Gross Domestic Product
HoF	Head of Family
ICDS	Integrated Child Development Services
IEDSS	Inclusive Education of the Disabled at Secondary Stage
IFSC	Indian Financial System Code
JAM	Jan Dhan, Aadhaar, and Mobile
JEE	Joint Entrance Examination
JSY	Janani Suraksha Yojana
KYC	Know Your Customer
LPG	Liquefied Petroleum Gas
MDM	Mid-Day Meal
MeitY	Ministry of Electronics and Information Technology
MGNREGS	Mahatma Gandhi National Rural Employment Guarantee Scheme
MNIC	Multi-Purpose National Identity Cards
NACO	National AIDS Control Organisation
NEET	National Eligibility-cum-Entrance Test
NEFT	National Electronic Funds Transfer
NMMSS	National Means-cum-Merit Scholarship Scheme
NPCI	National Payments Corporation of India
NPR	National Population Register
NSAP	National Social Assistance Programme
NSIGSE	National Scheme Incentives to Girls for Secondary Education
OTP	One-Time Password
PAHAL	Pratyaksh Hanstantarit Scheme
PAN	Permanent Account Number
PDS	Public Distribution System
PIN	Personal Identification Number
PLHIV	People Living with HIV
PMJDY	Pradhan Mantri Jan Dhan Yojana
PoS	Point of Sale Device
RMSA	Rashtriya Madhyamik Shiksha Abhiyan
RRB	Regional Rural Bank
RSBY	Rashtriya Swasthya Bima Yojana
SCB	Scheduled Commercial Bank
SFTP	Security File Transfer Protocol
SPQEM	Scheme to Provide Quality Education in Madrasas
SSA	Sarva Shiksha Abhiyan
UGC	University Grants Commission
UHID	Unique Health Identification Number
UIDAI	Unique Identification Authority of India
UPA	United Progressive Alliance
UPI	Unified Payments Interface

Glossary

Aadhaar

Aadhaar is a 12-digit number provided to eligible applicants. It serves as a unique identification number, that is usually biometrically verified, either using an iris scan or a fingerprint. It is issued by the Unique Identification Authority of India on behalf of the Government of India.*

Aadhaar Enabled Biometric Attendance System (AEBAS)

Aadhaar Enabled Biometric Attendance System (AEBAS) is an attendance tracking platform using Aadhaar at government offices.**

Aadhaar Enabled Payment System (AEPS)

Aadhaar Enabled Payment System is a system for banks to use Aadhaar authentication to provide basic bank account transactions such as balance enquiries, withdrawals, deposits, and transfers. AEPS mostly utilises an Aadhaar-enabled microATM to complete these transactions.§§

Aadhaar Seeding

Aadhaar seeding refers to the linking of each beneficiary's record on an entity's database to their Aadhaar number. Such entities can include government service providers (e.g. PDS, PAHAL, MGNREGS), banks, and hospitals.*

Aadhaar Payment Bridge System (APBS)

APBS is a unique payment system implemented by National Payments Corporation of India (NPCI), which uses an Aadhaar number as a central key for electronically channeling the Government subsidies and benefits in the Aadhaar Enabled Bank Accounts (AEBA) of the intended beneficiaries.§§

Authentication

Authentication refers the process of matching eligible information provided by an Aadhaar number holder with the information stored in the Central Identities Data Repository (CIDR). Authentication information can include the Aadhaar number along with demographic attributes, biometrics, or mobile number.*

Authentication Service Agency (ASA)

ASAs establish connectivity to the CIDR and transmit authentication requests from Authentication User Agencies (AUAs) to the Central Identities Data Repository (CIDR).*

Authentication User Agency (AUA)

AUAs are organisations that use Aadhaar authentication to enable their services. To gain access to the Aadhaar authentication facility, AUAs must enter into a formal agreement with the UIDAI.*

Basic Savings Bank Deposit Account (BSBDA)

Basic Savings Bank Deposit Accounts (BSBDAs) were introduced by the Reserve Bank of India in 2012 after discontinuing the 'no-frills' bank accounts. BSBDAs require that there are no charges for a zero-rupee balance, and that account holders are provided an ATM/debit card.§

Bharat Interface for Money (BHIM)

Bharat Interface for Money (BHIM) is an application that allows users to make simple, easy and quick payment transactions using Unified Payments Interface (UPI). Users can make instant bank-to-bank payments and pay and collect money using just a mobile number or Virtual Payment Address (VPA).§§

Biometrics

Biometric information captured by the UIDAI includes a facial photograph, ten fingerprints, and iris image captured at the time of enrolment of a resident.*

Business correspondent (BC)

Business correspondents (BCs) are retail agents commissioned by banks to provide banking services at locations where bank branches may not exist or are not readily accessible.§

Central Identities Data Repository (CIDR)

CIDR is the data centre where data of residents enrolled is stored and accessed from.*

Source: *UIDAI, **MEITY, §RBI, §§NPCI, †DigiLocker

Central Vigilance Commission (CVC)

CVC is conceived to be the apex vigilance institution, free of control from any executive authority, monitoring all vigilance activity under the Central Government and advising various authorities in Central Government organisations in planning, executing, reviewing and reforming their vigilance work. *Source: CVC Website*

Direct Benefit Transfer (DBT)

Direct Benefit Transfers aim to transfer benefits directly into the bank/postal accounts of beneficiaries. *Source: DBT Portal*

De-duplication

De-duplication is a process by which the biometric and demographic information collected during Aadhaar enrolment is used to verify no duplicate entries are created.[*]

DigiLocker

DigiLocker is an online documents platform that facilitates sharing of documents between government agencies and DigiLocker users. DigiLocker uses Aadhaar eKYC to gather relevant information about its users, and to provide them with additional services, such as retrieving documents from government agencies.[†]

Electronic Know-Your-Customer (e-KYC)

Electronic Know-Your-Customer or, more commonly, 'e-KYC' is a service provided by the Unique Identification Authority of India (UIDAI) which allows a person with an Aadhaar number to share details including name, address, date of birth, gender, phone number, and email after providing consent using a biometric authentication device, or by inputting a one-time-password (OTP) sent to the associated mobile phone number.[*]

Enrolment

Enrolment Agencies are entities hired by UIDAI-appointed Registrars, for enrolment of residents during which demographic and biometric data is collected as per the UIDAI enrolment process.[*]

Enrolment Agency

Enrolment Agencies are entities hired by the Registrars, for enrolment of residents during which demographic and biometric data are collected as per the UIDAI enrolment process.[*]

e-Sign

E-Sign is a service provided by the Controller of Certifying Authorities (CCA). E-Sign provides a way for a person with an Aadhaar number to electronically sign documents after completing an Aadhaar eKYC verification, either by using a biometric authentication device, or by inputting a one-time-password (OTP) sent to the associated mobile phone number. *Source: CCA e-Sign*

India Stack

The India Stack is a set of open Application Programming Interfaces (APIs), which aim to employ India's expanding digital infrastructure to improve service provision for both the public and private sectors. *Source: India Stack*

Indian Financial System Code (IFSC)

Indian Financial System Code (IFSC) is an alpha-numeric code issued by the Reserve Bank of India that identifies the bank name and the branch location. An IFSC code is issued to every bank branch that is included in the National Electronic Funds Transfer (NEFT) system.[§]

JAM Trinity

JAM Trinity stands for Jan Dhan (see Pradhan Mantri Jan Dhan Yojana), Aadhaar, and Mobile. These are the three components emphasised by the Government of India as a means to further financial inclusion of currently excluded communities. *Source: Ministry of Finance*

Know Your Customer (KYC)

Know Your Customer (KYC) is a process by which an entity seeks to gather more information about a potential or existing customer. The KYC process usually involves obtaining proof of address, proof of identification, and a photograph. Banks are required by law to complete this process before opening a bank account for a customer.[§]

Leakage

Leakages are the subsidies/subsidised-goods that don't reach the intended beneficiaries. *Source: Economic Survey 2016-17*

Lok Sabha

Lok Sabha (or House of the People) is the lower house of the Indian parliament. *Source: Lok Sabha*

Source: *UIDAI, **MEITY, §RBI, §§NPCI, †DigiLocker

MicroATMs

A microATM is a portable device that allows individuals to perform financial transactions using only their Aadhaar number and fingerprint as proof of identity. Unlike an ATM, the device is operated by an operator. MicroATMs allow individuals to do the following: deposit funds, withdraw funds, transfer funds, check balance.[*]

Money Bill

A bill may be deemed a Money Bill if it contains provisions dealing with six specific topics, or matters incidental to those topics. The topics include the imposition, alteration, or regulation of taxes, regulations relating to government borrowing, and payments to or from the Consolidated Fund of India. *Source: Constitution of India*

National Payments Corporation of India (NPCI)

National Payments Corporation of India (NPCI) is an independent organisation set up to administer all retail payments systems in India.[§§]

National Electronic Funds Transfer (NEFT)

National Electronic Funds Transfer (NEFT) is a nation-wide payment system facilitating one-to-one funds transfer. Under this scheme, individuals, firms and corporates can electronically transfer funds from any bank branch to any individual, firm or corporate having an account with any other bank branch in the country participating in the scheme.[§]

No-frills bank account

'No-frills' bank accounts were introduced by the Reserve Bank of India (RBI) in 2005 as a way of increasing bank accounts access to a wider population, with an added emphasis on allowing zero- or very low-minimum balance on the accounts at no charge.[§]

NPCI Mapper

NPCI Mapper is a database maintained by the National Payments Corporation of India (NPCI) which stores the Aadhaar numbers of bank account customers, along with their bank information.[§§]

Rajya Sabha

Rajya Sabha (or Council of States) is the upper house of the Indian parliament.
Source: Rajya Sabha

Regional Rural Bank (RRB)

Regional Rural Banks (RRBs) are banks that have a requirement from the Reserve Bank of India to ensure 60 percent of their outstanding advances are to the "priority sector" which the RBI defines as "agriculture and small scale industries".[§]

Registrar

Registrar is an entity authorised or recognised by the Authority for the purpose of enrolling the individuals for UID numbers. 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.[*]

Unified Payments Interface (UPI)

Unified Payments Interface (UPI) is a system that allows the transfer of funds between two parties using mobile phones.[§§]

Unique Health Identification (UHID)

Unique Health Identification (UHID) number is a number assigned to patients on the e-Hospital or the Online Registration System platform.[**]

Unique Identification Authority of India (UIDAI)

The Unique Identification Authority of India (UIDAI) is a statutory authority established under the provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ("Aadhaar Act 2016"). The UIDAI is responsible for Aadhaar enrolment and authentication, including operation and management of all stages of Aadhaar life cycle, developing the policy, procedure and system for issuing Aadhaar numbers to individuals and perform authentication and also required to ensure the security of identity information and authentication records of individuals.[*]

Unique Identity

Unique identity in the context of this report refers to statistically unique identity. Current technology has greater than zero false positive and false negative error rates, though they tend to be small.[*]

Source: *UIDAI, **MEITY, §RBI, §§NPCI, †DigiLocker

1 | INTRODUCTION

More than a billion Indian residents now have a biometric digital identity: Aadhaar. Its use across various sectors is increasing rapidly. This report aims to provide a comprehensive overview of Aadhaar's technological and operational architecture, legal and governance framework, uses in financial inclusion and social protection, and emerging applications in other sectors. This report will also highlight policy-relevant research themes useful for decision-makers in the Aadhaar ecosystem.

One-seventh of humanity has an Aadhaar number, a biometrically enabled unique digital identity issued to Indian residents.[1] With more than one billion enrollees, Aadhaar is the world's largest national digital identity system.[2] Today, about 140 million enrollees use their Aadhaar number every month to digitally authenticate themselves, up by three times from the past year.[3]

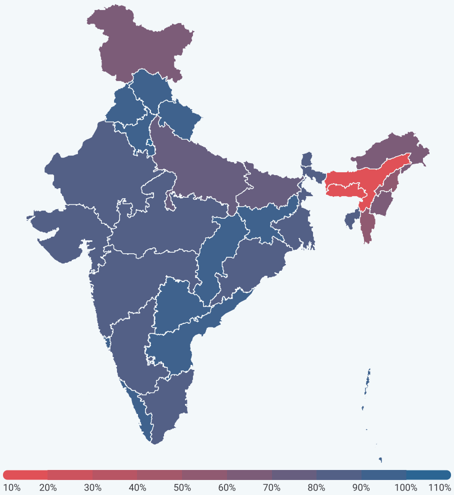
The Unique Identification Authority of India (UIDAI), which issues Aadhaar numbers, would like to use Aadhaar's scale and growth in usage to have a far-reaching impact on India's governance capabilities and socioeconomic prosperity.[4] For example, it enables individuals to open basic bank accounts with only their Aadhaar number and biometrics. By lowering the barriers to account opening, Aadhaar can potentially help Indian residents gain access to India's financial system.[6] Using Aadhaar-enabled systems to route and authenticate direct cash transfers between the government and beneficiaries, the government aims to curb financial leakages and improve the delivery of social protection programmes. And by opening the Aadhaar platform to various public and private sector organisations, the government may encourage innovative applications to improve service delivery in health, education, telecommunications, and a host of other sectors where establishing identity is a key requirement.[7]

The coverage of Aadhaar is increasingly rapidly and has reached varying levels of saturation in different sectors. In terms of financial inclusion, 44.7 million bank accounts have been opened using Aadhaar.[8] This was less than one-sixth of the total basic bank accounts opened in a similar timeframe.[9] Of the total volume of electronic financial transactions during March 2017, 6.7 percent were routed through Aadhaar enabled systems.[10] However, this represented only 0.06 percent of the value of these transactions.[11] Of the electronic transfers from the government to individuals, about 33 percent was routed using Aadhaar-enabled systems in the last half of financial year 2016-17.[12] With regards to social protection, we estimate that the Government of India spends more than ₹3 lakh crore per annum.[13] Programmes covering about two-thirds of this expenditure use Aadhaar in one or more ways. Aadhaar is also increasingly used in other sectors. Of the 558 Aadhaar use-cases we have compiled in our database, 92 are in other sectors. In Figure 1.1, we illustrate the coverage of Aadhaar and the distribution of these 558 use-cases across various use-types and sectors.

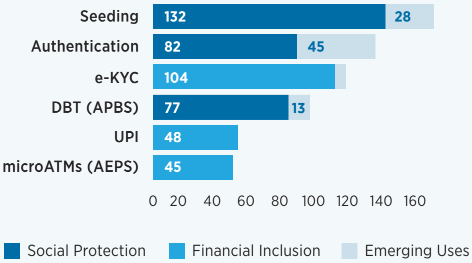
While the potential for Aadhaar's impact may be high, we need to build a stronger understanding of the progress to date on its stated goals. For each of Aadhaar's use-cases—whether it's enabling bank account opening, authenticating a cash transfer, or other innovative applications—it will be useful to answer foundational questions on coverage and performance. On coverage: What is the extent of adoption of a particular Aadhaar use-case? On performance: What are the intended and unintended impacts of the use-case? A clearer understanding of the answers to these questions

Figure 1.1: Overview of Aadhaar

1.14 billion people enroled in Aadhaar; most states with over 80% saturation



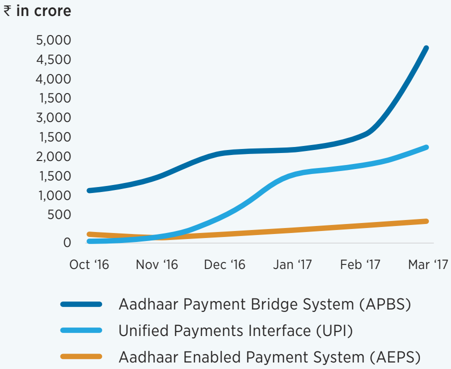
There are 581 use-cases of Aadhaar across India in our database



Millions using Aadhaar to open bank accounts and access financial services

44.7 million	Bank accounts opened using e-KYC by Mar '17; this is <16% of total Jan Dhan accounts opened by that time
400 million	Bank accounts seeded with Aadhaar by Mar '17

Payments using Aadhaar systems APBS, AEPS, and UPI are on the rise

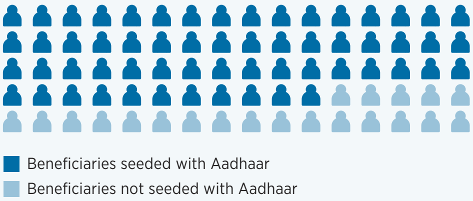


However they are a small portion of total digital financial transactions in India

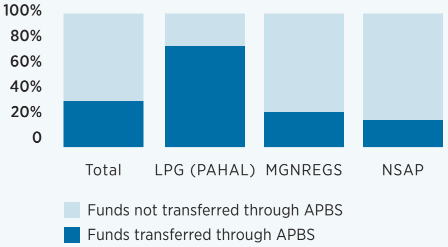
6.67%	Volume of total digital transactions using Aadhaar for Mar '17
0.06%	Value of total digital transactions using Aadhaar for Mar '17

Social protection programmes with a budget of more than ₹2.4 lakh crore per year use Aadhaar in one or more ways

74% of beneficiary names in four major social protection databases are seeded to Aadhaar



33% of Direct Benefit Transfers used Aadhaar for electronic payments in FY 2016-17



Notes: E-KYC stands for electronic Know Your Customer. LPG (PAHAL) is a cooking fuel subsidy; MGNREGS is an employment guarantee programme; NSAP is a pensions programme. The "four major social protection programmes" refer to the PDS (food subsidy programme), LPG (PAHAL), MGNREGS and NSAP. Total budget for programmes using Aadhaar are authors' calculations; see Chapter 5, *Social Protection*, for details.

Data sources: Food and Civil Supplies Annual Report; DBT portal, NPCI, Open Budgets India, PMJDY, RBI, StateofAadhaar.in, and UIDAI per use-case will allow government, civil society, and private sector practitioners to decide whether and how a use-case should be furthered, adjusted, or dropped.

Like all digital identity systems, Aadhaar's technological architecture is open to risks, including gaps in data quality and security of the biometric database. Poor data quality can reduce the ability of the digital identity platform to accurately identify and authenticate individuals, undermining its very premise. Data security breaches, especially of sensitive biometric information, can lead to misuse of identity and violate the terms upon which Aadhaar holders provided data.

It is therefore imperative to have a strong underlying architecture to safeguard against these risks. The UIDAI has built in various measures to control the quality of the biometric and demographic data it collects, and to maintain it securely. More independent research on the efficacy and effectiveness of the UIDAI's data quality and security measures will help it to improve its architecture further, while also providing input to practitioners in other countries planning to build similar national digital identity systems.

The potential for far-reaching positive benefits, alongside significant risks, point to the importance of a robust legal and governance framework for digital identity systems like Aadhaar. The Aadhaar Act 2016[14] lays down provisions governing enrolment into Aadhaar, what personal information can be collected, how it can be used, and how it should be managed to maintain security and confidentiality. Some of these provisions are facing legal challenges in Indian Courts. Given the evolving Aadhaar landscape, regular research can help policymakers test whether and how provisions of the Act can be further strengthened, and what additional legislation may be beneficial. Further, independent inquiry could also review how well the current provisions of the Act are being enforced.

About the Report

Methodology

The *State of Aadhaar Report 2016-17* builds exclusively on secondary research and is based strictly on official reports and public data portals. These sources include reports and data portals from the central and state governments and their various departments, the Parliament of India, the Supreme Court and High Courts, and multilateral institutions such as the World Bank.

This report is not a review of the Aadhaar literature and does not cite research studies. In addition, we also do not quote evidence from journalistic reports. While care has been taken not to omit any important topics related to Aadhaar, the exclusion of these sources is a limitation to keep in mind.

Objectives

The main aim of the *State of Aadhaar Report (SOAR) 2016-17* is to present an objective and comprehensive overview of the expansive Aadhaar landscape. The report covers Aadhaar's technological and operational architecture (Chapter 2), its legal and governance framework (Chapter 3), and its applications in financial inclusion (Chapter 4), social protection (Chapter 5) and emerging uses in other sectors, such as health, education, and telecommunications (Chapter 6). We hope that this report will enable evidence-informed public discourse, decision making in the public and private sectors, and spur future policy-relevant research projects. In Figure 1.2 we provide a guide to reading this report.

Another important aim of this report is to highlight specific policy-relevant research themes for future inquiry. Each chapter in this report ends with a section on future research, laying out the main themes on which more evidence could be useful for decision makers. Further, we highlight the stakeholders that may benefit from such research, and how.

Given the large scale and complicated nature of Aadhaar and its uses, we hope a summative report such as this one provides a much-needed pause to holistically reflect on the evolution of the Aadhaar landscape in the last decade. More importantly, we hope it provides a foundation for the future work to be done by practitioners and researchers in the Aadhaar ecosystem.

Figure 1.2: Guide to reading the *State of Aadhaar Report 2016-17*

The *State of Aadhaar Report 2016-17* is organised into seven chapters, including the present introductory Chapter.

While we encourage readers to read the entire report, each chapter is designed to be a self-contained unit. This enables readers to choose topics that are most relevant or interesting to them. Below, we provide a brief chapter-wise overview of the report.

Chapter 2, on the architecture of Aadhaar, is an overview of Aadhaar's technological and operational backbone. With this chapter, we aim to lay out clearly the nuts and bolts of the Aadhaar identity platform, including how enrolment and authentication take place, how data flows occur, and the safeguards that are built into the current system. We also provide a brief history of the evolution of Aadhaar.

Chapter 3 on Aadhaar's legal and governance framework provides a comprehensive review of the legislation governing Aadhaar, and related issues. In this chapter, we discuss the historical evolution of Aadhaar's legal framework, the current Act that regulates Aadhaar, and the legal challenges pending before the Supreme Court of India.

Chapters 4 and 5 on financial inclusion and social protection, respectively, explore the intersection between Aadhaar and these two sectors. Financial inclusion and social protection have witnessed significant and increasing use of Aadhaar-enabled applications and represent Aadhaar's most advanced use-cases. The chapters provide information on the reach of Aadhaar, its performance and impact on these sectors, and gaps in the current state of publicly available data.

Chapter 6, on emerging uses of Aadhaar, provides an overview of the up-and-coming uses of Aadhaar in various sectors, including health, education, and telecommunications. This chapter also provides information on new Aadhaar-enabled technologies—such as DigiLocker and e-Sign—under the umbrella of 'India Stack'.

We conclude with chapter 7, which lays out the key takeaways of this report and proposes a forward-looking **action plan for researchers and practitioners.**

2 | AADHAAR ARCHITECTURE

With more than 1.14 billion residents enrolled, Aadhaar is the world's largest national digital identity platform. Aadhaar's database and applications are supported by a complex ecosystem of processes and actors. Research can play an important role in strengthening Aadhaar's technical and operational architecture.

An estimated 1.5 billion people around the world cannot prove their identity.[1] Lack of formal identification can deny individuals access to entitlements such as social safety nets, voting rights, and basic financial products. An unidentified population also inhibits the state's capacity for effective governance. Targeted design and delivery of government services rest on a state's ability to identify (who are you?) and authenticate (are you who you say you are?) individuals.[2] Private enterprise, too, relies on establishing identity for the provision of a range of services.

The goals of identity systems—to uniquely identify individuals and to do so efficiently—may be well served by emerging digital technologies. Digital identity platforms have the potential to increase coverage, accuracy, efficiency, and convenience relative to traditional paper-based methods.[3] This potential has led nations across the world—from Germany to Ghana—to adopt digital identity as a key policy instrument.[4,5] At the same time, digital identities also raise important concerns for individuals' privacy and security.[6]

India, too, has seen an evolution in identification systems. Paper-based forms of identification are gradually giving way to digital forms of identity. The most ubiquitous among these is Aadhaar—a digital biometric identity backed by a unique number. With more than one billion residents enrolled, Aadhaar is both the largest form of digital identity in India as well as the largest national digital identity project in the world. Aadhaar is increasingly shaping how individuals and institutions interact in modern India.

In this Chapter, we provide an overview of what Aadhaar is, how it has evolved, the processes and operating systems that enable its uses, and areas of research that are pivotal to the Aadhaar project. With this overview, we aim to fulfil two important functions. One, we provide a granular understanding of the operational aspects of Aadhaar enrolment, authentication, and payment systems. In doing so, we hope to enrich policy research and discussion of Aadhaar's applications, data quality, and security. Two, we provide historical and operational insight into how the world's largest digital identity database was created, and how it operates today. This aims to serve as important background reading for researchers and practitioners involved with Aadhaar's applications. In addition, this Chapter may benefit those researching or working to strengthen Aadhaar's architecture, or those working on developing similar identity systems in other parts of the world.

What is Aadhaar?

Aadhaar means "foundation" in Sanskrit and other Indian languages. It is a unique biometric form of identification backed by a 12-digit random number. The Unique Identification Authority of India (UIDAI)—a statutory authority under the Ministry of Electronics and Information Technology—is responsible for issuing Aadhaar numbers.[7] Every Indian resident[8] is entitled to one. The UIDAI collects residents' demographic and biometric information, and issues unique Aadhaar numbers in turn. There are currently more than 1.14 billion Indian residents in the Aadhaar database, far exceeding the enrolment numbers of other identity databases in India.[9,10]

Aadhaar is distinct from traditional identity systems such as voter identification and ration cards[11] in two important ways: its utility across sectors and use-types, and its underlying technology enabling unique identification. First, it provides a cross-functional proof-of-identity and address, which is valid across states, sectors, and uses. While certain forms of identity such as the ration card are accepted as general proofs-of-identity in India, they were designed to perform a specific function—in this case, to identify individuals to receive a food subsidy. According to the UIDAI, an all-purpose identity proof has the potential to increase user convenience, lower transaction costs for service providers, and reduce the time spent in identity verification.[12]

Second, Aadhaar is designed to employ individuals' biometrics, which are inherently unique.[13] This aids in creating a database with almost no duplicates,[14] and in accurately verifying identities. Most traditional identity platforms in India are paper-based and suffer from varying degrees of duplicate identities.[15] Duplicates in identity databases can be misused to siphon resources from their intended uses.[16] Additionally, paper-based identities are liable to theft and forgery, impeding the accurate authentication of individuals for service delivery. The UIDAI aims to use Aadhaar to plug these gaps.[17]

Evolution of Aadhaar

In the early 2000s, two distinct government identity projects were taking shape. In 2003, the Government of India was contemplating preparing a national register of Indian citizens, and issuing Multi-purpose National Identity Cards (MNICs) based on the registry.[18] This project aimed at collecting a range of demographic and biometric information from individuals to provide a "credible identification system" that could streamline public and private service delivery.[19]

Between 2006-2008, the Registrar General of India (in charge of conducting the national census) was engaged in creating the National Population Register and issuing MNICs. Cards were issued to around 1.2 million citizens in about 12 districts.[20]

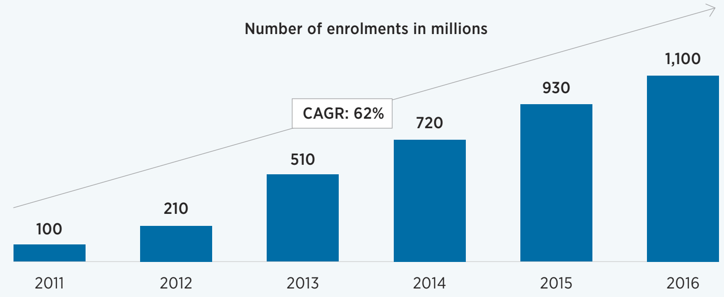
In parallel, the government approved a separate unique identity project for below-poverty-line families in 2006.[21] A vision document was prepared, and a proposal was submitted to the erstwhile Planning Commission (reconstituted as NITI Aayog) for approval.

In recognition of the overlap between the two identification projects, the government constituted an Empowered Group of Ministers (EGoM) to combine the two.[22] Subsequent to the decision of the EGoM, the UIDAI was constituted as the agency responsible for issuing Aadhaar numbers. The UIDAI was established by an executive order in 2009, and initially functioned as an attached office of the Planning Commission.[23]

Aadhaar enrolment began the next year, in 2010. Since then, it has increased steadily, with 85 percent of India's population (roughly 1.14 billion of 1.3 billion individuals) enrolled.[24] In Figure 2.1, we demonstrate the increase in cumulative enrolment in Aadhaar between 2011 and 2016.

As Aadhaar enrolment increased, the legal framework of the project underwent changes. Later in 2010, a few months after the first Aadhaar number was issued, the government introduced legislation to provide statutory backing to the Aadhaar project. The legislation was not passed by Parliament. In 2016, however, the

Figure 2.1: Cumulative enrolment in Aadhaar, 2011 – 2016



Data Source: UIDAI Press Releases

Parliament passed a new legislation called the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act. This established the UIDAI as a statutory authority under the Ministry of Electronics and Information Technology (MeitY).[25]

The UIDAI is headquartered in New Delhi, with eight regional offices across the country. It also has two data centres, located in Bangalore, Karnataka, and Manesar, Haryana. The UIDAI consists of a Chairperson and two Members (functioning on a part-time basis) as well as a full-time Chief Executive Officer (CEO). The Chairperson presides over UIDAI meetings and discharges other functions as may be prescribed. The CEO acts as the legal representative of the UIDAI and is responsible for day-to-day administration. Additional details on the UIDAI and Aadhaar's legal and governance framework are provided in Chapter 3.

Enrolment of Residents

Enrolment ecosystem

The UIDAI conducts Aadhaar enrolment using a tiered model of Registrars and Enrolment Agencies.[26,27] It enters into agreements with Registrars, which are entities recognised by the UIDAI for the purpose of enrolling residents. Registrars are commonly departments of the central or state government, banks, or public sector organisations. An example of a Registrar could be the Rural Development Department of a state government, or a public-sector insurance company such as the Life Insurance Corporation of India. Registrars carry out enrolment themselves, or appoint Enrolment Agencies to do so.

Enrolment Agencies may take two forms: third-party private entities empanelled by the UIDAI based on technical and financial capabilities, or existing offices of the Registrar. Enrolment Agencies receive payment from Registrars for successful Aadhaar generation. These agencies are required to use devices and follow technical processes delineated by the UIDAI. Enrolment Agencies set up Enrolment Centres, which function as touch-points for resident enrolment.

The UIDAI is also meant to partner with civil society organisations and community networks to broaden the reach of these enrolment touch-points and enable enrolment of marginalised populations.[28] As of May 2017, according to the UIDAI, there were 113 Registrars and 482 Enrolment Agencies.[29]

Enrolling residents

To enrol in the Aadhaar database, an individual must provide the demographic and biometric information detailed in Figure 2.2.

Of the requirements listed in Figure 2.2, name, gender, date of birth, and residential address are verified against existing documents. The UIDAI has published a list[30] of acceptable proofs-of-identity, date of birth, and address. An individual's biometrics (fingerprints,

Figure 2.2: Information provided at the time of enrolment

INFORMATION	REQUIREMENT	SOURCE
DEMOGRAPHIC		
Name	Mandatory	Proof-of-identity document
Gender	Mandatory	Proof-of-identity document
Date of birth	Mandatory	Proof-of-date-of-birth document[31]
Residential address	Mandatory	Proof-of-address document
Mobile number	Optional	Self-declared
Email ID	Optional	Self-declared
BIOMETRIC		
Photograph of face	Mandatory	Captured during enrolment
Fingerprints (all 10 fingers)	Mandatory	Captured during enrolment
Iris captures of both eyes	Mandatory	Captured during enrolment

Source: This table is based on the UIDAI's Strategy Overview document.

iris scans, and photograph) are captured at the time of enrolment. In addition to the aforementioned mandatory demographic and biometric information, individuals can optionally provide their mobile telephone number and email ID.

There are avenues to enrol for individuals unable to provide proofs-of-identity. These include being vouched for by a head of family or an appointed "introducer" from one's locality (both of whom must have an Aadhaar number and valid identity documents of their own). A UIDAI response to a Right to Information request[32] from 2015 states that about 219,000 Aadhaar numbers were generated through the introducer facility.[33] This suggests that about 0.02 percent of individuals enrolled as of 2015 did not possess either their own proofs-of-identity and address, or proofs belonging to a head of family, before Aadhaar enrolment.[34]

Whether and how individuals may enrol if they are unable to provide the required demographic or biometric information, the enrolment procedure for children under five, and other enrolment details are presented in Appendix 2.1.

Transfer of enrolment information to the Central Identities Data Repository (CIDR)

Upon enrolment, the personal information of residents must be sent to the CIDR in an encrypted form by the Enrolment Centre supervisor within 20 days.[35] The most common method for transferring data is the Secure File Transfer Protocol (SFTP)—an international benchmark. If this option is unavailable, centre supervisors may send encrypted data to the CIDR on portable hard disks through carriers such as India Post.

De-duplication and issuance of Aadhaar

The CIDR compares the incoming enrolment data of every individual with others enrolled in the Aadhaar database to identify and vet duplicates. This process, known as de-duplication, employs three steps.[36] The goal is to identify genuine duplicates, while minimising false rejection of enrolees (incorrectly denying someone an Aadhaar number on the grounds that she or he is already enrolled).

1. **Demographic de-duplication** is used to identify "trivial duplicates" or cases of duplicates arising from error or ignorance. An example of such a duplicate, as per the UIDAI,

would be an individual who mistakenly re-submits enrolment data at a centre having already done so. Demographic de-duplication is also used for children under the age of five years, as biometric data is not captured for them (see Appendix 2.1 for the enrolment procedure for this age group).[37]

2. **Biometric de-duplication** is the primary method of identifying duplicates. The UIDAI contracts with three vendors that provide automatic biometric identification systems (ABIS), which purportedly improve data accuracy. If one ABIS identifies a duplicate, it has to be verified by another ABIS, thereby increasing accuracy. Additionally, working with three vendors offers greater capacity for de-duplication and Aadhaar generation per day. Finally, the use of multiple vendors ensures that in case an individual vendor must be replaced, the system of de-duplication can continue.

3. **Manual adjudication** takes place if step two has resulted in identifying a duplicate. In this process, the duplicates are checked to assess if a process-related issue has led to the duplication (for example, mixing of enrolment operator and resident biometrics). Finally, each case is analysed manually and a human expert makes the final decision.

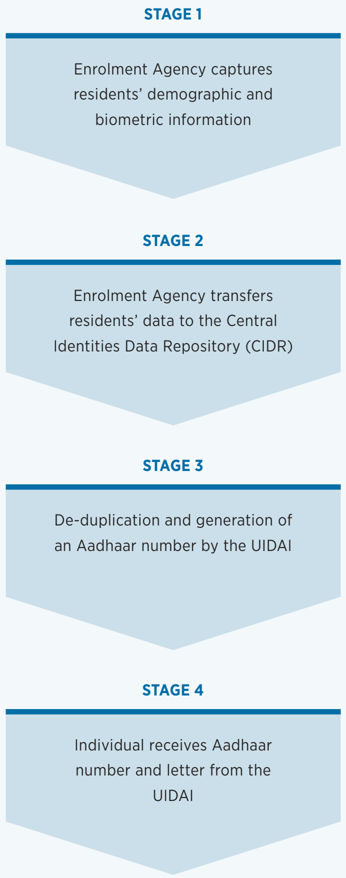
If a resident's data clears the de-duplication process, a 12-digit Aadhaar number is generated.

The CIDR then issues a letter (commonly referred to as an "Aadhaar card") with an individual's Aadhaar number and demographic data and delivers it to the resident. Residents who have submitted their email address during enrolment may also download e-Aadhaar, which contains the same demographic information as an Aadhaar card. The e-Aadhaar also contains the date of Aadhaar generation and date of download, and is digitally signed by the UIDAI. The e-Aadhaar is equivalent to the printed Aadhaar letter delivered by the UIDAI.[38]

If enrolment is unsuccessful, the resident and the enrolling Registrar are informed of the reason for rejection and steps to be taken post-rejection.[39]

In Figure 2.3 below, we summarise the chain of events that must take place for an individual to receive an Aadhaar number from the UIDAI.

Figure 2.3: Steps in Aadhaar enrolment from data capture to resident receiving Aadhaar[40]


STAGE 1
Enrolment Agency captures residents' demographic and biometric information
STAGE 2
Enrolment Agency transfers residents' data to the Central Identities Data Repository (CIDR)
STAGE 3
De-duplication and generation of an Aadhaar number by the UIDAI
STAGE 4
Individual receives Aadhaar number and letter from the UIDAI

Visual adapted from Enrolment Process Essentials, UIDAI

The UIDAI's technical reports and publications provide a high level of detail on the regulations and protocol for each step in the Aadhaar enrolment process. However, we lack rigorous evidence on the execution quality of each step. Systematic analysis of the design and implementation of the various enrolment steps may be an area for future research.

Enrolment Data Quality and Security

The UIDAI has put in place certain measures to strengthen data quality and security at various steps of the enrolment process. Independent assessment of these measures, and research to further strengthen data quality and security, are important areas of future inquiry. These are discussed in the last section of this Chapter.

Data quality

The quality of the Aadhaar database can be assessed by analysing the accuracy of individual data contained within it, as well as the completeness of the database with respect to the target population (which, in the case of Aadhaar, is all Indian residents). Accuracy and completeness can be competing concerns. For example, tightening eligibility criteria for enrolment (such as by requiring pre-existing identity proofs) may increase the accuracy of enrolee data, at the cost of excluding entitled individuals.

The UIDAI constituted two committees in 2009 to review the nature and procedure of the biometric and demographic information to be captured during Aadhaar enrolment.[41] Based on these committees' recommendations, the UIDAI adopted measures to improve the accuracy and completeness of the Aadhaar database. These measures, and any associated evidence, are discussed below.

Accuracy

The accuracy of the Aadhaar database relates to two features: whether all individuals in the database are real and unique persons, and whether the personal information of such individuals is accurate.

Biometric de-duplication (the process of eliminating duplicates using individuals' biometric data) is the main lever for achieving the first measure of accuracy. The UIDAI released performance data for the Aadhaar de-duplication process in 2012, when 84 million individuals had been enrolled. According to this data, the biometric false acceptance rate—the probability that the system erroneously accepts an individual as unique when in fact she or he is a duplicate—was pegged at 0.035 percent.[42] This implies that about 99.97 percent of duplicates submitted to the biometric de-duplication system are correctly identified by the system.

Further, the UIDAI pegged the rate of duplicate submissions at 0.5 percent of all submissions. According to the UIDAI, the false acceptance rate (0.035 percent) combined with the rate of duplicate submissions (0.5 percent) implies that only a small number of duplicates would be falsely accepted at scale. The UIDAI further states that the false acceptance rate remains steady and does not increase with the size of the database.[43]

While the 2012 data released by the UIDAI provides an important indication of the accuracy of the Aadhaar database, these figures would benefit from both updating and regular independent assessments.

A number of UIDAI regulations aim at achieving the second aspect of data accuracy: whether individuals' personal information recorded in the database is accurate. Some measures are detailed below:[44,45,46]

1. The UIDAI has outlined uniform provisions to be followed at every Enrolment Centre, to ensure data is collected consistently. These provisions include standardisation of enrolment devices, data formats, and software.

2. Quality control checks for biometric and demographic data, and consistency of biometric capture, are built into the Aadhaar enrolment software.

3. Enrolment Agencies receive feedback on data quality. According to the UIDAI, consistent feedback to Enrolment Agencies leads them to improve their training and enrolment processes. Enrolment Agencies are incentivised based on the number of successful Aadhaar numbers generated—and not the number of enrolments conducted—to encourage collection of high-quality data.

4. As noted above, individuals have to supply proofs-of-identity and address to verify their demographic information at the time of enrolment.[47]

Figure 2.4: Updating resident information in the CIDR

The UIDAI acknowledges that residents may need to update their demographic data in the Aadhaar database for a variety of reasons, including change of name, address, and contact information (mobile telephone number and email address). In addition, individuals may also need to update their biometric data as a result of changes from accident or injury, or because of authentication failures (discussed later in the Chapter). Children enrolled before the age of five, as well as children enrolling between the ages of five and fifteen, must submit and update biometrics at the ages of five and fifteen, respectively. The UIDAI recommends that all other residents update their biometrics every ten years. Poor quality capture of biometrics or error in capturing demographic data at the time of enrolment may also lead the UIDAI to notify residents to update their data.

Residents can update their data in three ways. Residents with a registered mobile number can update demographic data online by uploading the requisite proofs-of-identity and address. Residents can also update demographic details (except mobile number) by sending a request form by mail. Finally, an individual can update her or his biometric (or demographic) data by visiting a permanent Enrolment Centre.

Source: Aadhaar Data Update, Unique Identification Authority of India

5. A provision exists for individuals to update their demographic and biometric information after enrolment. In addition, the UIDAI may require individuals to do so periodically. See Figure 2.4 for a discussion on updating resident information in the CIDR.

More empirical research on whether, and to what degree, these measures lead to increased accuracy of personal information in the Aadhaar database, compared with other identity databases, would be valuable. Such research might include assessment of how well these provisions are enforced. This can strengthen existing procedures for the UIDAI and guide other national governments looking to build digital identity systems.

Completeness

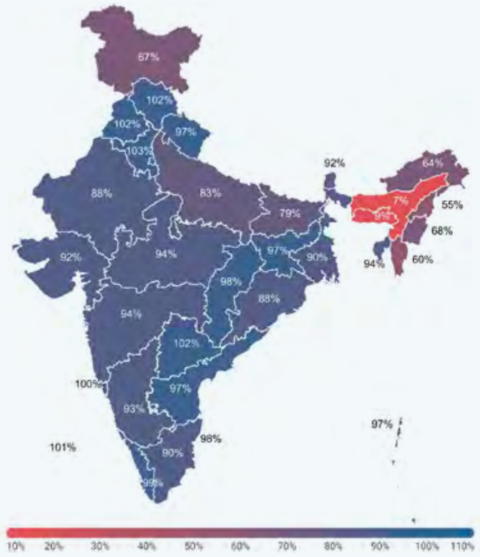
In addition to accuracy, another measure of data quality is the completeness of the database with respect to India's population. While 85 percent of India's population is enrolled, it is useful to examine variation by gender, age, and geography.

Gender: Just over half (52 percent) of total Aadhaar holders are male, which is in line with the country's gender ratio.[48]

Age: The UIDAI data estimates that the adult population is almost fully enrolled and 72 percent of children aged 5 to 18 are enrolled. Less than one-third (31 percent) of children below five are enrolled.[49]

Geography: Twenty-four (of thirty-six) Indian states and Union Territories have 90 percent or more of their populations enrolled in Aadhaar. The three states with the lowest enrolment are Assam (7 percent), Meghalaya (9 percent), and Nagaland (55 percent), all situated in India's north-east region.[50] In Figure 2.5 below, we show Aadhaar enrolment by state and Union Territory.

Figure 2.5: Aadhaar enrolment by state and union territory, as of Mar 2017



Notes: Proportion of population enrolled in Aadhaar for States and Territories calculated using enrolment numbers from March 2017 and projected population totals from 2015
Data Source: UIDAI Public Data Portal

The UIDAI has taken certain measures to reduce entry barriers to Aadhaar:[51,52]

1. All Indian residents are entitled to an Aadhaar number free of cost.

2. Aadhaar employs a decentralised enrolment system that makes use of multiple Enrolment Centres and outreach efforts.

3. The proofs-of-identity and address required from an Aadhaar enrolee may be one of a large number of accepted supporting documents. Eighteen proofs-of-identity and thirty-six proofs-of-address are considered valid for the purposes of enrolment.[53] For individuals lacking such documentation, alternate means of enrolment have been specified (discussed in Appendix 2.1).

4. Individuals who have incomplete biometrics (for example, because of disability or age) are eligible to enrol. As a matter of policy, no individual can be denied Aadhaar even if she or he does not possess usable biometrics.[54] Individuals lacking functional biometrics are meant to be de-duplicated using demographic information and manual adjudication. According to the UIDAI's data, about 99.9 percent of the population possesses biometrics that are sufficient according to Aadhaar requirements.[55] This issue is discussed further in Appendix 2.1.

Independent research on whether, and what, barriers to Aadhaar enrolment remain for individuals who wish to enrol would be useful. This research is of particular importance as difficult-to-access populations such as the homeless, or other marginalised groups, may face higher barriers, and it is pivotal to understand how these can be mitigated. Since Aadhaar increasingly links to a wide range of government benefits for the poor (see Chapters 3, *Legal and Governance Framework,* and 5, *Social Protection,* for details), reducing or eliminating exclusion because of the lack of an Aadhaar number is critical.

An important metric to assess the completeness of the Aadhaar database is the biometric false rejection rate. This refers to the percentage of individuals who will be falsely rejected by the Aadhaar biometric de-duplication system, despite being eligible (that is, unique) candidates. According to the UIDAI, the biometric false rejection rate as measured in 2012 (with 84 million enrolees) was 0.057 percent. All entries identified as duplicates by the biometric system must go through a manual adjudication process, where these errors may be corrected. (In addition, there will be genuine duplicates that will also require manual adjudication). Unlike the false acceptance rate, the false rejection rate is expected to grow linearly as the Aadhaar database expands.[56]

Two counteracting forces must be taken into account when estimating contemporary false rejection rates. Per-day enrolment in the Aadhaar database has fallen from a peak of one million enrolees per day, to an average of about 360,000 enrolments per day in May 2017.[57] This would imply fewer manual adjudications required each day, if false rejection rates were held constant. However, since the last enrolment quality studies were done in 2012, the Aadhaar database has grown from 84 million to 1.14 billion residents. Given that the false rejection rate is expected to grow linearly as the Aadhaar database expands, we can expect an increase in the rate of false rejections. Estimating this rate at current enrolment, and comparing it with those of other large biometric databases or international benchmarks, is an important area for future inquiry. In addition, assessing the UIDAI's capacity to resolve false rejections through manual adjudication is a key area of research to determine the extent of potential exclusion from Aadhaar. These topics are summarised in the final section of this Chapter.

Data security

In addition to the quality of the Aadhaar database, a key consideration is the security of Aadhaar holders' personal information. Below are certain provisions the UIDAI has embedded in the enrolment process to increase data security:[58,59]

1. All enrolment operators and supervisors must have an Aadhaar number to be uniquely identified and for their performance to be analysed.

2. Enrolment data sent from the Enrolment Agency is encrypted and is only decrypted once at the CIDR.

3. Upon reaching the CIDR, enrolment data is decrypted for de-duplication, but decrypted data is not held in storage.

4. The data sent to the ABIS is anonymised; that is, none of the ABIS systems have access to a resident's demographic information.

5. ABIS providers do not store biometric source data; they can only store templates for the purpose of de-duplication.

6. All data is stored in UIDAI storage and cannot leave its premises.

7. The original biometric images of fingerprints, irises, and face are archived and stored offline and are not accessible through an online network.

A 2011 Parliamentary Standing Committee raised concerns regarding the involvement of private sector entities in the data capture and de-duplication stages of the enrolment process.[60] The UIDAI has consistently maintained that it employs best-in-class technologies and rigorous security protocol throughout the enrolment process to ensure data security.[61] Independent assessment of these mechanisms may be an area for future research.

Aadhaar Authentication

The Aadhaar database allows government and private sector entities to authenticate individuals against their Aadhaar records. In this Chapter, we discuss the processes through which Aadhaar authentication functions. In Chapters 4 to 6 *(Financial Inclusion, Social Protection,* and *Emerging Uses)*, we cover a range of authentication applications.

The UIDAI provides two types of Aadhaar authentication services to the public and private sectors. First, there is a "yes/no" authentication facility. Second, there is an electronic Know Your Customer (e-KYC) facility. Both are discussed in the following sections.

Yes/No authentication

Yes/No authentication refers to the process by which an individual's Aadhaar number, along with demographic or biometric information, is submitted to the CIDR for verification. The CIDR checks the correctness, or lack thereof, of the data.[62] The purpose of Aadhaar Yes/No authentication is to provide a digital, online identity platform to validate the identity of Aadhaar holders "instantly, anytime, and anywhere."[63] Both government and private service providers can use this authentication service to verify an individual's identity for the provision of a service. For example, the Food and Civil Supplies Department of a state may require beneficiaries to authenticate themselves using their biometrics and Aadhaar numbers to receive grain under the Public Distribution System (a food subsidy programme).

Aadhaar Yes/No authentication can be performed in three ways:[64]

1. **Demographic authentication** wherein the Aadhaar number and demographic data of the Aadhaar holder is matched with the holder's demographic attributes stored in the CIDR. A "yes" or "no" response is returned, along with other information related to the transaction.

2. **Biometric authentication** wherein the Aadhaar number and biometric data submitted are matched with the biometric attributes of the Aadhaar holder stored in the CIDR. Biometric authentication may be carried out through fingerprint authentication or iris scans. The CIDR returns a "yes" or "no" response, along with other information related to the transaction.

3. **One-time Pin authentication** is when a One-Time Pin (OTP)[65] is sent to the mobile number of the Aadhaar holder as specified in the UIDAI's records. The Aadhaar holder shall provide this OTP along with her or his Aadhaar number during authentication and the same shall be matched with the OTP sent by the UIDAI. As before, a "yes" or "no" response is provided together with any other information related to the authentication transaction.

Multi-factor authentication is a combination of two or three approaches highlighted above. The UIDAI offers five types of authentication services, based on a combination of the three authentication types discussed above. These are detailed in Appendix 2.2. No personal information can ever be returned by the Yes/No authentication process. The process serves only to verify the identity of an Aadhaar holder to a requesting entity.

According to the Aadhaar Act 2016, all authenticating agencies (described in the next section) shall obtain the consent of an individual before collecting her or his identity information, in a manner specified by UIDAI regulations. They are also required to ensure that the identity information of an individual is used only for submission to the CIDR. See Chapter 3, *Legal and Governance Framework* for more information.

Data available from April 2016 to March 2017 demonstrates that the number of Yes/No authentications has increased rapidly during this period. The number of individual Aadhaar numbers authenticated has been increasing as well, albeit less rapidly. This is visualised in Figure 2.6.

Yes/No authentication ecosystem

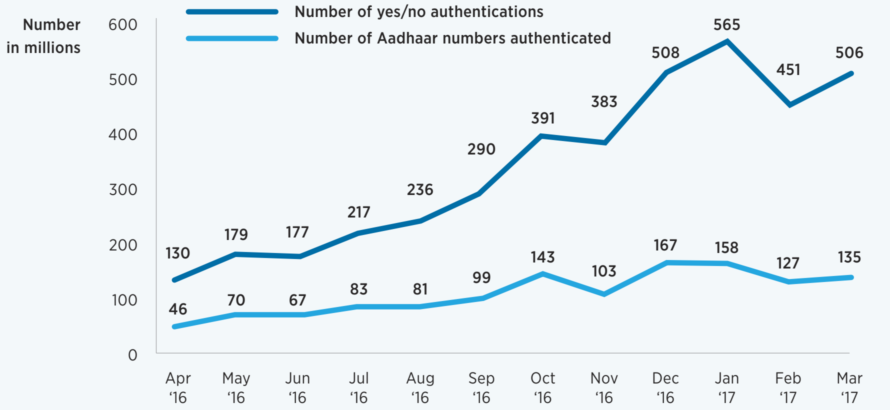
Several stakeholders comprise the Yes/No authentication ecosystem.[66,67] Information flow in the authentication process, and the role of each stakeholder, is discussed below.

UIDAI: The UIDAI functions as the regulator and overseer of the authentication ecosystem. It owns and manages the CIDR, which contains Aadhaar holders' personal information.

Authentication User Agency (AUA): AUAs are organisations that use Aadhaar authentication to enable their services. To gain access to the Aadhaar authentication facility, AUAs must enter into a formal agreement with the UIDAI. AUAs may also submit authentication requests from other entities that are "sub-AUAs." For example, a state government (such as the Government of Himachal Pradesh) may act as an AUA, with several state-level departments and ministries functioning as sub-AUAs. In the private sector, a large bank may establish itself as an AUA, and several small banks may access authentication as sub-AUAs. AUAs and sub-AUAs are commonly referred to as "requesting entities." As of April 2017, there were 352 AUAs in India.[68] The number of sub-AUAs is not publicly available.

Authentication Service Agency (ASA): ASAs establish connectivity to the CIDR and transmit authentication requests from AUAs to the CIDR. In turn, they transmit the CIDR's responses to authentication requests back to AUAs. ASAs build and maintain their connectivity to the CIDR on the basis of specifications and standards laid down by the UIDAI. As an example, a state government's

Figure 2.6: Monthly Aadhaar authentications, Apr 2016 to Mar 2017



Data source: UIDAI Authentication Portal

Information Technology department (for example, Directorate of Information Technology, Government of Maharashtra) could function as an ASA through which several state ministries or departments (AUAs or sub-AUAs) may channel their authentication requests. Similarly, a telecommunications carrier could establish connectivity to the CIDR and act as an ASA for private AUAs. An ASA may serve more than one AUA, and one AUA may choose to access Aadhaar authentication through multiple ASAs. An AUA could also choose to become its own ASA. As of April 2017, there were 27 operating ASAs in India.

Authentication devices: These devices collect personal information from Aadhaar holders, encrypt and transmit this data, and receive authentication results. They include personal computers, handheld devices, and kiosks. These are used and managed by AUAs or sub-AUAs.

Aadhaar holders: Aadhaar holders are individuals whose identity may be authenticated for service delivery.

Figure 2.7 below visualises the flow of information during the Yes/No authentication process.

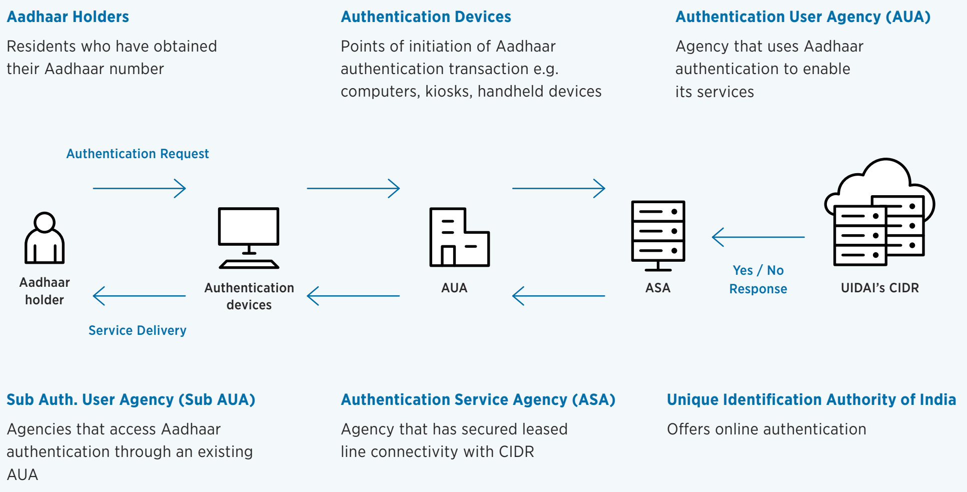
e-Know Your Customer (e-KYC)

The second type of authentication service provided by the UIDAI is Aadhaar-enabled e-KYC. This service authenticates an individual's identity and provides additional demographic details. Certain service providers—such as those in the banking industry—require individuals to provide proofs-of-identity, address, and other demographic information before they can receive services. For these, Aadhaar-enabled e-KYC provides an instant, electronic, and undeniable proof-of-identity, address, date of birth, and gender. In addition, it provides the resident's mobile number and email address to the requesting agency. KYC data can only be provided upon authorisation by an Aadhaar holder, through biometric or OTP-based Aadhaar authentication.

e-KYC ecosystem

Analogous to AUAs, KYC User Agencies (KUAs) are organisations that have access to the e-KYC service. KUAs gain access to e-KYC services through KYC Service Agencies or KSAs (analogous to ASAs). The flow of information for e-KYC is the same as that for Aadhaar authentication. As of April 2017, there were 274 registered KUAs in India.

Figure 2.7: Information flow and stakeholders involved in Aadhaar Yes/No authentication[69]



Aadhaar Holders
Residents who have obtained their Aadhaar number

Authentication Devices
Points of initiation of Aadhaar authentication transaction e.g. computers, kiosks, handheld devices

Authentication User Agency (AUA)
Agency that uses Aadhaar authentication to enable its services

Sub Auth. User Agency (Sub AUA)
Agencies that access Aadhaar authentication through an existing AUA

Authentication Service Agency (ASA)
Agency that has secured leased line connectivity with CIDR

Unique Identification Authority of India
Offers online authentication

Visual adapted from Aadhaar Authentication Overview, UIDAI

Between December 2012-2015, more than 35 million Aadhaar holders used the UIDAI's e-KYC authentication service.[70]

Authentication Quality and Security

The quality of Aadhaar authentication mechanisms is a critical factor determining individuals' access to services that require authentication—increasingly, a large number of government programmes. The UIDAI has also put in place technical safeguards to increase the security of authentication transactions. Both authentication quality and security would benefit from policy-oriented research, discussed below and in the last section of this Chapter.

Authentication quality

Of the three (biometric, demographic, and OTP-based) mechanisms of authentication, data on biometric authentication is most widely reported.

The UIDAI conducted a series of studies in five Indian states[71] in 2011-2012 to determine the technological systems and processes that would enable the highest possible quality of biometric authentication. They found that identifying a finger that produces the best matching result for every resident (known as "best finger") would ensure greater authentication accuracy than standardising one finger (for example, the right index finger) for all residents to use.

Further, the UIDAI determined that employing a system of identifying two "best fingers" for each resident, and allowing up to three authentication attempts, would ensure that only about 1 percent of individuals would be falsely rejected during authentication despite having valid biometrics.[72]

Available data from government social protection programmes in Andhra Pradesh and Telangana (two southern Indian states) reveals that on average about one in seven individuals faced authentication failures in 2016-17 after multiple attempts.[73] The transaction failure statistics may point to genuine beneficiaries being falsely rejected (for reasons such as poor capture of biometrics at the time of enrolment, change in biometrics over time, or infrastructure-related problems such as connectivity) or fraudulent authentication attempts. Individuals who face transaction failures may still receive services as paper-based authentication systems can be used to manually override the digital transaction.[74] A more detailed discussion of this data is presented in Chapter 5, *Social Protection*.

Detailed inquiry into authentication accuracy, rates of failure (including false rejections), and systems for handling authentication failures for genuine beneficiaries are critical areas of research. Since millions of beneficiaries of government programmes interact with these systems regularly, administrators would benefit from understanding how to reduce these failure rates, or fall back on more appropriate alternatives. These issues are discussed further in the closing section of this Chapter.

Authentication security

In addition to the quality of Aadhaar authentication, the security of Aadhaar holders' information transmitted through the authentication process is an important consideration. The UIDAI lists technical regulations to increase the security of (biometric and non-biometric) authentication transactions.[75,76]

1. All requesting entities must use certified biometric devices and software, conforming to regulations laid down by the UIDAI.

2. All identifying information received from individuals (including Aadhaar number, biometric or demographic information) must be encrypted after collection, and before transmission to the requesting entity's server.

3. All authentication requests must be digitally signed by the AUA or ASA.

4. The UIDAI allows Aadhaar holders to "lock" their biometrics. All authentication attempted using biometrics that have been locked by an Aadhaar holder receive a "No" response. A user may

unlock her or his biometrics temporarily when attempting authentication. This measure is designed to prevent anyone other than an Aadhaar holder from being able to fraudulently conduct authentication on the holder's behalf.

Independent and recurring studies of whether and to what degree technical safeguards for data security are upheld in the authentication process may be an area of future research.

Payment systems

In addition to its authentication feature, Aadhaar enables two types of payment systems. These are discussed below.

Aadhaar Enabled Payment System (AEPS)
AEPS employs the UIDAI's authentication services to allow residents to conduct banking transactions using only their Aadhaar number and biometrics.[77,78] Business correspondents, or agents employed by banks, conduct door-to-door banking through the use of microATMs (handheld devices that can execute banking transactions).[79] Aadhaar holders can provide their Aadhaar number, identify their bank, and provide their fingerprint to obtain access to Aadhaar-enabled banking services such as balance enquiry, cash withdrawal and deposit, and fund transfer between Aadhaar holders. The Aadhaar holder's biometric information is sent to the CIDR for authentication. The CIDR responds with a "yes" or "no" response. If the authentication response is "yes," the bank carries out the required transaction.

An Aadhaar holder's bank account must be linked to her or his Aadhaar number to gain access to Aadhaar-enabled banking services. For a more detailed discussion on AEPS, see Chapter 4, *Financial Inclusion.*

Aadhaar Payment Bridge System (APBS)
APBS is used for the disbursal of government benefits using Aadhaar numbers. Various government departments that provide subsidies and monetary entitlements to Indian residents make use of APBS to channel beneficiary payments. Similar to AEPS, APBS requires beneficiaries' Aadhaar number to be linked to a bank account. APBS is discussed in further detail in Chapter 4, *Financial Inclusion.*

Areas for Future Research

As discussed in later Chapters, Aadhaar's applications are growing. Understanding and strengthening Aadhaar's technical architecture is an important step towards improving how Aadhaar functions for individual users, private sector players, and government stakeholders. The strengths and risks of Aadhaar's architecture could also provide useful lessons for countries across the world building digital identity systems of their own.

Research on Aadhaar's architecture would be valuable for policymakers at the UIDAI, as well as users of Aadhaar-based services such as authentication and e-KYC. Technological and operational research focused on strengthening Aadhaar's systems and processes could a) improve Aadhaar's coverage and prevent inadvertent exclusion, b) strengthen Aadhaar authentication, and c) augment the accuracy and security of the Aadhaar database.

Four research themes encapsulate these objectives:

- Research on preventing inadvertent exclusion through Aadhaar's enrolment processes; assessing barriers (if any) to enrolment, exclusion due to insufficient demographic or biometric information, and false rejection from the Aadhaar database

- Assessment of Aadhaar authentication quality, including authentication devices, operating processes guiding information flow, and user experience and outcomes, to streamline authentication-based service delivery

- Research on the accuracy of Aadhaar's database; updated measurement of the false acceptance rate and the rate of duplicates enrolling, and mechanisms to improve the accuracy of enrolled individuals' personal data

- Assessment of the data security provisions in Aadhaar enrolment and authentication to protect Aadhaar holders' personal information

In addition to the research agenda above, regular release of data by the UIDAI on Aadhaar's performance relating to each theme above will provide valuable information on how to continually improve Aadhaar's architecture.

To maximise the impact of practitioner-oriented research, we recommend:

- **Framing research questions in collaboration with practitioners**
- **Being responsive to decision-making schedules and other practitioner constraints**
- **Presenting insights in succinct documents and in-person meetings**
- **Providing follow-up support to translate research to action on-the-ground**

APPENDIX 2.1: Aadhaar Enrolment Process

To enrol for an Aadhaar number, individuals are required to provide certain demographic and biometric information (detailed in Figure 2.2, reproduced below).

In case an individual does not possess valid forms of proof-of-identity and proof-of-address documents, she or he may provide a Certificate of Identity or a Certificate of Address issued by a government-approved authority. Since a large number of Indian residents do not possess a valid proof-of-date-of-birth, the UIDAI allows three types of records. A "verified" date of birth is recorded based on valid documentary evidence. A "declared" date of birth is one wherein the enrolee is aware of her or his date of birth but does not have supporting evidence. Finally, an "approximate" date of birth is recorded when the two procedures above are inapplicable. This date of birth is meant to be estimated and ascertained by trained enrolment operators.[80]

There are also two alternative methods for cases where individuals cannot furnish valid documents, and a separate procedure for children under the age of five. First, an individual may be enrolled using the Head of Family (HoF)-based system. In this method, the head of a family can vouch for the identity and address of her or his family members. The Head of Family must be enrolled in Aadhaar, with valid proof-of-identity and address documents. The enrolee also needs to provide a document serving as a proof of her or his relationship with the Head of Family.[81] Second, an individual may also be enrolled through the introducer system. An introducer is appointed by the Registrar and is entrusted to vouch for the identity and address of an enrolee in her or his locality. An introducer must possess a valid Aadhaar number, which is submitted during enrolment to ensure traceability.[82]

In the case of children below the age of five, one of either the parent's or guardian's names and Aadhaar numbers (or enrolment numbers) must be recorded.[83] A child cannot be enrolled until her or his parent or guardian has been enrolled. Children below the age of five do not have to supply biometrics at the time of enrolment. Upon reaching the age of five, they are required to re-enrol, and provide biometric data. If accepted into the Aadhaar database after the

Information provided at the time of enrolment

INFORMATION	REQUIREMENT	SOURCE
DEMOGRAPHIC		
Name	Mandatory	Proof-of-identity document
Gender	Mandatory	Proof-of-identity document
Date of birth	Mandatory	Proof-of-date-of-birth document[31]
Residential address	Mandatory	Proof-of-address document
Mobile number	Optional	Self-declared
Email ID	Optional	Self-declared
BIOMETRIC		
Photograph of face	Mandatory	Captured during enrolment
Fingerprints (all 10 fingers)	Mandatory	Captured during enrolment
Iris captures of both eyes	Mandatory	Captured during enrolment

Source: This table is based on the UIDAI's Strategy Overview document.

de-duplication procedure, the child retains the same Aadhaar number.[84]

A procedure is specified for cases in which an individual is not able to supply biometric information (for example, because of physical disability). A note is made of any mandatory biometric information that cannot be collected and a photograph is taken with a complete view of the missing biometrics, as evidence.[85] An inability to supply biometric information cannot be grounds to deny enrolment.

Operators at Enrolment Centres are required to record residents' consent for sharing their personal data, as well as for enrolling in Aadhaar. In addition, they are required to show enrolees the demographic data being recorded in the database for them to validate it. Copies of all documents received from an enrolee during the enrolment process, along with her or his enrolment form, are stored at the Enrolment Centre. These copies are then sent for permanent storage to the Registrar.[86] At the end of the process, enrolees receive a 14-digit enrolment number, which serves as proof of enrolment and can be used to check the status of application.

APPENDIX 2.2:
Forms of Aadhaar Authentication

The UIDAI allows Aadhaar authentication to be performed in three ways: demographic, biometric, and One-Time Pin authentications.[87] Combinations of these three authentication methods form five distinct authentication services.[88]

1. Type 1 Authentication: This consists of purely demographic authentication. An individual's Aadhaar number and demographic data are matched with her or his demographic attributes stored in the CIDR.

2. Type 2 Authentication: This consists solely of One-Time Pin (OTP) authentication. A One-Time Pin is sent to the registered mobile number of an Aadhaar holder, and is matched with the OTP sent by the UIDAI. This form of authentication may be used in locations where deployment of biometric authentication is not feasible.

3. Type 3 Authentication: This refers to single-factor biometric authentication. That is, either the fingerprint or iris scan of an Aadhaar holder is collected and matched with her or his biometric attributes stored in the CIDR.

4. Type 4 Authentication: This is a combination of types 2 and 3, wherein residents are authenticated based on single-factor biometric authentication as well as OTP-based authentication. The combination of biometric and OTP (two-factor) authentication is intended to provide a higher degree of authentication assurance.

5. Type 5 Authentication: This refers to three-factor authentication, wherein an Aadhaar holder is authenticated using finger print, iris scan, and OTP authentications. This form provides the greatest degree of authentication assurance.

3 | LEGAL AND GOVERNANCE FRAMEWORK

The legal framework of Aadhaar has evolved significantly since its inception in 2009. The Aadhaar Act 2016 constitutes the current legislative framework governing Aadhaar. Aspects of this Act and the Aadhaar project have been challenged in the Supreme Court and await resolution. These challenges—including the question of a right to privacy—inform important areas of future research.

Aadhaar's legal and governance framework has been the subject of keen interest throughout the project's eight-year history. Since Aadhaar's conception in 2009, its legal framework has undergone significant change. Currently, the Aadhaar Act 2016[1] and subsequent regulations govern the use of Aadhaar in public and private applications. Together they prescribe procedures for the collection, transfer, maintenance, and sharing of personal information under Aadhaar. In addition, notifications issued by several central and state government ministries also regulate the use of Aadhaar in public service delivery.

Over the years, several aspects of Aadhaar have been contested in court and await final resolution. These challenges may have far-reaching impact, including the determination of whether India's Constitution affords a right to privacy and what the nature and limitations of such a right may be.

In this Chapter, we trace Aadhaar's legal evolution, discuss important features of the Aadhaar Act 2016, and outline associated legal challenges. Together with Aadhaar's technical architecture (discussed in Chapter 2, *Aadhaar Architecture*), a better understanding of Aadhaar's governing framework can aid engagement with its use-cases in financial inclusion, social protection, and other emerging areas.[2] The Chapter concludes with suggestions for future research to inform improved policy.

Legal History

Aadhaar was created through an executive order in 2009. Legislation governing Aadhaar was introduced twice—in 2010 and 2016—and passed the second time in the form of the Aadhaar Act 2016. In the interim years, enrolment into Aadhaar continued to grow. The Supreme Court of India has also issued several directives on Aadhaar's permissible uses. The history of Aadhaar's conception, passage of supporting legislation, and associated judicial verdicts are discussed below.

Legislative history

The United Progressive Alliance (UPA) government created the Unique Identification Authority of India (UIDAI) through an executive order on 28 January 2009.[3] The creation of the UIDAI capped several years of movement towards a national identity project in India.[4] Housed under the erstwhile Planning Commission,[5] the UIDAI was envisioned as a pan-departmental agency responsible for issuing a unique identifier — Aadhaar — to every Indian resident. The first Aadhaar number was issued on 29 September 2010.[6]

Two months into the enrolment process, on 3 December 2010, the government introduced the National Identification Authority of India Bill in Parliament to provide statutory backing for the Aadhaar project. This bill sought to establish a "National Identification Authority of India" and specified regulations on the collection, storage, use, and disclosure of individuals' personal information under Aadhaar. The bill was referred by the Lok Sabha (Lower House) to the Standing Committee on Finance (2011-12).[7] The committee raised objections to Aadhaar's conception, design, implementation, and potential outcomes. It recommended that the government reconsider the scheme and introduce a new bill. It also described the executive's issuance of Aadhaar numbers, while lawmaking related to Aadhaar was under way, as "unethical" and in violation of Parliament's prerogatives.[8] A fuller discussion of the concerns expressed in the 2011 Standing Committee report is presented later in this Chapter. Official amendments to the Bill were proposed to be moved in 2013, but were not passed.[9]

The next attempt to formalise the Aadhaar project in law came with the introduction of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Bill 2016 (henceforth referred to as the "Aadhaar Bill" or "Aadhaar Act" as relevant). The bill was introduced in Parliament in March 2016 by the Finance Minister of the National Democratic Alliance (NDA) government. The Act specified that the government could require individuals to possess an Aadhaar number or undergo Aadhaar authentication for the receipt of government benefits financed from the Consolidated Fund of India,[10] in addition to objectives outlined by the previous bill.[11]

The Aadhaar Bill 2016 was introduced as a Money Bill.[12] The Rajya Sabha (Upper House) may suggest amendments to Money Bills, but the Lok Sabha is not bound by them. In this case, the Rajya Sabha suggested five amendments on 16 March 2016. In accordance with the Lok Sabha's powers, it passed the bill without accepting the amendments. The Act came into effect on 12 September 2016 and constitutes

Figure 3.1: What is a Money Bill?

According to the Indian Constitution, a bill may be deemed a Money Bill if it contains only provisions dealing with six specific topics, or matters incidental to those topics. The topics include the imposition, alteration, or regulation of taxes, regulations relating to government borrowing, and payments to or from the Consolidated Fund of India. A Money Bill can only be introduced in the Lok Sabha. After it has been passed by the Lok Sabha, it is transmitted to the Rajya Sabha for its recommendations. The Lok Sabha may thereafter accept or reject any or all of the Rajya Sabha's recommendations. If the Lok Sabha does not accept any of the recommendations of the Rajya Sabha, the Money Bill is deemed to have passed in the form in which it was initially passed by the Lok Sabha.

Source: Constitution of India

the current legal framework governing Aadhaar (alongside the regulations and notifications enlisted in Appendix 3.1). Between September 2010 (when the first Aadhaar number was issued) and 2016, the UIDAI continued to issue Aadhaar numbers on the basis of the 2009 executive order.

Other Acts of Parliament can shape the usage of Aadhaar as well. For example, the Finance Act 2017 made Aadhaar a requirement for filing income tax returns, and applying for and retaining a Permanent Account Number (the identification issued by India's Income Tax Department).[13]

The requirement of Aadhaar for tax returns, and the introduction and subsequent passing of the Aadhaar Bill as a Money Bill have been challenged in the Supreme Court. These issues are taken up in the last section of the Chapter.

Judicial history

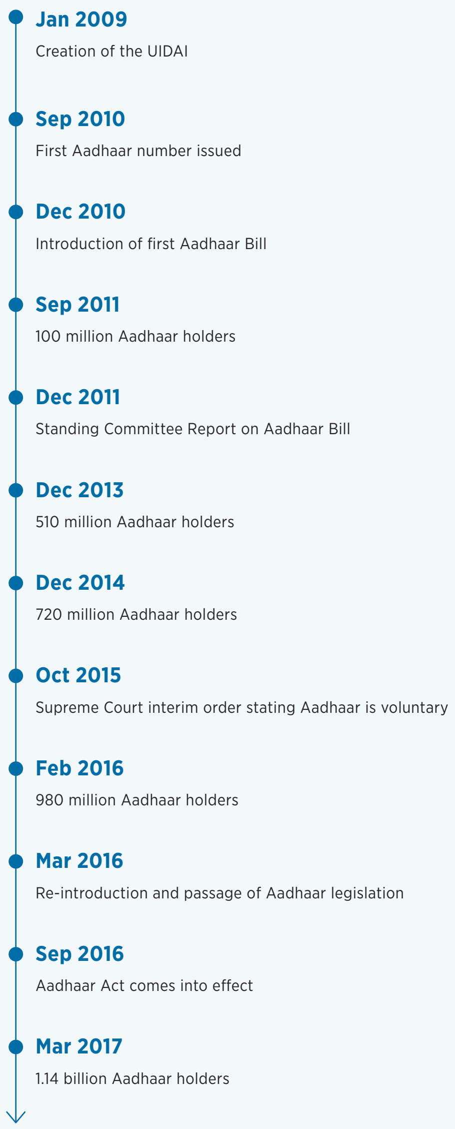
Petitions challenging the legality of the Aadhaar project have been filed before several Indian High Courts and the Supreme Court of India. In this Chapter, we will focus on petitions before the Supreme Court. While these cases await resolution, the Supreme Court issued directives in 2013, 2014, and 2015, emphasising that Aadhaar could not be made a condition for the receipt of government benefits, and that possession of an Aadhaar number must be voluntary.[14,15,16]

In an interim order in 2015, the Supreme Court stated that Aadhaar could not be used for any purpose other than for two schemes pertaining to food and cooking fuel subsidies.[17] In a later order in the same year, the Supreme Court expanded this list of schemes to include government programmes relating to an employment guarantee, cash transfers to the poor, opening bank accounts, and savings for retirement.[18] It further directed that enrolment into Aadhaar is "purely voluntary" and cannot be made mandatory until the matter is decided by the Court.[19]

In parallel, several government ministries have issued circulars requiring Aadhaar for the receipt of benefits and allowing its use in schemes other than those specified by the Supreme Court. Both before and after the passage of the 2016 Act, Aadhaar has increasingly been made compulsory for a wide range of government schemes and benefits.[20,21,22,23] In addition, it is now required for the filing of income tax returns.[24] Meanwhile, the Supreme Court has yet to hear a batch of petitions raising concerns about the legality of the Aadhaar project and Aadhaar's use in government service delivery.

In Figure 3.2, we illustrate key events in the legislative and judicial evolution of Aadhaar.

Figure 3.2: Timeline of Aadhaar's evolution



Jan 2009
Creation of the UIDAI

Sep 2010
First Aadhaar number issued

Dec 2010
Introduction of first Aadhaar Bill

Sep 2011
100 million Aadhaar holders

Dec 2011
Standing Committee Report on Aadhaar Bill

Dec 2013
510 million Aadhaar holders

Dec 2014
720 million Aadhaar holders

Oct 2015
Supreme Court interim order stating Aadhaar is voluntary

Feb 2016
980 million Aadhaar holders

Mar 2016
Re-introduction and passage of Aadhaar legislation

Sep 2016
Aadhaar Act comes into effect

Mar 2017
1.14 billion Aadhaar holders

Aadhaar Act 2016: Salient Features

This section discusses some key features of the Aadhaar Act 2016. We also highlight features that interact with the 2011 Standing Committee's report on the 2010 Bill. Amendments to the 2016 Bill suggested by the Rajya Sabha (but not passed by the Lok Sabha) are also presented.

Eligibility and enrolment

The Aadhaar Act allows for the issuing of Aadhaar numbers to all Indian residents (individuals residing in-country for 182 days or more in the year before application). Aadhaar cannot be proof of citizenship or domicile.

The 2011 Standing Committee report expressed concern that illegal immigrants would be able to obtain an Aadhaar number, posing risks to national security and allowing them access to government benefits. The Committee expressed concerns about the security of the "introducer" system and entrusting the responsibility of verifying Aadhaar applicants' personal information to Registrars (discussed in Chapter 2, *Aadhaar Architecture*). It asserted that the complete verification of information of all Aadhaar holders seemed infeasible on a practical basis, and that the possibility of illegal residents possessing Aadhaar numbers through false affidavits or inaccurate introductions could not be ruled out.

Finally, the committee noted that while Aadhaar could provide a proof-of-identity, it could not by itself determine eligibility for receiving government benefits. As things stand, while all residents are eligible for an Aadhaar number, muster rolls (beneficiary lists) are maintained by the relevant government departments implementing a particular scheme or service. Aadhaar can serve as a proof-of-identity or residence while accessing government services, but does not determine eligibility for these services.[25]

Collection of personal information

The Act defines the information that may be collected for the issuance of an Aadhaar number. Currently, this includes biometric (photograph, fingerprint, and iris scan) and demographic (name, date of birth, and address) information. In addition, the UIDAI can specify other biometric and demographic information to be collected through regulations. These regulations have the status of delegated legislation.[26] The Act specifies that information pertaining to "race, religion, caste, tribe, ethnicity, language, records of entitlement, income, or medical history" cannot be collected.

The 2011 Standing Committee report noted that it may be beyond the scope of the Aadhaar legislation to link biometric information with personal information without amending the Citizenship Act 1955 or Citizenship Rules 2003. It recommended this issue be examined in detail by Parliament. In addition, it also identified as concerns the duplication of effort by other government bodies collecting personal information and the continuance of other forms of proof-of-identity and address. No amendments pertaining to Aadhaar have been made to the Citizenship Act 1955 or Citizenship Rules 2003 since the creation of the UIDAI. The impact of Aadhaar on the collection of personal information by different government agencies is a potential area of further research.

Use of Aadhaar

The Act allows for both government and non-government use of the Aadhaar platform.

Government use

The Aadhaar Act specifies that the government can require an individual to have an Aadhaar number for the purpose of receiving a subsidy or service. As noted above, the Supreme Court issued directives in 2013, 2014, and 2015, stating that the lack of Aadhaar identification cannot be grounds for denial of government subsidies and services. The Rajya Sabha passed an amendment allowing for the receipt of government benefits even if an individual chooses not to opt for Aadhaar enrolment.[27] However, this amendment was not passed by the Lok Sabha, and is therefore absent from the current legislation governing

Aadhaar. The Supreme Court is hearing cases that may have implications on the use of Aadhaar for provision of subsidies and other services.

Private Use

The Act allows for private sector use of Aadhaar. Any public or private entity may use Aadhaar to establish the identity of an individual. The same data protection and consent provisions (enumerated in the section below) apply to private and public entities alike. The Rajya Sabha passed an amendment to delete the provisions allowing for private and non–governmental applications of Aadhaar, which was not accepted by the Lok Sabha. Today, Aadhaar is being used by several private sector entities for uses ranging from e-KYC for SIM card issuance to background verification of potential employees, as detailed in Chapter 6, *Emerging Uses*.

Information management

The Act specifies provisions governing the collection and use of individuals' personal information.

Data collection and storage

Enrolling agencies are required to inform individuals about the manner in which their information shall be used, the nature of recipients with whom it will be shared, the right to obtain access to information, and the procedure for this. In addition, the UIDAI is responsible for guaranteeing the security of individuals' Aadhaar data, including authentication records.

The Act delineates several measures that the UIDAI must take to ensure data confidentiality and security. These include implementing technical and organisational security measures, guaranteeing that all entities operating in connection with the Act have adopted equivalent security measures and that these entities act only on the instruction of the UIDAI and are bound by equivalent obligations.

The 2011 Standing Committee report noted that the Aadhaar project allowed the UIDAI to create a large database of personal information, creating the possibility of information misuse. Given this concern, the Committee advocated the enactment of a national data protection law as a prerequisite to any legislation allowing large-scale collection of personal information and linkage across databases. The committee noted that the absence of data protection legislation would make it difficult to deal with issues such as "access and misuse of personal information, surveillance, profiling, linking and matching of databases, and securing confidentiality of information." Meanwhile, no data protection legislation has been passed by Parliament.

In response to media reports of data misuse by private agencies and individuals, the UIDAI and the Government of India have stated that the Aadhaar database is secure.[28,29] Instances of government entities publishing residents' Aadhaar numbers have been reported in some states, including Jharkhand. In April 2017, the Aadhaar numbers and bank details of more than a million pension beneficiaries in the state were displayed on a state government website.[30]

While these instances constitute a clear violation of the Aadhaar Act (which forbids the publication of an individual's Aadhaar number), the Government stated that these do not represent a vulnerability in Aadhaar's framework itself.[31] The UIDAI has directed the Jharkhand state government to identify the individuals responsible for the leak in order for action to be initiated against them.[32]

Data authentication

Any entity (public or private) requesting authentication of an Aadhaar number is required to obtain consent of the individual before collecting or verifying her or his identity information. Entities are also required to ensure that identity information of the individual is used only for submission to the Central Identities Data Repository (CIDR) for authentication. In addition, the requesting entity must apprise the individual—whose data is to be authenticated—of the following:

1. The nature of the information that may be shared upon authentication,
2. the uses to which information received by the requesting entity may be put, and,
3. alternatives to submitting personal information to the requesting entity.

The UIDAI shall respond to an authentication query with a positive, negative, or other appropriate response sharing identity information, excluding core biometric information (fingerprints and iris scan). In addition, the UIDAI will maintain authentication records in such manner and for such period as specified by regulations. However, the UIDAI will not collect or maintain data on the purpose of authentication. A detailed discussion of the authentication process is presented in Chapter 2, *Aadhaar Architecture.*

Data disclosure

No member of the UIDAI nor any of its contracted agencies is entitled to disclose any information contained in the CIDR or authentication record. An individual's core biometrics (fingerprints and iris scan) may never be disclosed (except under the national security clause discussed below). Authenticating agencies too are forbidden from using individuals' information in any way other than in the manner specified to Aadhaar holders. They may not disclose individuals' personal information without their consent.

The Act allows for exceptions wherein the UIDAI may share information about individuals, as specified by regulations. Two specific circumstances have been outlined where information disclosure will be permissible.

First, a district judge or higher court can mandate that identity information, including name, date of birth, address and gender, but not fingerprints or iris scan, be disclosed. Currently, there is no known case of a court requiring that an individual's personal information—collected under Aadhaar—be disclosed.

Second, a government official of Joint Secretary or higher rank can order the release of an individual's Aadhaar data, including biometrics, in the interest of national security. This decision would require review by an Oversight Committee before taking effect. The Committee will consist of the Cabinet Secretary (the highest-ranked civil servant in India), as well as the Secretaries of Legal Affairs and Information Technology. Any such decision would be valid for three months, which may be extended further by three months after additional review by the Oversight Committee. The Act does not contain any provisions regarding how the disclosed data (including biometrics) is to be treated after this validity period. Information is not publicly available on whether any release of biometric or demographic information has been mandated by the Oversight Committee so far.

During Parliamentary debate, certain Members argued that citing "national security" as an exception was ambiguous and liable to misuse. The term is not currently defined in either the Indian Penal Code or the National Security Code. Similar but distinct terms such as "public emergency" or "public safety" could be used, it was argued, as they are mentioned in other laws.[33]

Members also discussed a purported lack of specificity in the data-sharing guidelines of the Act, which do not provide clarity on with whom, and in what form, data may be shared when concerning a national security breach. Concern was also raised with regard to lack of opportunities for individuals affected under the national security clause to present their case to, or to appeal the decision of, a court.

For these sections of the Act, the Rajya Sabha passed two amendments. The first amendment sought to replace the term "national security" with "public emergency or in the interest of public safety." The second amendment proposed the addition of the Central Vigilance Commissioner (CVC) or the Comptroller and Auditor-General (CAG) to the Oversight Committee in charge of reviewing orders pertaining to the release of an individual's biometric data. Neither of these amendments was accepted by the Lok Sabha.

Role of UIDAI

The Act lays out the governing structure and powers of the UIDAI. Under the Act, the UIDAI consists of a Chairperson, two part-time Members, and a Chief Executive Officer. Members must have at least 10 years of experience in a wide range of matters such as technology, governance, law, finance, or administration. The UIDAI is responsible for specifying the information to be collected under the Act, assigning and authenticating Aadhaar numbers, and specifying the use of Aadhaar numbers for delivery of subsidies and services.

The UIDAI has the power to frame rules governing:

1. The process of information collection and verification,
2. individual access to information,
3. data sharing and disclosure, and the alteration of personal information,
4. data privacy and security processes, and,
5. establishment of grievance redressal mechanisms.

The UIDAI has published detailed regulations governing enrolment, authentication, data security, and disclosure. These are discussed in Appendix 3.1.

User rights and obligations

An Aadhaar holder may request the UIDAI to provide access to her or his identity information, not including the core biometric information. The powers of the UIDAI to accept or deny such requests have not been defined under the Act. In addition, the Act allows Aadhaar holders to request the UIDAI to alter their demographic information in its records. The UIDAI may also require individuals to update their demographic information from time to time. Information is not publicly available about the number of such requests and how many of them were granted.

There exist certain safeguards for the user against misuse of data. The Act imposes a penalty on a data-requesting entity upon non-compliance with the data-storage and data–sharing provisions of the Act. The Act also states that only the UIDAI or its authorised officer can file a complaint before a court for offences defined under the Act. Individual Aadhaar holders cannot independently approach the courts for these offences. The UIDAI has so far filed at least two First Information Reports under the Act for illegal use of biometrics.[34,35]

The Rajya Sabha passed an amendment inserting a provision empowering individuals to opt out of Aadhaar and to ask for their personal records to be destroyed within 15 days. The Lok Sabha did not accept this amendment. Therefore, there is no provision for a resident to de-enroll from Aadhaar.

Offences and penalties

Penalties are defined for impersonation and unauthorised conduct with regard to Aadhaar data. Individuals are prohibited from impersonating others to enrol or alter another's details in the Aadhaar database. Similarly, individuals or bodies pretending to be authorised to collect personal information when not allowed to do so under the Act are also liable to be punished. Penalties for unlawful data storage and disclosure are summarised in Appendix 3.2 of this Chapter. Information is not publicly available about the number and nature of penalties that have been imposed under the Act.

Legal Challenges

The Supreme Court is currently hearing three key challenges to the Aadhaar Act 2016 and the Aadhaar project more broadly. The judicial outcomes of these challenges hold significant import for the future of Aadhaar.

One challenge constitutes a writ petition filed on 6 April 2016 by Jairam Ramesh, a former Union Minister in the UPA government (2009-2014) and current Member of Parliament. The petition challenges the classification of the Aadhaar Bill as a Money Bill (see Figure 3.1 for a description of Money Bills). It argues that the bill does not fulfill the constitutional provisions for a Money Bill, and that the Speaker's decision to classify a bill as such may be judicially reviewed in cases of a substantive infraction. There is no historical precedent for the Supreme Court nullifying the Parliament's classification of a bill as a Money Bill. If the Court were to rule in favour of the petitioners, the Act may be struck down.

A second legal challenge consists of a series of individual petitions combined with a writ petition filed by Justice K.S. Puttaswamy, a retired High Court judge, challenging the Aadhaar project on various grounds. These petitions challenge the legality of collection of personal information on a large scale, the mandatory status of Aadhaar, and most significantly, potential violations of individual privacy engendered by Aadhaar.

No express right to privacy is currently afforded by the text of the Indian Constitution, and varying interpretations of whether such a right may exist have been offered by different court judgements. Various judgements delivered by benches of two or three judges from 1975 onwards have read it to be implicit in the fundamental right to life and liberty enshrined in the Constitution. However, older court judgements dating from 1954 and 1963 (delivered by larger benches) have observed there is no such right afforded under the Constitution.[36]

The Supreme Court, recognising the divergent judicial verdicts on a right to privacy, has recommended the creation of a bench of at least five judges to settle the matter. The case is pending before the Court. Depending on whether, and how, the Supreme Court reads a right to privacy into the Constitution, this could have varying impact on the legality of the Aadhaar project and whether and how it is used for government service provision.

If a right to privacy were read into the Constitution —in accordance with more recent, but smaller-bench judgements of the Supreme Court—there there may be an impact on procedural norms regarding the collection, use, and protection of individual data under Aadhaar. As some petitioners have argued, such a decision may allow individuals to choose to not hold an Aadhaar number, while still availing themselves of government services or interacting with government institutions. However, the implications (if any) of this challenge are unclear until the matter is heard and adjudicated by the Supreme Court.

A third set of petitions challenge Aadhaar's mandatory linkage to the filing of income tax returns and the holding of a Permanent Account Number (PAN). This link was established by the Finance Act 2017. The petitioners have highlighted that the Aadhaar Act's provisions do not require every citizen to hold an Aadhaar number (unless seeking to access government benefits), and the UIDAI has maintained that enrolment into Aadhaar is voluntary. According to the petitioners, the voluntary character of Aadhaar enrolment means it cannot be made mandatory for tax returns—which all citizens (above a certain income threshold) are legally bound to submit. In addition, petitioners have raised (1) the right to equality; arguing that the link creates two classes of taxpayers and discriminates against those without Aadhaar, (2) freedom of trade and practice; since the lack of a PAN inhibits individuals from engaging in basic transactions such as opening a bank account, and (3) the right to personal autonomy and self-determination of information disclosure. The Supreme Court is yet to deliver a final judgement on this case. The judgement will determine whether or not the concerned legal provision enforcing Aadhaar's linkage to tax filing and PAN will stand as is. This will have an impact on the procedure for tax submissions and PAN card documentation for all taxpayers, effective from the current financial year.

The substance of these legal challenges points to important areas for future research.

Figure 3.3: Privacy concerns with digital identities

Digital identities, such as Aadhaar, carry a number of potential risks with regard to identity holders' privacy. The World Bank highlights four important general concerns:
(1) unauthorised access, use or disclosure of information, (2) profiling, through linking databases in illicit ways, including for surveillance objectives, (3) "function creep" whereby data collected for one or more reasons is used for others to which the identity holder has not consented, and (4) inaccuracies in data, leading to mistaken identity or unjust treatment.

Source: Identification for Development Strategic Framework, World Bank Group

Areas for Future Research

Aadhaar's legal framework has seen significant change over the years. Legal challenges to Aadhaar's legislative framework and use-cases await resolution, and associated judicial verdicts may reshape the contours of Aadhaar and its uses.

Multi-disciplinary research on Aadhaar's legal and governance framework can benefit legislators and members of the judiciary as they make decisions on how Aadhaar should be governed, used, and safeguarded. This research may be used to strengthen the legal and regulatory framework for Aadhaar in particular, and digital identity more generally.

We present three important themes of future research:

- Research to improve the implementation of legal safeguards in the Aadhaar Act 2016, and independent and regular assessments of the quality of enforcement of Aadhaar's legal protections to increase their effectiveness
- Research drawing on international privacy principles, domestic norms, and judicial precedent to inform court judgements and potential legislation on defining and safeguarding individual privacy—including, but not limited to, Aadhaar
- Research focused on informing a modern national data protection framework to strengthen the governance of digital information—including, but not limited to, Aadhaar

To maximise the impact of practitioner-oriented research, we recommend:

- **Framing research questions in collaboration with practitioners**
- **Being responsive to decision-making schedules and other practitioner constraints**
- **Presenting insights in succinct documents and in-person meetings**
- **Providing follow-up support to translate research to action on-the-ground**

APPENDIX 3.1: Regulations and Notifications on Aadhaar

Following the notification of the Aadhaar Act 2016, the government has introduced various regulations pertaining to the enrolment, authentication, and sharing of information, which have the status of delegated legislation. This Appendix provides a summary of key features of these regulations. The regulations discussed below were notified in September 2016.

Unique Identification Authority of India (Transaction of Business at Meetings of the Authority) Regulations 2016[37]

These regulations provide details on the frequency with which UIDAI meetings shall take place, norms regarding scheduling meetings and notifying members, as well as conduct of meetings. They state that the four members of the Authority should meet at least three times a year. They also detail how the UIDAI will take decisions in these meetings. The UIDAI CEO is empowered to make decisions without the conduct of a meeting in certain urgent scenarios, subject to regulations. All decisions taken in the meeting are to be published online, barring cases in which the Chairperson deems that certain content is confidential.

Aadhaar (Enrolment and Update) Regulations 2016[38]

These regulations set the standard for processes related to Aadhaar enrolment, including provisions on enrolment agencies and registrars, personal information to be collected, and specification of technologies used in the enrolment process. In particular, the regulations detail certain optional information that may be recorded (mobile number and email address) in addition to the biometric and demographic information specified in the Act. Additional information to be collected for children under the age of five, as well as individuals being enrolled through the "introducer" system or using the head of the family's data, is also noted (see Chapter 2, *Aadhaar Architecture*, for details). Provisions discuss how to enroll individuals who are unable to provide biometrics.

The regulations also delve into norms regarding the generation of an Aadhaar number and its delivery to residents, updating resident information in the database, omission or deactivation of Aadhaar, and grievance redressal. In particular, Section 32 envisages a contact center to serve as a grievance redressal mechanism for the resolution of queries through calls and emails.

A 2017 amendment[39] to this regulation states that UIDAI may authorise Registrars, Enrolling Agencies, and other service providers to collect a fee for updating demographic and biometric information.

Aadhaar (Authentication) Regulations 2016[40]

These regulations contain rules on the types of authentication provided by UIDAI and provisions on the appointment and actions of authenticating agencies. A detailed discussed of authentication types is presented in Chapter 2, *Aadhaar Architecture*. The regulations detail the information authenticating agencies must provide to the Aadhaar holder, the procedure for obtaining consent, and capturing biometrics. They also outline certain data security norms for the operations of these agencies. They allow individuals to "lock" their biometrics, and unlock them only when required for authentication. All attempted biometric authentication against locked biometrics shall fail, unless biometrics are temporarily unlocked.

The regulations also state that authentication data shall be maintained for a period of six months and thereafter archived for a period of five years by the UIDAI. Authentication logs will be maintained by the requesting entity for a period of two years and archived for a period of five years.

A 2017 amendment[41] expanded the eligibility criteria for appointment as a requesting entity to include airline operators.

Aadhaar (Data Security) Regulations 2016[42]

According to these regulations, UIDAI may specify an information security policy setting out technical and organizational measures to be followed by UIDAI and its personnel as well as any and all associated agencies or service providers. The UIDAI shall be responsible for monitoring compliance with the information security policy and will designate a Chief Security Officer for this purpose. Regulations further require all agencies and service providers engaged by UIDAI to undergo audits by recognised entities at specified time periods.

Aadhaar (Sharing of Information) Regulations 2016[43]

These rules specify norms regarding the sharing of personal information by UIDAI, authenticating entities, and others. They also specify restrictions on the sharing or circulating of Aadhaar numbers, and the liability for contravention of these regulations. The regulations stipulate that no core biometric information can be shared by UIDAI or stored by requesting entities. Requesting entities have also been directed to not use or share an individual's Aadhaar number for purposes beyond which consent has been given.

APPENDIX 3.2: Offences and Penalties for Unauthorised Data Disclosure in the Aadhaar Act 2016

OFFENCES	PENALTIES
DATA DISCLOSURE	
Intentional dissemination of identity information collected in the course of enrolment or authentication in a manner unauthorised by the Act (or ensuing regulations)	Imprisonment of up to three years, and/or a fine up to ₹10,000 (for individuals) and ₹1,00,000 (for companies)
DATA IN THE CENTRAL IDENTITIES DATA REPOSITORY (CIDR)	
Intentional acts corresponding to: • Unauthorised access • Disruption/denial of authorised access • Unauthorised data extraction • Damage or destruction • Unauthorised disclosure • Theft or modification of computer source codes used by UIDAI	Imprisonment of up to three years, and a fine not less than ₹1,00,000
OTHER	
Use or tampering of data in the CIDR or a removable storage device with the intent of modifying or discovering information related to an Aadhaar holder	Imprisonment of up to three years, and a fine up to ₹10,000
Use of an individual's identity information by a requesting entity in contravention to the Act	Imprisonment of up to three years, and/or a fine up to ₹10,000 (for individuals) and ₹1,00,000 (for companies)
Enrolment agencies or requesting entities failing to comply with the requirements of the Act	Imprisonment of up to one year, and/or a fine up to ₹10,000 (for individuals) and ₹1,00,000 (for companies)
Offences under the Act for which no specific penalties have been provided	Imprisonment of up to one year, and/or a fine up to ₹25,000 (for individuals) and ₹1,00,000 (for companies)

4 | FINANCIAL INCLUSION

Increasing access to financial services can lead to improved economic prospects for poor individuals and communities. According to the government, Aadhaar has the potential to promote financial inclusion by addressing certain critical barriers, mainly documentation requirements and physical access to banking services. Understanding whether and how Aadhaar has played a role in increasing financial inclusion is an important area of future research.

A growing body of evidence demonstrates the strong positive relationship between access to formal financial services and economic prospects for poor individuals and communities.[1] Banking the unbanked is a stated priority of the Government of India.[2] Through significant effort on the part of the public and private sectors, Pradhan Mantri Jan Dhan Yojana (PMJDY or "Jan Dhan")—a central government scheme to drive financial inclusion—has facilitated the opening of 282 million accounts as of March 2017.[3] However, despite this progress, we estimate that more than a hundred million people in India remain excluded from financial services.[4] Further, among those who have recently opened accounts many do not regularly use them, thereby missing out on the economic benefits of financial inclusion.[5]

The government states that Aadhaar has a role in increasing financial access for underserved populations and reducing the cost of processing bank applications.[6] For instance, Aadhaar provides a proof of identity and address, and can overcome the barrier of lack of legal documentation, which accounted for as many as 20 percent of exclusions in India.[7,8] The development of innovative services and products that use Aadhaar also have the potential to promote financial transfers, banking in remote areas, and mobile banking.[9]

Citing these potential benefits, the government has promoted the widespread adoption of Aadhaar in financial services.[10] Alongside PMJDY and increasing mobile access, Aadhaar forms the core of the government's financial inclusion drive. Nearly 400 million bank accounts were linked to Aadhaar as of April 2017, and it was used to digitally provide proof of identity to open more than 6 million accounts in March 2017.[11,12]

In this Chapter, we explore these topics in more detail. We begin with an overview of the trends in financial inclusion. We then evaluate four ways in which Aadhaar is being used to increase financial inclusion, namely e-KYC for account opening, Aadhaar-enabled microATMs for remote banking, Direct Benefit Transfer (DBT), and Aadhaar-enabled payments systems. We close this Chapter with areas for future research that could enable a better understanding of the role of Aadhaar in increasing financial inclusion.

Financial Inclusion Trends

As a step toward fulfilling its commitment to financial inclusion, the Reserve Bank of India (RBI) introduced standards on "no-frill accounts" in 2005. These basic savings accounts were devised as a way to increase access to bank accounts for a wider population. The accounts had an added emphasis on allowing zero- or very low-minimum balance in the accounts at no charge.[13] Seven years later, in 2012, these standards evolved into guidelines on Basic Savings Bank Deposit Accounts (BSBDAs). See Figure 4.1 for a list of characteristics of basic savings accounts.[14,15]

Despite these efforts, hundreds of millions of people in India were still excluded from financial services as of late 2014.[16] The government has made efforts to reduce that number. Between 2014 and 2016, the financial services sector experienced rapid growth in the overall number of BSBDAs (see Figure 4.2).

Most of the increase in BSBDAs is associated with the Jan Dhan scheme mentioned above. Launched in 2014, PMJDY aims to ensure access to financial services for low-income groups through the use of technology.[17] As of March 2017, 282 million PMJDY accounts and 255 million other BSBDA accounts[18] have been opened.[19]

In line with the aims of Jan Dhan, the Government of India has continued to turn to technology to accelerate financial inclusion. The government has developed and promoted a triad of solutions, known as the "JAM trinity," which stands for Jan Dhan, Aadhaar, and Mobile.[20] The next section describes how the government envisions the use of Aadhaar, in particular, may be able to help overcome challenges that continue to exclude people from the formal financial and banking system.

Figure 4.1: Characteristics of basic savings accounts

- No requirement for minimum balances
- Comes with expected banking features: ATM usage, electronic payments/receipts, deposit/collection of cheques
- No limits on number of monthly deposits
- Maximum of four withdrawals a month
- Provides usage of ATM/debit cards

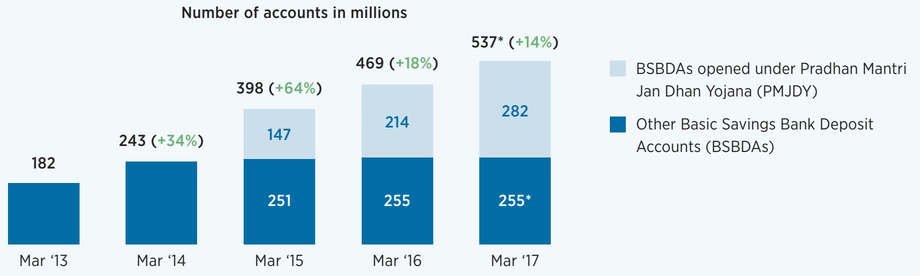
All of the above are provided at zero cost to the account holder.

Source: Reserve Bank of India

Role of Aadhaar in Financial Inclusion

Despite the progress of PMJDY, the barriers to financial inclusion in India are persistent and include obstacles

Figure 4.2: Cumulative number of Basic Savings Bank Deposit Accounts (BSBDAs), Mar 2013 – Mar 2017



*Data for total number of BSBDAs as of Mar 2017 was not available. Thus, we kept the 2016 number constant.

Note: "Other BSBDAs" is calculated by subtracting the total PMJDY accounts released by the PMJDY website from the total number of BSBDAs released by RBI.

Data sources: Reserve Bank of India (RBI) & Pradhan Mantri Jan Dhan Yojana (PMJDY) to both the opening and use of accounts within the formal financial system. In Figure 4.3, we outline the key barriers to financial inclusion from the perspective of an individual.[21,22] This discussion is limited to barriers faced by individuals; it does not include supply-side factors relating to banks or larger financial or policy systems. A broader discussion of more sophisticated financial services such as insurance, while important, falls outside the scope of this report.

First, there may be a lack of understanding of the financial sector. This can manifest itself in two ways: either individuals do not know about financial products (such as a bank account), or are provided incomplete information by the banker. Second, for individuals who are *willing* to open an account, they may be unable to do so because they do not have surplus income, lack the necessary identification documents, or are located at a distance far from the financial service provider.[23,24] Third, even if an individual opens an account, it can remain unused—retaining no money or facilitating no transactions.[25,26] Reasons for this include lack of physical or technological access to banks, a preference for cash, or simply inertia.

While Aadhaar's design and functionality may not help to overcome all barriers of exclusion, the system can address and mitigate some important challenges, particularly regarding access. There are four main ways that Aadhaar can play a role in access to financial services: enabling the opening of a bank account through e-KYC; using authentication and microATMs to encourage remote banking; Direct Benefit Transfers (DBTs) to citizens from the government to encourage the regular use of accounts; and various Aadhaar-enabled systems in the financial services sector to facilitate the movement of money. These are described in the following four sections.

Opening a Bank Account through e-KYC

Across the world, banks are required to obtain acceptable identity and address documents for account openings by individuals. In 2004, the RBI established a set of mandatory Know Your Customer (KYC) procedures for all banks operating within India. In September 2013, the RBI expanded those

Figure 4.3: Barriers to basic financial inclusion of individuals

	AADHAAR-BASED SOLUTIONS	ROLE OF AADHAAR
LACK OF AWARENESS OR UNDERSTANDING		
Lack of understanding about financial products	No	
Information asymmetries about banking	No	
UNABLE TO OPEN AN ACCOUNT		
Not enough money to open an account	No	
Lack of necessary documentation	Yes	Aadhaar-enabled e-KYC
Distance from a bank / ATM	Yes	Aadhaar-enabled e-KYC + microATM
Discrimination against low-income customers	No	
OPEN ACCOUNTS REMAIN UNUSED		
Preference for cash	No	
Status quo bias or other behavioural biases	Partially	APBS used for DBT
No access to a bank / ATM	Yes	Aadhaar-enabled microATM; AEPS/UPI
High transaction costs	No	

Sources: This table is the authors' compilation based on the World Bank's Global Financial Development Report 2014 and supplemented by the World Bank's Global Findex Database 2014.

procedures to allow the use of Aadhaar biometric and demographic data in a process known as electronic Know Your Customer (e-KYC).[27]

Role of Aadhaar

Now, Aadhaar is a sufficient form of documentation to open an account through e-KYC. Using e-KYC,[28] one's Aadhaar number and matching biometrics can be employed to retrieve information (such as an address) from the UIDAI, which is used as proof of identification and documentation for account opening. This instantaneous electronic system has the potential for faster processing, lower material costs, and reduced error rates as well as the ability to provide accurate data for audits by regulators.[29] Further, e-KYC lowers the costs of transactions of KYC processes for banks.[30]

Adoption of Aadhaar

Since the RBI began accepting e-KYC in September 2013, 15 of 22 private sector banks, 27 of 29 public sector banks,[31] and 36 of 56 regional rural banks began offering e-KYC as a way to open a bank account.[32] According to a UIDAI statement in March 2017, 44.7 million bank accounts had been opened through e-KYC.[33] For comparison, this number is less than 16 percent of the Jan Dhan accounts opened by that date.

In Figure 4.4, we illustrate the growth in the number of e-KYC verifications for financial services over the past year. This data comprises all types of e-KYC tracked by the National Payments Corporation of India (NPCI). The breakdown between various kinds of financial undertakings, such as opening a bank account or buying insurance, is not available.

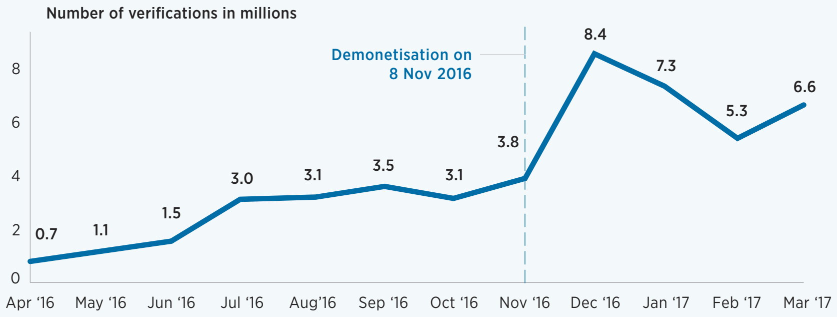
There are three ways in which it would be helpful to understand the impact of Aadhaar-enabled e-KYC on inclusion within the banking sector: gains or losses experienced by the customer, gains or losses experienced by the banks, and increase in access to and use of banking services by those previously unbanked or underbanked. Research in these areas would be useful to understand Aadhaar's role to date, and provide data on whether and how this function should be extended.

Authentication of Identity and MicroATMs

Role of Aadhaar

A microATM is a portable, handheld point-of-sale device that facilitates banking transactions. With Aadhaar-enabled microATMs, an individual's Aadhaar number and biometrics authenticate identity and allow

Figure 4.4: Monthly number of successful Aadhaar e-KYC verifications as per NPCI, Apr 2016 – Mar 2017



Note: e-KYC verifications data as released by the NPCI. It may be for opening of new bank accounts and for other financial services products as well.
Data source: National Payments Corporation of India

her or him to withdraw money or make bank transfers, without requiring other forms of authentication such as debit cards or personal identification numbers (PIN).[34] The mobility of microATMs transported to remote villages by business correspondents (BCs) can offer services to individuals who do not live close to a brick-and-mortar bank.[35]

Adoption of Aadhaar

While we do not have data on the coverage of microATMs in rural areas[36], we have it on the prevalence of BCs, which provides an upper-bound estimate under reasonable assumptions.[37] As of 2016, there was 1 BC per 6,630 persons. Kenya, often considered a leader in last-mile delivery of financial services, has a BC-to-population ratio of 1:172.[38] According to NPCI, the value of transactions conducted through microATMs, using Aadhaar authentication, grew by 26 times in the past year, from ₹86 crore ($12.8 million) in FY 2015-16 to ₹2,282 crore ($341 million) in FY 2016-17. We also have access to the number of transactions, including balance inquiries, mini-statements, withdrawals, deposits, and transfers. There were 345 million transactions in FY 2016-17, representing a nearly four-fold increase from FY 2015-16 (95 million), and twenty-one-times the number in FY 2014-15 (16 million).[39]

More Aadhaar-enabled microATMs in underserved communities could increase access to financial services. However, implementation challenges, such as infrastructure failures (malfunction of microATMs) and connectivity issues (weak Internet), may create barriers that reduce access and usage. Empirical evidence about these barriers and on the impact of microATMs on financial inclusion is an important area for further research.

Direct Benefit Transfers (DBTs) from Government to Citizens

Direct Benefit Transfer (DBT) refers to electronic money transfers directly to the bank accounts of eligible citizens in lieu of in-kind or cash subsidies. DBTs have become a priority for both state- and central-level government ministries.

Role of Aadhaar

The Aadhaar Payment Bridge System (APBS) uses Aadhaar-enabled infrastructure to facilitate payments from the government to individuals. The government states APBS is a more efficient way to distribute DBTs because it eliminates the need for intermediaries, thus decreasing the likelihood of leakages and cutting the time between distribution and receipt of payment.[40] The system is hosted by the National Payments Corporation of India (NPCI) and requires only basic information for each transfer: the transferee's Aadhaar number and the bank to which the Aadhaar number is linked.[41]

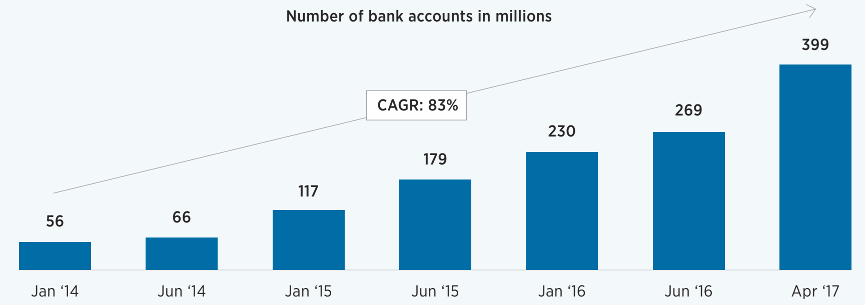
Transferring money requires that eligible individuals first open or have an account. The next steps include the seeding (linking) of the individual's Aadhaar number to a bank account and the seeding (linking) of the individual's Aadhaar number to the beneficiary lists of various government programmes, such as an employment guarantee scheme or food subsidies.

Adoption of Aadhaar

As of April 2017, nearly 400 million individuals have seeded their bank accounts to an Aadhaar number (see Figure 4.5).[42] In Figure 4.6, we show the growth in PMJDY accounts seeded to Aadhaar since November 2015, by bank type. As of March 2017, public sector banks accounted for 151 million of the 183 million Aadhaar-seeded PMJDY accounts.

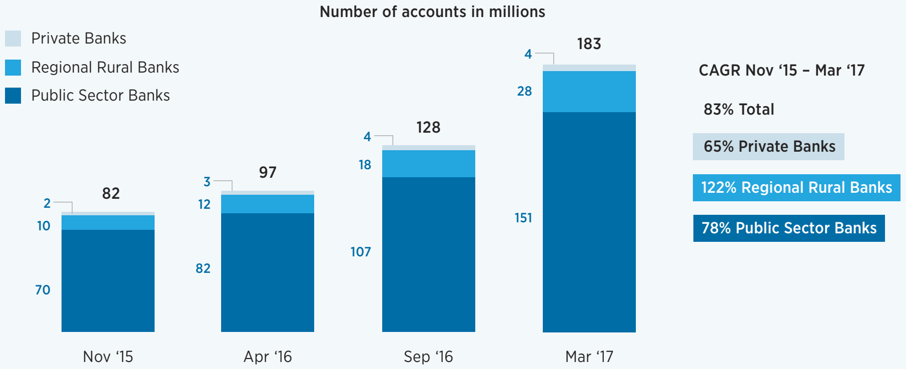
DBTs have the potential to increase financial inclusion by encouraging individuals to engage with the banking system. Since funds are directly deposited into accounts, this increases the incentive to use banking services.[43] Field-based evidence to support or refute the effectiveness of DBTs as a gateway to financial inclusion would be an important addition to our understanding of this use-case of Aadhaar. A discussion of DBTs from a social protection point of view follows in Chapter 5 of this report.

Figure 4.5: Cumulative number of Aadhaar-seeded bank accounts, Jan 2014 – Apr 2017



Data source: National Payments Corporation of India

Figure 4.6: Cumulative number of Aadhaar-seeded PMJDY bank accounts by bank type, Nov 2015 – Mar 2017



Data Source: PMJDY dashboard

Aadhaar-Enabled Systems for Payments and Transfers

Role of Aadhaar

UIDAI, in coordination with NPCI, RBI, and various other entities, has helped to develop several Aadhaar-enabled systems to facilitate the movement of money.[44] Three important systems include the APBS for DBTs, the Aadhaar Enabled Payments System (AEPS) for microATMs, and the Unified Payments Interface (UPI) for mobile banking.

Adoption of Aadhaar

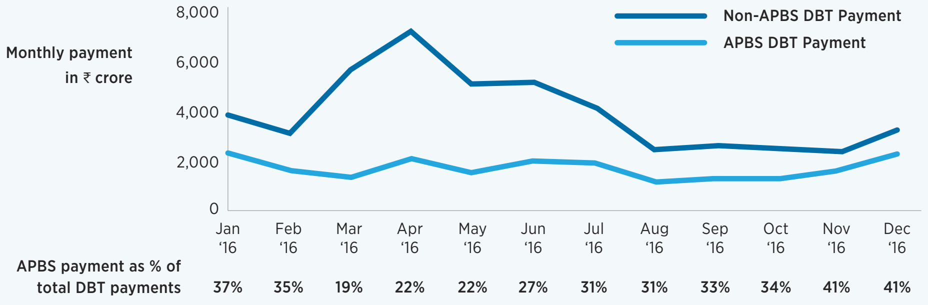
Aadhaar Payment Bridge System

As discussed above, the APBS allows government agencies to transfer funds to citizens using only their Aadhaar number and bank name. This system is used in subsidy and other social protection programmes. In Figure 4.7, we show the trends in DBT payments made through APBS. Over the past year, APBS DBT payments as a proportion of all DBT payments seem to have remained about one-third of all DBT payments.

Aadhaar Enabled Payment System

The AEPS allows for biometric authentication of transactions by individual users.[45] As discussed above, microATMs using AEPS carried out transactions worth ₹2,282 crore ($341 million) in the fiscal year 2016-17.

Figure 4.7: Monthly Direct Benefit Transfer (DBT) payments over non-APBS and APBS, Jan 2016 – Dec 2016



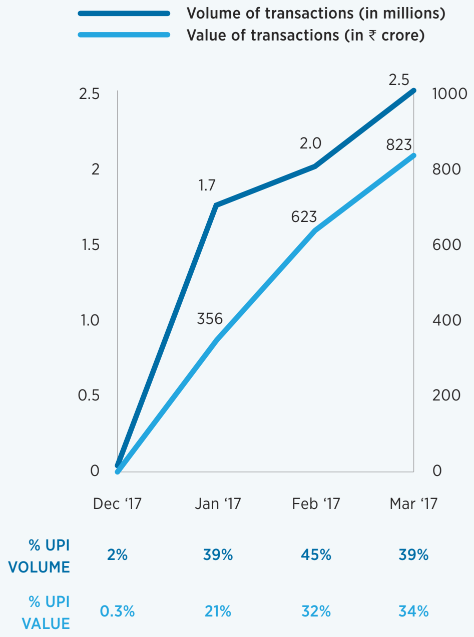
Note: Non-APBS DBT Payment can be done through instruments such as NEFT and RTGS.
Data source: DBT monthly reports

Unified Payments Interface

The Unified Payments Interface (UPI) is a system that facilitates banking transactions using mobile phones. Launched in April 2016, UPI allows the usage of an Aadhaar number as a payment address.[46] According to NPCI, there are five channels through which funds can be transferred with UPI, one of which is with an Aadhaar number. UPI features are available on both smartphones and feature phones.[47]

At its sixth month mark, September 2016, about 80,000 transactions, and a total of ₹32 crore ($4.8 million), were processed through the UPI platform. However, at its twelfth month mark, March 2017, 6.4 million transactions and a total of ₹2,425 crore ($362 million) were sent through UPI. It should be noted that in November 2016, the Government of India demonetised the 500- and 1000-rupee notes from circulation, prompting a surge in usage of digital money platforms.[48,49]

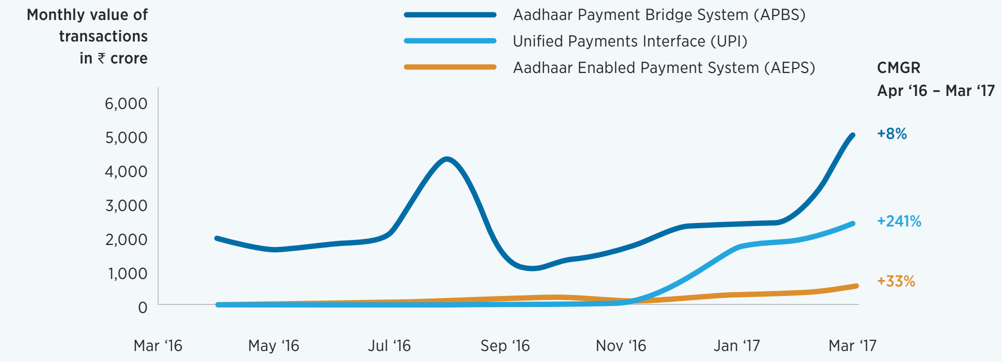
Figure 4.8: Monthly transactions on the BHIM App, Dec 2016 – Mar 2017



Source: National Payments Corporation of India

The increase in monthly UPI transactions also coincided with the launch of the Bharat Interface for Money (BHIM) mobile application in December 2016.[50] BHIM is an example of an application that uses UPI. BHIM was designed by NPCI to ease the transfer of digital payments between bank accounts.[51] As seen in Figure 4.8, both the value and volume of BHIM transactions have sharply increased since its launch. The BHIM app now comprises a sizeable amount of overall UPI volume (39 percent) and value (34 percent).[52] The main appeal of BHIM is that it allows people to download one single application for all mobile payments, which can then be linked directly to one's bank account, rather than downloading individual bank apps or other mobile wallet apps. BHIM can also be used on feature phones using the *99# service maintained by NPCI.[53]

Figure 4.9: Monthly transactions of Aadhaar-enabled systems for payments and transfers, Apr 2016 – Mar 2017



Avg. transaction size in ₹	APBS	249	278	180	215	278	542
	UPI	10	44	4,000	3,483	3,803	3,805
	AEPS	19	37	65	38	73	109

Data Source: National Payments Corporation of India

Individuals have the option to send money using the payee's Aadhaar number as the payment address.[54]

UPI has seen the greatest increase across these three systems (AEPS, APBS, and UPI), as seen in Figure 4.9. UPI had a compound monthly growth rate of 241 percent for the 2016-17 fiscal year. In addition, its average transaction size for the month of March 2017 is seven times that of APBS, and 35 times that of AEPS.

However, it should be noted that all these systems grew steadily throughout the last fiscal year, suggesting increasing adoption of these payment systems in the wider landscape. All experienced an increase in the value of monthly transactions as well as an increase in the average size of transactions.

The average monthly transaction was two times higher in March 2017 compared with April 2016 for APBS, 381 times for UPI, and six times for AEPS.

Payment systems that use Aadhaar have the potential to increase the level of access an individual has to a range of financial tools, including a basic savings account and financial transactions. Access may be limited in areas with low smartphone penetration and weak telecommunications networks. Since these Aadhaar-enabled systems are still new, there is no current data or evidence about expansion of financial inclusion resulting from their use. This is an important area of further research.

Areas for Future Research

Earlier in this Chapter we estimated that there are at least one hundred million unbanked people living in India—and many more remain underbanked. The government has articulated plans to use Aadhaar to help bring these individuals into the formal financial sector, and in doing so, potentially raise their overall welfare.

Research on Aadhaar's role in expanding access to financial services will be valuable for senior decision-makers in government, regulatory bodies, and the banking sector. Research can guide best practices to expand the reach of financial inclusion to underserved populations. Research can also inform resource allocation decisions on which financial inclusion use-cases of Aadhaar to expand.

We outline two themes for future research that can be applicable for practitioners today:

- Research on how best to implement Aadhaar use-cases for financial inclusion, with a particular focus on take-up, efficiency, connectivity, and infrastructure
- Research on the impact of Aadhaar-enabled use-cases on three dimensions: (1) *access* to financial services, especially bank accounts, (2) *usage* of financial services, and (3) *welfare impacts* of increased access and usage of financial services

More research and publicly available data will be valuable to learn which uses should be expanded and which may have limited potential. A platform aimed at collaboration and sharing such research would be particularly useful to disseminate information and short policy briefs to practitioners. Targeted, high quality research will contribute to a meaningful dialogue among stakeholders on this critical topic.

To maximise the impact of practitioner-oriented research, we recommend:

- **Framing research questions in collaboration with practitioners**
- **Being responsive to decision-making schedules and other practitioner constraints**
- **Presenting insights in succinct documents and in-person meetings**
- **Providing follow-up support to translate research to action on-the-ground**

5 | SOCIAL PROTECTION

The Government of India aims to provide a comprehensive set of safety nets to India's poor, including food subsidies, employment guarantees, and targeted cash transfers. Financial leakages and service delivery issues, however, reduce its effectiveness. The government aims to use Aadhaar's authentication and fund transfer capabilities to address these problems. Policy-relevant research on the intended and unintended impacts of the use of Aadhaar can provide actionable insights to practitioners.

A third of the world's ultra poor—those earning below $2 a day—live in India.[1] Successive governments have introduced social protection programmes to alleviate poverty and provide for basic needs. Social protection in India takes many forms, including food and essential commodity subsidies, employment guarantees, and targeted cash transfers. The central government spends more than ₹3 lakh crore ($47 billion) per year on eight programmes that we define as social protection.[2] This is more than a sixth of its entire annual budget,[3] reflecting the scale of social protection programming and the importance the government places on it. While these safety nets have contributed to alleviating poverty, their potential is undercut by financial leakages and service delivery issues, among other reasons.[4]

The government states that Aadhaar has the potential to improve the status quo by curbing certain types of leakages from India's social protection programmes while improving service delivery.[5] More specifically, Aadhaar can uniquely identify individuals using biometrics, which can remove duplicate beneficiaries and authenticate identity for transactions.[6] Aadhaar can also facilitate direct transfer of social protection benefits to individual bank accounts. This can remove intermediaries who have the potential to siphon funds and reduce payment delays.[7]

Citing this potential for "substantial impact," India's central and state governments are adopting Aadhaar in various social protection programmes.[8] The extent of this adoption varies across schemes but has increased steadily over recent years.[9] Today, programmes accounting for more than two-thirds of government spending on social protection use Aadhaar in one or more ways.[10]

The precise impact of Aadhaar's use-cases in curbing leakages and improving service delivery in India's social protection programmes is an area for future research. Central and state governments report large savings in social protection programmes from digitisation and removal of fake beneficiaries, partly due to the use of Aadhaar.[11] However, a portion of these savings may accrue from the exclusion of genuine beneficiaries.[12] In addition, the governments of Andhra Pradesh and Telangana report that some beneficiaries are facing transaction difficulties when trying to access benefits using Aadhaar-enabled authentication devices.[13] These reports, while indicative, do not provide a comprehensive view of Aadhaar's current role in India's social protection. A comprehensive learning agenda and more open data are essential to understanding whether and how Aadhaar can be used to provide social protection in India.

In this Chapter, we review these topics in more depth. First, we provide a brief overview of social protection in India. Next, we discuss the role of Aadhaar in social protection, and its current state of adoption and performance. We conclude with an agenda for future research aimed at generating useful information for practitioners.

Social Protection in India

The government intends for India's social protection programmes to reach a majority of the country's population.[14] Through these schemes, the government seeks to provide economic security and protection from adverse shocks to India's poor.

Social protection in India takes many forms and is administered through hundreds of central and state government programmes. For this Chapter, we focus on four important programmes of the central government; together, these four account for more than two-thirds of national social protection spending.[15] We highlight these programmes, given their extensive use of Aadhaar. We list them below and describe them in more detail in Figure 5.1:

1. Food subsidy: Public Distribution System (PDS), dispensing foodstuffs and cooking fuel,
2. Employment guarantee: Mahatma Gandhi National Rural Employment Guarantee Scheme (MGNREGS),
3. Essential commodity subsidy: Cooking fuel subsidy on Liquefied Petroleum Gas (LPG), and,
4. Pensions: Cash transfers to vulnerable populations through the National Social Assistance Programme (NSAP). State-level pension programmes are also discussed where appropriate.

While India's social protection programmes provide welfare support to millions of individuals, their impact is constrained by several challenges. A major issue is

Figure 5.1: Four major social protection programmes in India

1. **Food subsidy:** Subsidised foodstuffs and cooking fuel (including rice, wheat, coarse grains, sugar, and kerosene)[16] are provided at government-licensed shops in most villages and urban neighbourhoods in India. This is India's largest social protection programme and is popularly called the Public Distribution System (PDS). Central government spending on PDS in FY 2015-16 was ₹1,39,419 crore ($20.8 billion).[17]

2. **Employment guarantee:** The Mahatma Gandhi National Rural Employment Guarantee Scheme (MGNREGS) assures employment opportunities in rural areas at minimum wages for 100 days a year to anyone who opts in. In drought-prone districts, the guarantee is up to 150 days. The programme is designed for the poor to self-select into it since only those who do not have an alternative to accepting minimum wages will avail themselves of the guarantee. The central government expenditure for MGNREGS was ₹37,341 crore ($5.6 billion) in FY 2015-16.[18]

3. **Essential commodity subsidy:** Cooking gas, in the form of liquefied petroleum gas (LPG), is provided at subsidised rates by India's three nationalised petroleum companies. It is largely an urban household subsidy – albeit increasing in its rural coverage – and usually collected by those who can afford a gas stove. Starting in 2015, the government replaced an in-kind subsidy with a cash subsidy. This programme is called PAHAL. Central government spending for PAHAL was ₹19,802 crore ($3 billion) and for the entire LPG programme was ₹21,803 crore ($3.3 billion) in FY 2015-16.[19]

4. **Pensions:** Under the National Social Assistance Program (NSAP), small monthly cash transfers are provided to the more vulnerable amongst the poor: the elderly, widows, and the disabled. The amounts can be small; for instance, a 70-year-old widow who is below the poverty line in Bihar, one of India's poorest states, is entitled to ₹300 (about $4.60) per month.[20] This amount is equivalent to about one-third of India's monthly rural poverty line.[21] The central government expenditure for NSAP in FY 2015-16 was ₹8,616 crore ($1.3 billion).[22] Many state governments use their own funds to run separate pension programmes or top up the amounts received from the central government.

Subsequent to the passage of the Aadhaar Act 2016,[23] the government can require the use of Aadhaar for social protection provision, including these four programmes. Since the Act came into effect, government agencies have issued circulars detailing these requirements.[24]

More information on Aadhaar's role in these programmes is provided at the end of this chapter in the Appendix.

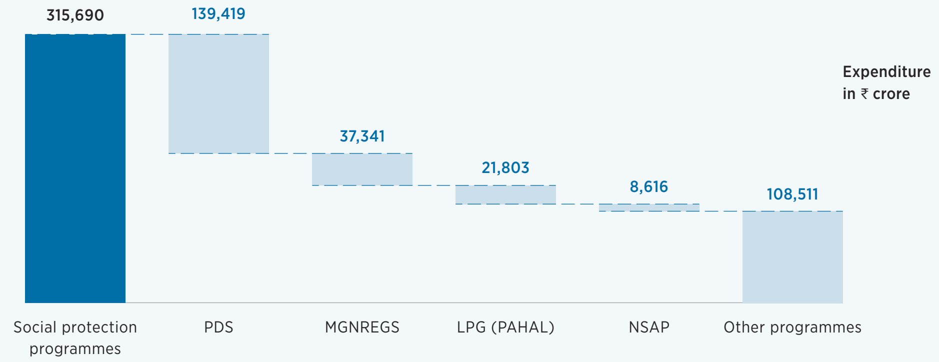
financial leakages. According to the *Economic Survey 2016-17*, an annual publication of the Finance Ministry, 36 percent and 20 percent of PDS and MGNREGS funds, respectively, leak from the system.[25] One of the ways funds leak is through siphoning by intermediaries through duplicate or "ghost" beneficiaries.[26,27] Intermediaries and layers of bureaucracy may also lead to delays in delivering foodstuffs or transferring benefit payments.[28] In the financial year (FY) 2016-17, more than half of the wage payments under MGNREGS were delayed.[29]

Aadhaar and Social Protection

According to the government, Aadhaar can help address the leakage problem in India's social protection programmes in three ways. One, fake beneficiaries and duplicates can be removed by linking a person's (unique) Aadhaar number to her or his identity record in each programme's database.[30] Two, Aadhaar-enabled electronic transactions can authenticate each beneficiary using her or his biometrics, thus reducing the potential for fraudulent transactions.[31] Three, Aadhaar enables direct benefit transfers (DBTs) to beneficiary bank accounts, which can reduce siphoning by middlemen and payment delays.[32] In Figure 5.2, we illustrate which of these use-cases apply to which of the four focal programmes, and their associated budget expenditure in financial year 2015-16.

An additional benefit of Aadhaar, according to the Unique Identification Authority of India (UIDAI), is that it can serve as a common identification platform and provide access to social protection programmes across India, and not just in an individual's home state.[33] This can be particularly valuable for migrants. However, we do not examine this channel because the government's social protection benefits have yet to incorporate this feature in a significant manner.[34]

Figure 5.2: Budget expenditure and role of Aadhaar in major social protection programmes, Apr 2015 – Mar 2016

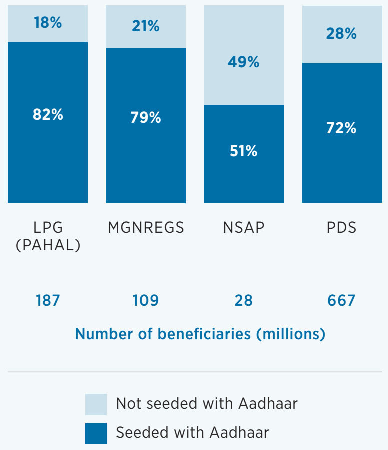


	PDS	MGNREGS	LPG (PAHAL)	NSAP	Other programmes
Aadhaar seeding	Yes	Yes	Yes	Yes	
Transaction authentication	Yes	Yes	No	Yes	
Direct Benefit Transfer	Pilot	Yes	Yes	Yes	

Notes: "Social protection programmes" comprise of the largest Government of India programmes that include income augmenting cash transfers to the poor or subsidies for the basic needs of food and housing. This is a lower bound estimate. "Other programmes" includes fertiliser subsidy, ICDS, Mid-Day Meals, and Pradhan Mantri Awaas Yojana.

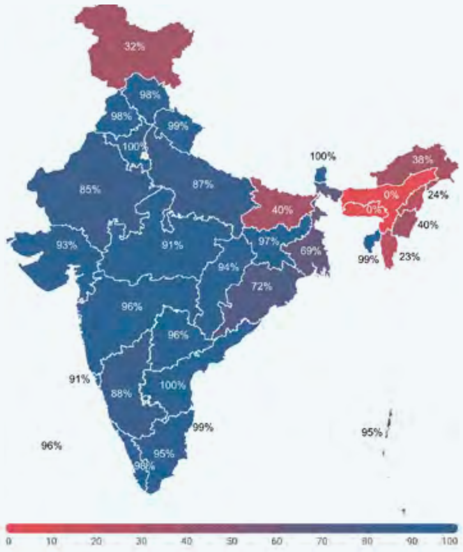
Data sources: Open Budgets India; DBT portal; APOnline portal; TSOnline portal; AePDS AP portal; NSAP portal

Figure 5.3: Percentage of Aadhaar seeding in four social protection programmes, as of Dec 2016



Notes: Seeding data is from 31 December 2016 for LPG, MGNREGS and NSAP, and 27 December 2016 for PDS. Total beneficiaries for PDS was calculated using data from central and state government PDS portals.
Data sources: PDS: Food and Civil Supplies Annual Report, central and state govt. PDS portals. LPG, MGNREGS, NSAP: DBT portal

Figure 5.4: State-wise distribution of the proportion of MGNREGS beneficiaries seeded with Aadhaar, as of Mar 2017



Data source: MGNREGS MIS portal, Aadhaar Demographic Verification Report

In the following three sections, we detail the three potential channels to use Aadhaar for social protection: Aadhaar seeding to remove fake beneficiaries; authentication to verify beneficiaries during transactions; and DBTs to reduce intermediaries and payment delays.

Aadhaar Seeding to Remove Fake Beneficiaries

Role of Aadhaar

According to the UIDAI, seeding Aadhaar numbers to the databases of social protection programmes can help remove duplicate and "ghost" beneficiaries from programme lists.[35] This in turn can reduce the potential of intermediaries to siphon benefits in the name of these fake beneficiaries, leading to savings for the government.[36,37]

To eliminate fake beneficiaries in programme databases—using Aadhaar—the government follows a two-step process. First, beneficiary lists are digitised.[38] Some programmes, like MGNREGS, already have digitised records. For older social protection programmes, however, beneficiary lists are maintained locally and need digitisation. In the second step, known as Aadhaar seeding, each beneficiary's record in the programme's database is linked to her or his Aadhaar number.[39]

Adoption of Aadhaar

About three-quarters of the beneficiaries enrolled in the four social protection programmes we discuss have already been seeded with Aadhaar.[40] In Figure 5.3, we show how this varies by programme, from 51 percent to 82 percent. For programmes with a high ratio of Aadhaar seeding, most states—except those in eastern India—have seeded evenly. We illustrate in Figure 5.4 the interstate variation of Aadhaar seeding of MGNREGS beneficiaries. The map looks similar for PDS as well.[41]

Performance of Aadhaar

The Indian government cites large savings in its safety nets portfolio through the removal of ineligible or fake beneficiaries. According to the DBT portal of the Government of India, ₹14,000 crore ($2.1 billion) was saved in the provision of food subsidies by removing 23.3 million fake beneficiaries.[42] The corresponding figure for cooking gas subsidies was ₹26,000 crore ($3.9 billion) and 35 million duplicates.[43] However, according to the Comptroller and Auditor General of India, a body that audits government finances, total savings for cooking gas subsidies were ₹1,764 crore ($263 million).[44] The data and methodology with which the government calculated these savings figures are not in the public domain for all programmes.

Aadhaar's role in the savings in PDS and LPG, however, may be limited. By 2014, the total number of duplicates eliminated in PDS was 12 million, of which about 2 million were removed using Aadhaar.[45] More recent data on Aadhaar's role in the savings reported by the DBT portal is not available.

The process of seeding each beneficiary's Aadhaar number to a programme's database can lead to unintended exclusion. This can happen through three channels: clerical errors in data entry; inability to reach certain individuals (if they are away from home, cannot travel, or reside in remote areas) to ascertain their Aadhaar number; and inability to include individuals who do not have an Aadhaar number. The extent of exclusion and the contribution of each of these three channels, is an important area of future research.

Authentication to Verify Beneficiaries During Transactions

Role of Aadhaar

The UIDAI can digitally authenticate the identity of an individual using their biometrics. For field-level transactions, such as the provision of food rations or wages in cash, an authentication device can be set up in a distribution centre to verify each beneficiary's transaction.[46] According to the UIDAI, authenticating each transaction digitally makes it difficult for officials and middlemen to siphon entitlements by fudging identity records, thereby helping to curb leakages.[47]

Adoption of Aadhaar

Currently, three of the four programmes use Aadhaar for field-level transaction authentication: PDS, MGNREGS, and NSAP. In the case of PDS, 35.5 percent of the shops in India designated to deliver the subsidy now have electronic point of sale (ePoS) devices, and are therefore capable of authenticating beneficiaries for each transaction.[48] Similar statistics for the MGNREGS and NSAP are not available.[49] In Figure 5.5, we highlight the wide variation in the adoption of ePoS devices in PDS shops across states.

Performance of Aadhaar

While Aadhaar authentication may reduce leakages, it can also result in beneficiaries—about one in seven in Andhra Pradesh and Telangana over FY 2016-17—facing transaction failures on Aadhaar-enabled ePoS devices. This does not automatically lead to exclusion of beneficiaries from getting access to their benefits, as officials are allowed to manually override the system using paper-based authentication and processes.[50]

Authentication failures can take place in three ways.[51]

One, biometric mismatches can lead to a failure in authentication. Fingerprint quality can diminish over time (for example, because of manual labour) or change because of injury, resulting in the Aadhaar database rejecting the print.[52] Intact fingerprints may also go unrecognized because of faulty capture at the time of the transaction.[53] Biometric errors may also reflect fraudulent authentication attempts, which is precisely what the authentication process is attempting to eliminate. According to data available from the governments of Andhra Pradesh and Telangana, biometric mismatches caused 85.9 percent of total authentication failures for the financial year 2016-17.[54] See Figure 5.6 for a breakdown, by programme, of the reasons for authentication failures.

Figure 5.5: State-wise distribution of ePoS devices in PDS shops, as of Mar 2017

STATES AND UNION TERRITORIES	TOTAL PDS SHOPS	% OF PDS SHOPS WITH ePoS DEVICE
Andhra Pradesh	28,546	100.0%
Dadra & Nagar Haveli	62	100.0%
Daman & Diu	51	100.0%
Madhya Pradesh	22,401	100.0%
Rajasthan	25,685	100.0%
Tamil Nadu	34,773	100.0%
Gujarat	17,237	99.1%
Chhattisgarh	12,350	98.6%
Haryana	9,631	97.5%
Jharkhand	23,379	87.1%
Andaman & Nicobar	509	57.0%
Karnataka	20,497	18.9%
Maharashtra	51,259	16.4%
Telangana	17,159	9.5%
Goa	447	9.4%
Odisha	13,844	7.8%
Sikkim	1,421	1.4%
Tripura	1,798	1.4%
Delhi	2,254	1.2%
Uttar Pradesh	79,402	0.9%
Bihar	42,117	0.1%
Uttarakhand	9,212	0.1%
Arunachal Pradesh	1,731	0.0%
Assam	38,794	0.0%
Himachal Pradesh	4,877	0.0%
Jammu & Kashmir	5,970	0.0%
Kerala	14,335	0.0%
Lakshadweep	39	0.0%
Manipur	2,052	0.0%
Maghalaya	4,651	0.0%
Mizoram	1,268	0.0%
Nagaland	1,691	0.0%
Punjab	16,657	0.0%
West Bengal	20,278	0.0%
Total	**526,377**	**35.5%**

Notes: Chandigarh, Puducherry, and Dadra & Nagar Haveli (partially) are conducting a pilot of Direct Benefit Transfers in lieu of in-kind PDS benefits. The period of this data is not available. The data was presented in Parliament on April 2017.
Data source: Response to Lok Sabha Unstarred Question 6046: PoS devices in Fair Price Shops

Two, in some cases, an individual's biometrics are missing from the Aadhaar database, or the beneficiary's Aadhaar enrolment stands cancelled or inactive. It is unclear why these issues occur. Of the total transaction failures highlighted in the Andhra Pradesh and Telangana data, 4.0 percent can be attributed to such issues.[55]

Finally, server-related errors and other operational bottlenecks can also lead to transaction failures.[56] In Andhra Pradesh and Telangana, these reasons account for 10.1 percent of total failures.

Data from the governments of Andhra Pradesh and Telangana permit trend analysis of the percentage of unique persons facing failed transactions. For pensioners in Andhra Pradesh, from April 2015 to March 2017, the percentage of individuals facing authentication failure despite repeated attempts has varied considerably, with an average of 17.4 percent. During the same time period, the failure rate has increased and averaged 7.8 percent for MGNREGS in Telangana. While these numbers are for fingerprint authentication, they are slightly lower for iris authentication. In 2011-12, when the UIDAI tested authentication processes, it expected only one percent of beneficiaries to face such difficulties.[57] The trends in authentication failures faced by beneficiaries are illustrated in Figure 5.7.

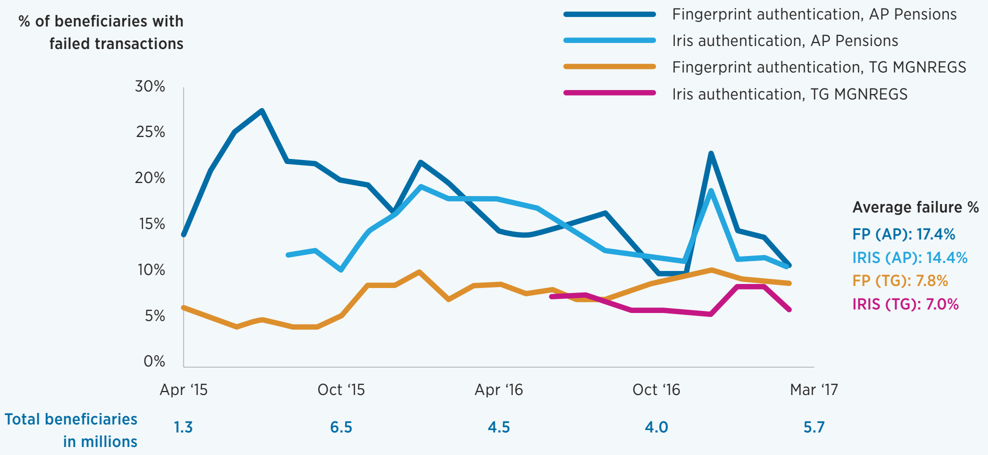
As mentioned above, authentication failures do not automatically translate into exclusion. Field-based empirical evidence on the extent of exclusion, if any, owing to Aadhaar—and its contributing factors—is a vital area of future research. Furthermore, the political economy of curbing leakages by intermediaries using Aadhaar-enabled authentication, and the consequences of the same, are also important to explore.

Figure 5.6: Reasons for authentication failure of transactions on Aadhaar-enabled devices in Andhra Pradesh and Telangana, Apr 2016 – Mar 2017

CATEGORY OF FAILURE REASONS	PENSIONS (ANDHRA PRADESH)	MGNREGS (TELANGANA)	MGNREGS (ANDHRA PRADESH)	WEIGHTED AVERAGE
Biometric mismatches	84.2%	94.8%	84.3%	85.9%
Aadhaar database related errors	15.7%	2.2%	2.3%	4.0%
Server connectivity and operational errors	0.1%	3.0%	13.4%	10.1%

Notes: The three categories have been grouped from 86 error codes provided by the UIDAI for authentication failures. Biometric mismatches may also include fraudulent attempts. Total number of transaction failures were used to calculate the weighted average. Data is not available for pensions in Andhra Pradesh for April 2016. Pensions (Andhra Pradesh) refers to the NTR Bharosa programme, while data for MGNREGS in Telangana and Andhra Pradesh also includes Social Security Pensions data from the two states.
Data sources: MGNREGS (Telangana): TSOnline portal, Pensions (Andhra Pradesh): NTR Bharosa portal, MGNREGS (Andhra Pradesh): APOnline portal

Figure 5.7: Percentage of beneficiaries with failed transactions, after multiple attempts, using fingerprint and iris in Andhra Pradesh and Telangana, Apr 2015 – Mar 2017



Notes: AP & TG refer to Andhra Pradesh and Telangana, respectively. Pensions AP refers to the NTR Bharosa programme, while data for MGNREGS TG also includes Social Security Pensions data.
Data sources: MGNREGS TG: TSonline portal, and Pensions AP: NTR Bharosa portal

Direct Benefit Transfers to Reduce Intermediaries

DBTs refer to the electronic transfer of funds from the government to an individual's bank account. Central and state-level governments have steadily transitioned existing cash-based social protection programmes (like MGNREGS or NSAP) to DBTs or have converted in-kind social protection programmes to equivalent-value DBTs (like the PAHAL initiative with LPG - refer to Figure 5.3). Chandigarh, Puducherry, and parts of Dadra and Nagar Haveli are also piloting the transition of in-kind social protection of PDS into cash.[58] Currently, the government has highlighted 499 social protection programmes as "DBT-eligible," of which 243 have converted to DBT payments. In Figure 5.8, we show the increasing trend in this transition since March 2015.

Role of Aadhaar

By enabling DBTs, the government states that Aadhaar can help curb leakages.[59] Using the Aadhaar Payment Bridge System (APBS), the government can directly transfer benefits to uniquely identified individuals' bank accounts. This can eliminate fake beneficiaries, and certain tiers of intermediaries, potentially reducing their ability to siphon funds.[60]

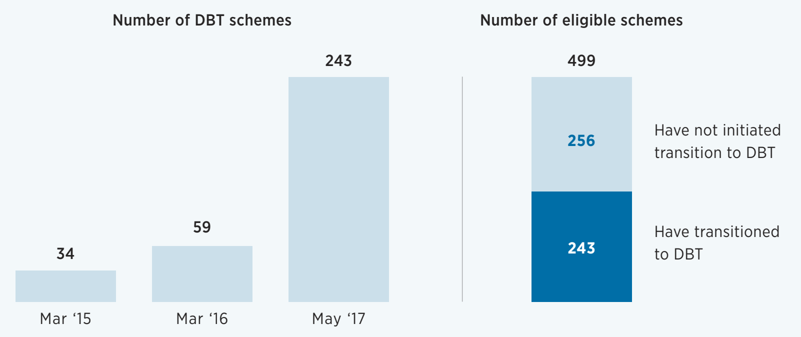
Removing bureaucratic layers can also reduce payment delays.[61] Using another Aadhaar technology that powers microATMs, Aadhaar Enabled Payment Systems (AEPS), business correspondents are able to deliver cash from DBTs directly to an individual's home or nearby location.[62] To learn more about APBS, AEPS, and microATMs, please refer to Chapter 4, *Financial Inclusion.*

The administrators and beneficiaries of social protection programmes undertake three steps before they can transition to Aadhaar-based cash transfers. First, each beneficiary should have a bank account (Aadhaar facilitates this using e-KYC, see Chapter 4, *Financial Inclusion*).[63] Second, the beneficiary's bank identification number[64] and Aadhaar number needs to be added to the social protection programme's database. Third, the individual's bank account should be linked to Aadhaar (if it isn't already).

Adoption of Aadhaar

DBTs do not depend exclusively on Aadhaar and can be sent through other platforms. It is possible to send funds directly to individual bank accounts using the National Electronic Funds Transfer (NEFT) and other means.[65] While the proportion of APBS-enabled payments is increasing, they are still a minority compared with other forms of electronic transfer, such as NEFT. See Figure 5.9 for a breakdown, by programme, of this trend. Similarly, business

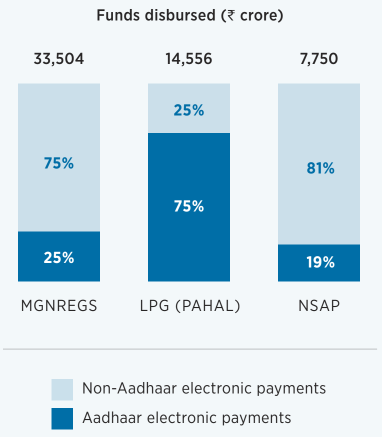
Figure 5.8: Growth in number of schemes transitioning to DBT, Mar 2015 – May 2017



Data source: DBT Portal; accessed 26 May 2017.

correspondents are able to provide doorstep-banking services using other handheld devices that do not use Aadhaar's biometric capabilities.[66]

Figure 5.9: Proportion of electronic payments using Aadhaar and non-Aadhaar payment systems, Apr 2016 – Mar 2017



Note: For MGNREGS, LPG, and NSAP, the electronic payments form 70.5, 66.8, and 81.6 percent, respectively, of the total budget allocation for these programmes in FY 2016-17.
Data sources: DBT portal, Open Budgets India

Performance of Aadhaar

More research is required on Aadhaar's performance in facilitating provision of social protection programmes through DBTs in India. It is valuable to understand whether and how the transition to Aadhaar-enabled DBTs, compared with other forms of electronic transfers, can lead to further reductions in leakage, minimize payment delays, and improve the overall experience for beneficiaries.

Areas for Future Research

Aadhaar has a significant and expanding role in India's social protection programmes. The government aims to use Aadhaar to reduce leakages and improve service delivery. In order to answer the government's questions on whether and how Aadhaar can improve social protection outcomes, we recommend a practitioner-oriented research agenda, combined with more publicly available data.

In particular, a practitioner-oriented research agenda can provide actionable insights for administrators at the centre and state levels on a) how to strengthen implementation, b) whether and how much Aadhaar can curb leakages and improve service delivery in a particular context, and c) reduce any unintended consequences, such as exclusion of genuine beneficiaries.

To this end, we outline three important themes for future research in social protection that can be directly useful for practitioners today:

- Representative estimates on whether genuine beneficiaries are excluded and, if so, what the contributing factors are: to design strategies that reduce exclusion

- Research on implementation topics related to Aadhaar; for example, technology preparedness, beneficiary time-use and experience, personnel training, and connectivity infrastructure: to strengthen implementation

- Evaluations that examine the impact of each Aadhaar use-case on financial leakages and service delivery: to facilitate decisions on which use-cases to expand

More publicly available data on Aadhaar use-cases—especially transaction or beneficiary-level data (after appropriate anonymisation)—will help advance such research. Practitioners releasing more data will enable researchers to uncover important empirical insights. These in turn can benefit practitioners to improve implementation strategies, creating a positive cycle of collaboration.

To maximise the impact of practitioner-oriented research, we recommend:

- Framing research questions in collaboration with practitioners
- Being responsive to decision-making schedules and other practitioner constraints
- Presenting insights in succinct documents and in-person meetings
- Providing follow-up support to translate research to action on-the-ground

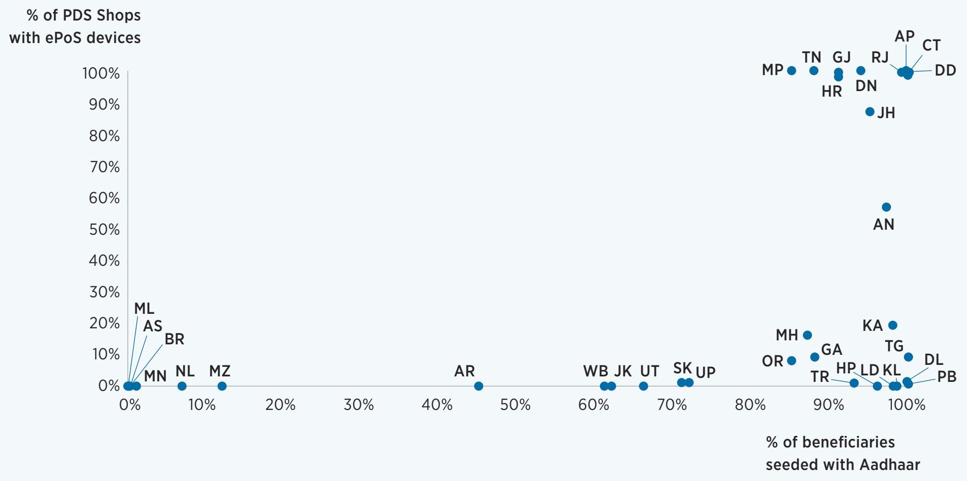
APPENDIX 5.1: Spotlight on PDS

Food subsidies—subsidised foodstuffs and cooking fuel, including: rice, wheat, coarse grains, sugar, and kerosene[67]—are provided at government-licensed shops in most villages and urban neighbourhoods in India. This is India's largest social protection programme and is popularly called the Public Distribution System (PDS). Central government spending on PDS in FY 2015-16 was ₹1,39,419 crore ($20.8 billion).[68] As of March 2017, there were 232 million ration cards (the identification document—one for each family—required for PDS) in India.[69] The total food grain allocated under the PDS in 2015-16 was 52.34 million tonnes, of which 94.8 percent was utilised by the system.[70]

In February 2017, the Department of Food and Public Distribution issued a notification stating that an eligible beneficiary is "required to furnish proof of possession of Aadhaar number or undergo Aadhaar authentication."[71] Those who do not possess an Aadhaar number are required to make an application by 30 June 2017.[72]

With this notification in place, Aadhaar is being used for seeding beneficiaries to PDS databases, for transaction-level authentication and, in a limited way in certain union territories,[73] for direct benefit transfers. As mentioned in the chapter, about 72 percent of PDS ration cards have been linked to Aadhaar and 35 percent of PDS shops have ePoS machines. There is, however, large inter-state variation in the adoption of Aadhaar in the PDS. In Figure 5.10, we illustrate that there is a cluster of states (in the top-right) where most shops are equipped to use Aadhaar for transaction authentication and most beneficiaries have been seeded with Aadhaar. These states can or already do use Aadhaar for PDS delivery. For almost all the remaining states, only a small proportion of shops are equipped with ePoS devices.

Figure 5.10: State-level variation in Aadhaar usage in PDS



Data source: Food and Civil Supplies Annual Report, Question No. 6046 in Lok Sabha

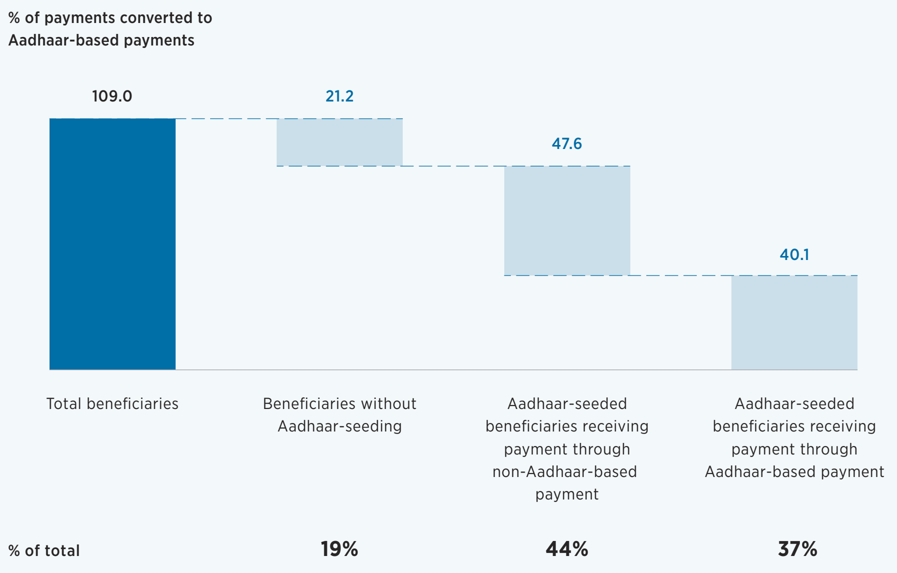
APPENDIX 5.2: Spotlight on MGNREGS

The Mahatma Gandhi National Rural Employment Guarantee Scheme (MGNREGS) assures employment opportunities in rural areas at minimum wages for 100 days per year to anyone who opts in. In drought-prone districts, the guarantee is up to 150 days. The programme is designed for the poor to self-select into it since only those who do not have an alternative to accepting minimum wages will avail themselves of the guarantee. The central government expenditure for MGNREGS was ₹37,341 crore ($5.6 billion) in FY 2015-16.[74] Through this programme, the government provided employment to 72.3 million beneficiaries in 2016-17.[75]

Aadhaar is used in the MGNREGS for seeding of beneficiaries, transaction-level authentication, and direct benefits transfer. While nearly 81 percent of the 109 million beneficiaries have been seeded with their Aadhaar number, only about 37 percent receive their payments through Aadhaar-based methods (see Figure 5.11). The majority of Aadhaar-seeded beneficiaries continue to receive their wages through the electronic fund management system (e-FMS), cash, or other modes of payments. Under the e-FMS, the funds are disbursed to the master account of the nodal bank, which then credits the accounts of the beneficiaries.[76]

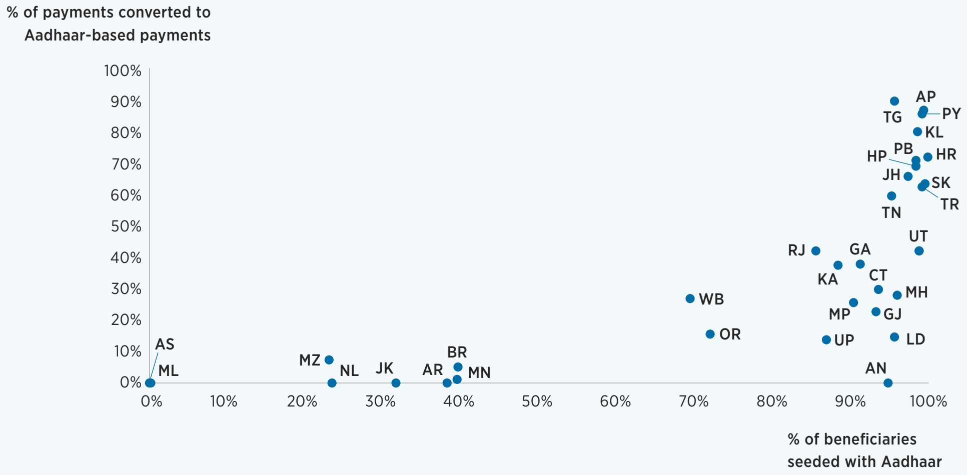
As we illustrate in Figure 5.12, there is significant inter-state variation in the usage of Aadhaar for the MGNREGS. On the right side of the figure, we see that a large number of states have high percentages of beneficiaries seeded with Aadhaar; however, there is high variation among the states in terms of the percentage of Aadhaar-based payments.

Figure 5.11: Aadhaar Usage in MGNREGS, as of Mar 2017



Data source: MGNREGS MIS

Figure 5.12: State-level variation in Aadhaar usage in MGNREGS, as of Mar 2017



Data source: MGNREGS Portal: Aadhaar Demographic Verification Status Report

APPENDIX 5.3: Spotlight on LPG PAHAL

Cooking gas, in the form of liquefied petroleum gas (LPG), is provided at subsidised rates by India's three nationalised petroleum companies, referred to as Oil Marketing Companies (OMCs). These three companies service nearly 181 million active LPG connections in the country, resulting in a national LPG coverage of 71.7 percent as of March 2015.[77,78] The coverage in rural areas, 46 percent, is lower than the national average.

In 2015, the government introduced PAHAL, a scheme to replace the earlier in-kind subsidy with a monetary subsidy. Under this scheme, consumers get LPG cylinders at non-subsidised prices and receive the subsidy, as per their entitlement, directly into their registered bank accounts.[79] Central government spending for PAHAL was ₹19,802 crore (about $3.3 billion) in FY 2015-16.[80]

Aadhaar is used for de-duplication and direct benefits transfer (DBT) under the PAHAL scheme. Before approving a new connection to a prospective consumer, de-duplication is carried out within and between the OMCs. Once approved, the consumer can then purchase LPG cylinders from the OMCs. A DBT is done electronically within 48 hours of purchase. According to the Ministry of Petroleum and Natural Gas, from inception of the scheme to July 2016, of the 1.7 billion transactions, 98.4 percent were successful in transferring money to the bank accounts of the consumers.[81] One of main reasons for the failures was the "involvement of several stakeholders like LPG distributors, the National Payments Corporation of India and banks in the subsidy transfer process."[82] Another reason given was the mismatch between datapoints on bank account details, Aadhaar number, and the LPG consumer number.[83]

6 | EMERGING USES

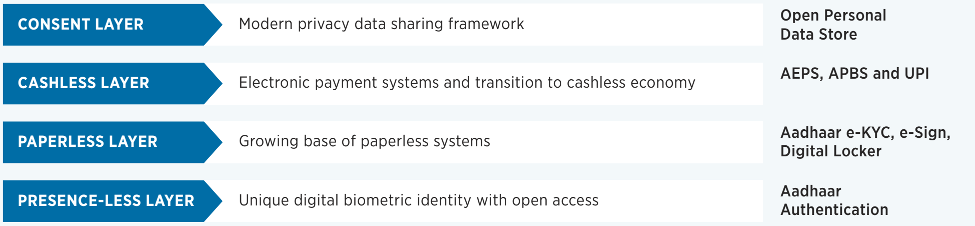
Aadhaar's identity platform has encouraged experimentation and creativity in applications across the public and private sectors. A diverse set of uses has emerged in health, education, and governance, among other sectors. The evolution, operational performance, and impact of these emerging applications are important areas for further understanding.

Identification and authentication of individuals—Aadhaar's key services—are required in almost every sector of the modern economy. Two sectors that are using Aadhaar at scale are financial inclusion and social protection, highlighted in Chapters 4 and 5, respectively. However, newer uses of Aadhaar are emerging in a diverse set of other arenas, including health and education. We will explore a variety of these uses in this Chapter.

In addition, we will discuss the crosscutting set of applications, called "India Stack," that enable these emerging uses (see Figure 6.1). The India Stack is a set of open Application Programming Interfaces (APIs),[1] which aim to employ India's expanding digital infrastructure to improve service provision for both the public and private sectors.[2]

Innovation is rapid, and this Chapter provides an illustrative list of the new uses being piloted and introduced in this area. Not much data exists on the emerging uses discussed below. Therefore, we rely on the stated aims and benefits of each application as outlined by official sources—generally the Government of India. Once data on adoption and performance is available, researchers and consumers alike will be able to determine if the stated benefits have been fully realised.

Figure 6.1: India Stack layers



CONSENT LAYER	Modern privacy data sharing framework	Open Personal Data Store
CASHLESS LAYER	Electronic payment systems and transition to cashless economy	AEPS, APBS and UPI
PAPERLESS LAYER	Growing base of paperless systems	Aadhaar e-KYC, e-Sign, Digital Locker
PRESENCE-LESS LAYER	Unique digital biometric identity with open access	Aadhaar Authentication

JAM (Jan Dhan, Aadhaar, Mobile) serves as a supporting function for all layers.

Data source: Adapted from IndiaStack.org

India Stack Applications

There are five main Aadhaar technologies making up the India Stack: Aadhaar Authentication, Electronic Know Your Customer (e-KYC), Unified Payment Interface (UPI), DigiLocker, and Electronic Signature (e-Sign). Authentication is discussed extensively in Chapters 2 and 5, *Aadhaar Architecture* and *Social Protection*, respectively. E-KYC and UPI are explored in Chapter 4, *Financial Inclusion*. They are also described in Figure 6.2. DigiLocker and e-Sign are uses we introduce below.

DigiLocker

DigiLocker is a cloud-based storage platform or "locker." Launched in 2015, DigiLocker enables users to store, receive, and request documents digitally. Individuals are granted 1 GB of cloud storage space, which they can voluntarily link to their Aadhaar number. The advantage of linking to Aadhaar is that, when linked, the locker serves three functions in addition to just providing storage space.

An Aadhaar-linked DigiLocker has "push," "pull," and "request" functionalities.[3,4,5] With the "push" function, authorised *issuers* push documents to users through the locker.[6] One example is UIDAI, which became an authorised issuer on the DigiLocker platform in early 2017, allowing users to download a digital copy of their Aadhaar card (known as eAadhaar). As of May 2017, there were 28 registered issuers.[7]

Registered individuals can also "pull" documents into their lockers from official sources. One example is the Ministry of Road Transport and Highways, which is authorised to issue digital driving licenses and vehicle registrations when an individual enters a registration number and other details.[8]

With the "request" function, authorised *requesters* ask for access to official documents through their websites, allowing individuals to load a stored document, which can then be submitted as part of an application or official record. The user receiving the request maintains control of her or his own documents and can decide to share or not share them. As of May 2017, there were eight registered requesters.[9] One example is the National Employment Service of Kerala.

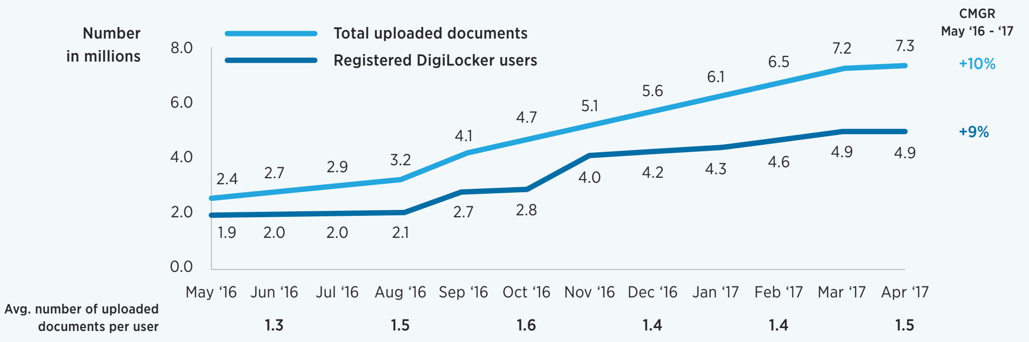
As discussed, to use these three functions, individuals must link their Aadhaar numbers to their DigiLocker accounts. If a locker is not linked with an Aadhaar number, then the cloud space only serves as digital

Figure 6.2: India Stack technologies

AUTHENTICATION	Aadhaar authentication is the process wherein an Aadhaar number, along with other attributes, including biometrics, are submitted online to the CIDR for its verification on the basis of information or data or documents available with it.
E-KYC	Aadhaar e-KYC is a paperless Know Your Customer (KYC) process, wherein the identity and address of the subscriber are verified electronically through Aadhaar authentication.
UPI	Unified Payment Interface (UPI) enables all bank account holders in India to send and receive money instantly from their mobile phones without the need to enter bank account information or net banking user-ID/password.
DIGILOCKER	DigiLocker, or Digital Locker, is a platform for digital issuance and verification of documents and certificates, thus eliminating the use of physical documents.
E-SIGN	e-Sign allows applications to replace manual paper-based signatures by integrating an API that allows an Aadhaar holder to electronically sign a form/document anytime, anywhere, and on any device legally in India.

Source: IndiaStack.org (with minor edits from authors)

Figure 6.3: Cumulative number of registered users and uploaded documents on DigiLocker, May 2016 – Apr 2017



Data Source: DigiLocker Dashboard

storage for documents uploaded independently by the user.

In Figure 6.3, we highlight the growth of DigiLocker in number of users as well as user-uploaded documents since May 2016. The number of registered users on DigiLocker is low relative to estimated Internet users in India, constituting only about 1.4 percent of the estimated 350 million Internet users in India.[10] Only 39 percent of registered DigiLocker users (about 1.9 million) have linked their Aadhaar number to their DigiLocker account.[11] This means that only 0.5 percent of Internet users have an Aadhaar-enabled DigiLocker account.

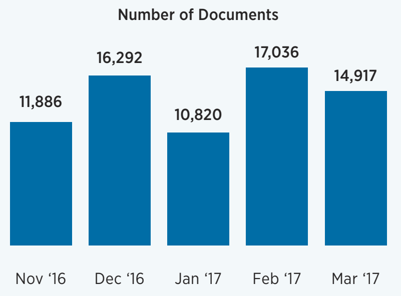
DigiLocker is one example of a Digital Locker, which is part of the Digital India initiative.[12] In March 2017, the Digital Locker Authority[13] published an advertisement for other parties to become a Digital Locker Service Provider, to encourage further developments in the area of digital documents.[14]

e-Sign

E-Sign is a process that allows a user to digitally sign an electronic document using Aadhaar authentication. The e-Sign feature can be used on a website or an application, allowing users to authenticate themselves either through a compatible biometrics device or by typing in a One Time Password (OTP) issued to the mobile number associated with the user's Aadhaar number. Successful e-signing of a document will issue a digital certificate, which is a document recognized by the Controller of Certifying Authorities, and is compliant with the Information Technology Act of 2002, and thus legally valid.[15] According to the India Stack, the advantages of using e-Sign are lower costs and added convenience to users.[16]

As of early April 2017, the number of e-signed documents on DigiLocker totaled 382,195. E-Signed documents account for only 5 percent of total user-uploaded documents on DigiLocker.[17] In Figure 6.4, we offer a snapshot of uploads of e-signed documents on DigiLocker over five recent months. The total number of e-signed documents—including documents not on the DigiLocker—is not readily available on any official public portal.

Figure 6.4: Monthly number of e-Signed documents uploaded onto DigiLocker by month, Nov 2016 – Mar 2017



Data Source: DigiLocker Dashboard

Health Sector

The health sector is using Aadhaar's applications—including authentication and Direct Benefit Transfers (DBTs)—in a wide variety of programmes. We highlight several of these use-cases below. Measuring performance of these use-cases, and their net benefits, is an important area of future research.

DigiLocker for Health Records

DigiLocker can be used in many applications, but a particularly relevant one could be digitising and storing electronic health records. The platform could become a place for patients to upload health and immunisation records, test results, and other medical documents for easy tracking and quick access. Hospitals can issue various records to an individual's account with their consent.

Unique Health Identity (UHID) and Online Registration System (ORS)

Unique Health Identity (UHID) is a digital identity issued by healthcare providers. The ID is intended to track patients as they move through a hospital system. It helps keep track of patients' records, including test results and previous appointments. A patient's UHID can now be linked to their Aadhaar number, which serves as a way for the individual to obtain access to their records, even if she or he loses or forgets the UHID. The Ministry of Health and Family Welfare has also expressed interest in promoting Aadhaar linkages to UHID to resolve instances of multiple UHIDs being issued to one patient.[18]

Patients with an Aadhaar number can also register for a medical appointment on the Online Registration System (ORS). ORS is currently being used by 81 public hospitals. The system processed about 5.7 million appointments between July 2015 and mid-May 2017.[19]

Health DBTs

Janani Suraksha Yojana (JSY) is a central government scheme whereby a small cash payment is directly deposited into the bank account of an eligible pregnant woman, using her Aadhaar number.[20]
The programme is targeted at low-income women, specifically those living in rural areas. The government has stated that beneficiaries are required to seed their Aadhaar number to the JSY scheme to receive a payment through DBT; however, data from the DBT Bharat Dashboard demonstrates that seeding of beneficiary data and payments transferred using the Aadhaar Payment Bridge System are each only at 10 percent as of March 2017.[21]

In addition, the government has identified the following schemes as being eligible for inclusion in the DBT platform[22] and for which Aadhaar linkage has not begun:

- **Integrated Child Development Services (ICDS):** ICDS is a scheme providing nutritional inputs for mothers and young children. The proposal is to send honorarium payments to frontline workers and helpers using the DBT platform.

- **Rajiv Gandhi National Creche Scheme for Children:** Also honorarium payment to workers.

Identification of target segments

Within the health sector, Aadhaar may also provide opportunities to better target vulnerable populations for additional health services.

HIV+ patients
The National Aids Control Organisation (NACO) has begun the process to link their "People Living with HIV" (PLHIV) database with Aadhaar numbers. NACO states that the link to Aadhaar will help beneficiaries get access to various schemes for which they are eligible, including health programmes, financial assistance, and social sector schemes. The project to link PLHIV with individuals' Aadhaar numbers is being tested in Delhi, with a phased scale-up planned after the pilot.[23]

In Chapter 3, *Legal and Governance Framework,* we briefly discuss Aadhaar-related concerns regarding privacy. Privacy becomes acutely important in situations where one's Aadhaar number may become linked to highly sensitive information—such as one's HIV status. Further research is needed to understand the appropriate safeguards required to ensure that vulnerable populations are protected from abuse of their information.

Elderly patients
In early 2017, the Minister of Finance announced the introduction of Aadhaar-based smart cards that would contain the health information of elderly people. The smart cards system for the elderly will be piloted in 15 districts in 2017-2018.[24]

Education Sector

Education is another sector where Aadhaar is being applied across a broad range of services. As with health, more empirical evidence on whether these use-cases achieve their intended goals—and whether there are any unintended consequences—are important issues for researchers to pursue.

DigiLocker for education records

DigiLocker can also be used within education. The Central Board of Secondary Education (CBSE) is a registered DigiLocker *issuer* and is authorised to share students' mark sheets, migration certificates, and passing certificates. Digital cloud storage allows students to obtain access to school records as needed. CBSE has issued more than 11 million documents onto DigiLocker. Of those, passing certificates and mark sheets comprise 57 percent of documents, and migration certificates comprise the rest.[25,26]

Registration for school enrollment and mid-day meals

As of March 2017, an Aadhaar number is required to enrol into Sarva Shiksha Abhiyan (SSA)—a scheme aiming to universalise primary education.[27] In addition, students are required to provide proof they possess an Aadhaar number to receive the mid-day meals (MDMs) provided through government primary schools in India.[28] The motivations listed for mandating Aadhaar for MDMs were transparency, efficiency of service delivery, simplification of the government delivery process, benefits directly reaching intended beneficiaries, and added convenience to beneficiaries. Those without an Aadhaar number will need to apply for a number. The deadline for enrolment is 30 June 2017.[30,31]

Registration for examinations

The Central Board of Secondary Education (CBSE) requires the use of Aadhaar to enroll for the National Eligibility cum Entrance Test (NEET) and the Joint Entrance Examination (JEE).[32] In response to a Parliamentary Question raised in the Lok Sabha, the government stated the following rationale for requiring Aadhaar for NEET: to increase accuracy of the applicants' details, to "help in ascertaining identity of the applicants at the examination centres in a convenient and hassle-free manner," and to eliminate the need for producing multiple documents as proof of identity.[33,34]

Scholarships

In 2016, Aadhaar was made compulsory as part of the application process for the following scholarship schemes: pre-matric, post-matric, and merit-cum-means.[35] The stated reasoning from the government is to make the process more transparent and to facilitate direct and timely transfers of scholarships. In response to a question submitted to the Lok Sabha, the government asserted that scholarships were not being denied in absence of an Aadhaar number—and that alternative identifiers could be used, such as a bank passbook.[36]

Aadhaar will also be required for scholarships dispersed by the University Grants Commission (UGC) in FY 2016-2017. Furthermore, UGC has been instructed to disburse the scholarship funds as Direct Benefit Transfers, which can leverage the Aadhaar Payment Bridge System (APBS) as a mechanism for payments.[37,38]

Governance Sector

Using DigiLocker for e-Districts

The Ministry of Electronics and Information Technology (MeitY) launched its e-District initiative in late 2015. MeitY conceptualised the project to enhance the district-level efficiencies of departments and to "...enable seamless service delivery" to citizens.[39] In particular, the e-District programme is targeting the creation of official certificates such as birth, income, domicile, caste, and death. As of April 2017, e-District programmes in six states are using DigiLocker to facilitate the dissemination of documents and have issued 56 million documents.[40]

Aadhaar-Enabled Biometric Attendance (AEBAS)

The Aadhaar-Enabled Biometric Attendance System (AEBAS) authenticates and records the attendance of registered employees on the system. Government offices or other registered organisations can use the system, supported by the UIDAI. The system logs the entry and exit of registered employees. This information is displayed in an anonymised fashion on a public dashboard.

Aadhaar-Linked Birth Registration (ALBR)

Aadhaar-Linked Birth Registration (ALBR) is a programme that provides an Aadhaar number—linked to a birth certificate—for newborns. For ALBR, healthcare workers are trained by the government to facilitate the enrolment. The government-stated benefits of the programme are: increased access to birth certificates through a Common Services Centre (CSC),[41] ease of tracking children for welfare schemes, and ease of integration for databases, such as the Mother Child Tracking System (MCTS).[42,43]

Private Sector

Owing in large part to the open nature of the APIs build around the India Stack, there are a growing number of Aadhaar applications within the private sector.

Telecommunications

In addition to the uses of e-KYC discussed in Chapters 2, *Aadhaar Architecture*, and Chapter 4, *Financial Inclusion*, Aadhaar e-KYC can also be used to open an account and activate a SIM card with telecommunications companies. According to official government communications, the use of e-KYC simplifies the requirements for the purchase of a SIM card and allows for "instant activation" of an account.[44] In the paper-based KYC process, customers provide copies of official documents, such as a passport, as proof of identity and proof of address, along with a passport-size photograph. Salespersons attach these documents to a customer acquisition form, and forward them to the subscriber database of the telecommunications provider.[45]

Since the introduction of e-KYC for telecommunications purposes, several companies have adopted this technology, including the three largest, accounting for more than 70 percent of the sector's market share.[46] Some telecom companies assert that 20 to 30 percent of the KYC for new mobile subscribers is done using Aadhaar e-KYC, and that 15 to 20 percent of their point of sales are equipped with e-KYC devices.[47] The adoption of this technology is expected to increase following the recent Supreme Court Order that requires telecommunications operators to complete re-verification of existing customers using e-KYC by February 2018.[48]

Background verifications

Aadhaar authentication can now be used for instant background checks through mobile applications using mobile One Time Password verification. Companies can use these applications to verify the identities of potential employees, customers, and vendors. Similarly, Aadhaar authentication can also be used to verify online identity, such as user profiles. Examples of organisations employing this technology include job sites, which use it to verify the authenticity of the information provided by candidates.[49]

Areas for Future Research

Applications of Aadhaar are proliferating at a rapid rate, and greater research is needed on the welfare impacts of each use case in various contexts. A precise understanding of the impact of these emerging schemes will help inform decisions-makers in government and the private sector on whether specific uses should be dropped, adjusted or expanded.

Two important themes for future research on emerging uses of Aadhaar are as follows:

- Research on which uses have been implemented well and which are facing challenges, especially in terms of take-up, efficiency, connectivity, and infrastructure
- Impact evaluations on the welfare effects of Aadhaar-linked uses compared to counterfactual comparisons with viable alternatives

Existing data on the uses and sectors outlined in this Chapter is limited. Public and private sector actors should be encouraged to release more data on the adoption of Aadhaar. This will promote faster feedback loops on the effectiveness of Aadhaar-enabled uses as well as opportunities to strengthen them.

To maximise the impact of practitioner-oriented research, we recommend:

- **Framing research questions in collaboration with practitioners**
- **Being responsive to decision-making schedules and other practitioner constraints**
- **Presenting insights in succinct documents and in-person meetings**
- **Providing follow-up support to translate research to action on-the-ground**

APPENDIX 6.1:
Reference Table for Emerging Uses

SECTOR	USE TYPE	PROGRAMME	DESCRIPTION
CIVIC GOVERNANCE	Authentication	Voter card	Voter ID cards linked to an individual's Aadhaar number to facilitate voting
	e-KYC	PAN card	PAN card linked to an individual's Aadhaar number to facilitate the payment of income tax
	e-KYC	Passport	Passport applicants can submit their Aadhaar number as a proof of identity and proof of address
	Authentication	Drivers license	Driver's license linked to Aadhaar to prevent individuals from possessing multiple licenses
	Authentication	Business registration (SMEs)	Small business owners can use their Aadhaar number to register their enterprise with the Ministry of Micro, Small, and Medium Enterprises
TRANSPORT	Authentication	Railway reservation verification	Aadhaar-based ticketing system for railway reservations intended to end fraudulent bookings and curb cases of impersonation
FINANCIAL TOOLS	e-KYC	Mobile wallet	Individuals can use their Aadhaar number as proof of identity to open mobile money accounts; they can also use Aadhaar e-KYC for account openings
	e-KYC	Insurance	Insurance applicants can submit their Aadhaar number as a proof of identity

7 | LOOKING AHEAD

The scope and usage of Aadhaar and Aadhaar-enabled tools will affect hundreds of millions of lives. Timely and rigorous research efforts—in active collaboration with practitioners—can provide insights and direction into how we build, govern, and use digital identity systems.

Key Takeaways from the *State of Aadhaar Report 2016-17*

As discussed throughout this report, more empirical research will be pivotal to inform how the Aadhaar architecture is governed and used across the economy. We believe this research is important, complex, and timely. It is important because it affects more than a billion Indian residents and interacts with almost every sector of the Indian economy. It is complex because digital identity research encompasses various fields—including economics, financial technology, computer science, sociology, and law—that need to work together to further our understanding. And finally, this is the right time for research because despite near universal coverage of adult Indian residents and a resulting proliferation of uses across various sectors, there remain important gaps in our understanding of Aadhaar. This is the right window to launch research efforts that can provide insights and direction to practitioners who build, govern, and use digital identity systems.

In Chapter 2 of this report we discuss Aadhaar's technological and administrative architecture:

- Researchers: This Chapter provides initial ideas for researchers interested in furthering how digital identity systems are built and maintained to achieve their goal of uniquely and efficiently providing identification services, while building in appropriate technological safeguards.
- Practitioners: It is also useful reading for practitioners using Aadhaar in their area of work. Moreover, this chapter is helpful initial reading for those looking to build similar systems for other governments. For instance, countries ranging from Bangladesh to Tanzania have sought the counsel of the Indian government to better understand the roll out of Aadhaar.[1] The references in this Chapter will also point to more detailed resources from the UIDAI.

In Chapter 3, on Aadhaar's legal and governance framework, we lay out Aadhaar's legal evolution:

- Researchers: Those interested in advancing understanding on whether and how digital identity systems should be regulated on topics such as privacy and data security will benefit from this overview and the areas of future research outlined in the chapter.
- Practitioners: This is also important reading for individuals seeking to understand the history and complexity of Aadhaar's legal framework, and how it may interact with the various uses of Aadhaar.

In Chapters 4 through 6 we discuss how Aadhaar is used in financial inclusion, social protection, and other emerging uses. According to the government, Aadhaar and its accompanying systems have the potential to streamline transaction processes, reduce payments leakage, and enhance last-mile service delivery.

- Researchers: More evidence, especially empirical, is required in almost all uses of Aadhaar to ascertain whether its use is appropriate and beneficial. For promising situations, more data will be needed to determine how to improve on-the-ground functionality. To be impactful, research in this area will require collaboration between practitioners and researchers.
- Practitioners: These chapters discuss available data on Aadhaar's adoption and performance till date. This review provides practitioners in these sectors a foundational overview on what is known about Aadhaar's use and what remains to be learnt. This clarity will hopefully be useful for decision-makers considering whether and how to leverage Aadhaar for their programming. In addition, it guides practitioners on areas where active collaboration with researchers may be beneficial.

The Aadhaar landscape is still poorly understood. Preliminary research has been informative, but the collective body of knowledge on the adoption, implementation, and performance of Aadhaar is limited and fragmented. The multidisciplinary nature of these aspects of Aadhaar demands the effort of experts across a range of disciplines.

Call to Action

In order to support informed policy choices, close collaboration between those conducting research and those informing policies that may benefit from the use of evidence is essential. Quick, multidirectional feedback loops between practitioners and researchers will ensure that the most pressing questions of those on the frontlines of digital identity are answered in thoughtful and rigorous ways. Below, we detail concrete ways for stakeholders to get involved.

Researchers

We invite researchers to become a part of the digital identity ecosystem, lending your voices through a wide variety of activities, especially through our online portal: StateofAadhaar.in.

First, engage with and enhance our online literature database. We have created a database of more than 100 reports and papers relevant to digital identity in India. Use the database as a resource for literature reviews for your respective projects. Please inform us of any papers that you recommend be added to the database.

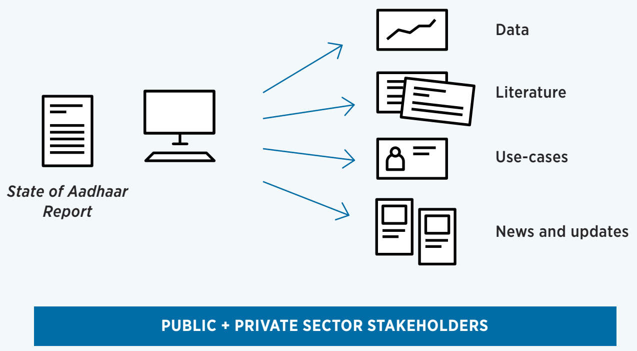
Second, use and update our online data library. This library contains downloadable datasets and provides a list of sources of where to find additional data. You can use filters and the search function to target what datasets you would like to access. We also request you to submit your datasets after appropriate anonymisation for the public good to help enable more research.

Third, discuss issues of digital identity with other stakeholders. We hope to periodically convene researchers and policymakers to discuss important questions and research regarding digital identity. We invite those who may be interested in attending to sign up for updates on our website homepage.

Public and private sector practitioners

We encourage policymakers and officials at all levels of government to gain insights from the data visualisations and summaries available on the website (see "Focus Areas"). This will provide a platform for practitioners to access research that is actionable. They can also establish relationships with researchers to ensure that research projects ask the right questions. Keeping in mind the needs of government officials will encourage researchers to operate on timelines that are practical for real-world decision making, and answer questions relevant to on-the-ground operations. It will also bring high research standards to the discussion on Aadhaar.

Figure 7.1: *State of Aadhaar Report* resources



In addition, the private sector is building an increasingly large presence within Aadhaar's digital identity landscape. Stakeholders working in the private sector have much value to add to conversations about digital identify and its applications.

Our recommended action steps for public and private sector practitioners follow:

First, help shape the research agenda. Let us know what questions you want answered. Go to StateofAadhaar.in and send an email with issues you have encountered and pressing questions regarding digital identity.

Second, discuss issues of digital identity with other stakeholders. We hope to convene policymakers and researchers to enhance dialogue and facilitate working relationships. Private sector participants are encouraged to attend our conferences. Sign up at StateofAadhaar.in if you would like to be notified of those gatherings.

Third, collaborate with researchers and provide access to datasets. Are you willing to collaborate with a research team to address questions of interest to your locality or sector? A great way to collaborate with researchers is to grant them access to relevant anonymised datasets.[2] The government, as well as private sector entities, collects and maintains large amounts of data that may be used to fill some of the critical knowledge gaps we have discussed. Sharing existing information will help speed up research timelines as well as better inform research questions.

Fourth, share this report with colleagues. The *State of Aadhaar Report* is meant to be a foundational document for those interested in the current uses of Aadhaar. We request that you help introduce our work to others who may be interested in learning more.

How Aadhaar is used will affect hundreds of millions of lives in India. We seek to engage a variety of stakeholders from diverse backgrounds and divergent perspectives to generate evidence that can inform decision-making on the appropriate use of digital identity in India and across the globe.

ENDNOTES Chapter 1: Introduction

1. When this report went to print, more than 1.14 billion statistically unique Aadhaar numbers were issued and the world population, according to the United Nations Population Fund, was 7.5 billion people.
2. Compared to other government digital identity systems; not compared to private sector digital identity systems maintained by Facebook, Google, and others.
3. Average number of Aadhaar numbers authenticated from January to March 2017.
   "UIDAI Authentication Portal." Data dashboard. Unique Identification Authority of India. Accessed June 7, 2017.
   https://authportal.uidai.gov.in/.
4. "Advancing the Development Agenda with Aadhaar." Unique Identification Authority of India, 2014.
   https://uidai.gov.in/images/Aadhaar-English.pdf.
5. "Aadhaar Enabled Service Delivery." Unique Identification Authority of India, 2012.
   https://uidai.gov.in/images/resource/whitepaper_aadhaarenabledservice_delivery.pdf.
6. Ibid.
7. Unique Identification Authority of India. "About UIDAI: Vision and Mission." Accessed May 9, 2017.
   https://uidai.gov.in/about-uidai/about-uidai/vision-mission.html.
8. "Press Statement 05.03.2017." Press Release. Unique Identification Authority of India, Government of India, March 5, 2017.
   https://www.uidai.gov.in/images/news/Press_Statement_06032017.pdf.
9. "No of Accounts Opened under PMJDY as on 29.3.2017 (Summary)." Dataset. Archive Reports - Accounts Opened & Rupay Cards Issued. Department of Financial Services, March 29, 2017.
   https://pmjdy.gov.in/ArchiveFile/2017/3/29.03.2017.pdf.
10. This calculation contains two components: Total digital transactions and total Aadhaar enabled transactions. Total digital transactions include: ECS credit and debit, NEFT, RTGS, mobile banking, APBS, IMPS, AEPS, UPI and USSD. Of this, the transactions that can be done through Aadhaar are APBS, AEPS, UPI and USSD. The total number of digital transactions in March 2017 was 1573 million and those through Aadhaar was 105 million. In terms of value, the total digital transactions amounted to ₹13,344 crore and transactions through Aadhaar amounted to ₹800 crore. This proportion is an upper-bound estimate as UPI and USSD transactions can be done without Aadhaar. Calculations use data from: RBI and NPCI.
11. Ibid.
12. "DBT Monthly Reports Sent to Prime Minister's Office." Dataset. DBT Mission, Cabinet Secretariat, Government of India, December 2016.
    https://dbtbharat.gov.in/data/documents/DBT_MPR__Dec_2016.pdf.
13. This calculation is of the largest social protection programmes of the Government of India that include an income augmenting cash transfer to the poor or a subsidy for the basic needs of food and housing: PDS, urea and nutrient subsidy, MGNREGS, LPG subsidy, ICDS, Pradhan Mantri Awas Yojana, mid-day meals, and NSAP. This is a lower bound estimate. Calculations use 2015-16 actual budget expenditure from the Ministry of Finance.
14. The full title is Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act 2016.

ENDNOTES Chapter 2: Aadhaar Architecture

1. The World Bank. "Identification for Development (ID4D)." Accessed May 7, 2017.
   http://www.worldbank.org/en/programs/id4d.
2. For more information, see the World Bank's "Brief on Digital Identity": "Digital ID connects people to electoral participation, educational opportunities, health and social welfare, banking, and economic development. It gives people a chance to better communicate and be recognised by their government, while also giving governments the opportunity to listen and improve the lives of their citizens."
   The World Bank. "Brief on Digital Identity." Accessed May 8, 2017.
   http://pubdocs.worldbank.org/pubdocs/publicdoc/2015/6/413731434485267151/BriefonDigitalIdentity.pdf.

3. “Spotlight on Digital Identity.” Working Paper. Internet for Development. The World Bank, May 2015.
http://pubdocs.worldbank.org/en/959381434483205387/WDR16-Spotlight-on-Digital-ID-May-2015-Mariana-Dahan.pdf.
4. “Digital Dividends.” World Development Report. World Bank Group, 2016.
http://documents.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf.
5. Julia Clark, Mariana Dahan, Vyjayanti Desai, Marta Ienco, Stephanie de Labriolle, Jean-Pierre Pellestor, Kyla Reid, and Yolanda Varuhaki. “Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation.” Discussion Paper. World Bank Group, GSMA and Secure Identity Alliance, July 2016.
http://documents.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUBLIC-WB-GSMA-SIADigitalIdentity-WEB.pdf.
6. “Spotlight on Digital Identity.” Working Paper. Internet for Development. The World Bank, May 2015.
http://pubdocs.worldbank.org/en/959381434483205387/WDR16-Spotlight-on-Digital-ID-May-2015-Mariana-Dahan.pdf.
7. “About UIDAI.” Unique Identification Authority of India. Accessed May 7, 2017.
https://uidai.gov.in/about-uidai/about-uidai.html.
8. The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016 defines a resident as any individual resident in India for 182 days or more in the year before application for Aadhaar enrolment.
9. Data on total Aadhaar numbers issued from “State-Wise Saturation Report,” Unique Identification Authority of India, March 31, 2017.
https://uidai.gov.in/beta/enrolment-update/ecosystem-partners/state-wise-aadhaar-saturation.html.
10. Other forms of digital identity have not reached the same scale as Aadhaar. The total number of Permanent Account Number (PAN) cards (identification issued by India’s Income Tax Department) generated is about 52 million, the number of driver’s licenses is about 170 million, and the number of beneficiaries possessing a ration cards (necessary for receiving a food subsidy under the Public Distribution System) is about 667 million. The Voter ID scheme further covers about 450 million individuals.
PAN: “Time Series Data Financial Year 2000-01 to 2014-15.” Income Tax Department, Government of India. Accessed May 14, 2017.
http://www.incometaxindia.gov.in/Documents/Time-Series-Data-Final.pdf.
Driving license: “State/UT Wise Number of Valid Drivers Licences Issued during the Year 2011-2012.” Accessed May 14, 2017.
https://data.gov.in/catalog/stateut-wise-number-valid-drivers-licences-issued.
PDS: Figure calculated using data from different State Portals.
Voter ID: “The Function (Electoral System).” Election Commission of India. Accessed May 14, 2017.
http://eci.nic.in/eci_main1/the_function.aspx.
11. Ration cards are required for obtaining access to food and fuel subsidies under the Public Distribution System.
12. “Aadhaar Enabled Service Delivery.” Unique Identification Authority of India, 2012.
https://uidai.gov.in/images/authDoc/whitepaper_aadhaarenabledservice_delivery.pdf.
13. Non-Aadhaar biometric identities have been used in health and employment programmes such as the Rashtriya Swasthya Bima Yojana (RSBY), the Mahatma Gandhi National Rural Employment Guarantee Scheme (MGNREGS), and for issuing passports in India, among other uses. However, the scale of these is smaller than Aadhaar and the biometric information is not used for eliminating duplicates.
14. An identity system cannot guarantee complete uniqueness; instead, it can only lower the probability of duplication to a certain threshold. In the case of Aadhaar, as discussed later in the Chapter, the probability of duplicates is low. For the rest of this Chapter and report, when referring to Aadhaar’s uniqueness, we will assume such “statistical uniqueness,” but will not use this phrase each time.
15. The UIDAI carried out a de-duplication exercise in August 2015 and identified 3.94 percent duplicates in food subsidy (Public Distribution System), 0.75 percent duplicates in cooking gas (Liquefied Petroleum Gas) subsidy, and 1.08 percent duplicates in an employment guarantee programme (Mahatma Gandhi National Rural Employment Guarantee Scheme).
“Report on Aadhaar Enabled De-Duplication & Verification Exercise.” Unique Identification Authority of India, August 2014.
https://uidai.gov.in/images/resource/bangalore_analysis_report_v_1.1_26052015.pdf.
16. “Aadhaar Enabled Service Delivery.” Unique Identification Authority of India, 2012.
https://uidai.gov.in/images/authDoc/whitepaper_aadhaarenabledservice_delivery.pdf.
17. Ibid.
18. Census of India. “Census Newsletter,” 2003.
http://censusindia.gov.in/Census_Data_2001/Census_Newsletters/Newsletter_Links/eci17.pdf.
19. Ibid.
20. “Multipurpose National Identity Cards (MNICs).” Office of the Principal Scientific Adviser of the Government of India, 2006.
http://psa.gov.in/initiatives/multipurpose-national-identity-cards-mnics.

21. “Background.” Unique Identification Authority of India. Accessed May 7, 2017.
https://uidai.gov.in/about-uidai/about-uidai/background.html.

22. Ibid.

23. Later, in September 2015, the government revised the Allocation of Business Rules to attach the UIDAI to the Department of Electronics and Information Technology (DeitY).
“About UIDAI.” Unique Identification Authority of India. Accessed May 18, 2017.
https://uidai.gov.in/about-uidai.html.

24. The United Nations estimates India’s population in 2017 at 1,342,513,000 people.
Department of Economic and Social Affairs, United Nations. Data dashboard. *World Population Prospects, the 2015 Revision.* Accessed May 23, 2017.
https://esa.un.org/unpd/wpp/DataQuery/.
Data on total number of Aadhaar numbers issued: “State-Wise Saturation Report,” Unique Identification Authority of India, March 31, 2017.
https://uidai.gov.in/beta/enrolment-update/ecosystem-partners/state-wise-aadhaar-saturation.html.

25. “About UIDAI.” Unique Identification Authority of India. Accessed May 18, 2017.
https://uidai.gov.in/about-uidai.html.

26. “Enrolment Partners.” Unique Identification Authority of India. Accessed May 7, 2017.
https://uidai.gov.in/enrolment-update/ecosystem-partners.html.

27. “Training Module on Aadhaar Enrolment Process.” Unique Identification Authority of India. Accessed May 7, 2017.
https://uidai.gov.in/images/training/downloads/Module2-Aadhaar_Enrolment_Process-Ver1.0.pdf.

28. Ibid.

29. “UIDAI Public Data Portal.” Data dashboard. Unique Identification Authority of India. Accessed May 7, 2017.
https://portal.uidai.gov.in/uidwebportal/dashboard.do.

30. “List of Valid Documents.” Unique Identification Authority of India. Accessed May 7, 2017.
https://uidai.gov.in/images/commdoc/valid_documents_list.pdf.

31. Individuals who cannot provide a proof-of-date-of-birth can register their date of birth through other means detailed in Appendix 2.1.

32. The Right to Information Act provides the framework for citizens to request information pertaining to or kept by public authorities in an attempt to create greater accountability and transparency. Parliament of India. The Right to Information Act, 2005 (2005).
http://rti.gov.in/webactrti.htm.

33. Unique Identification Authority of India. “Response to RTI by Ujjainee Sharma.” Accessed May 7, 2017.
https://i0.wp.com/thewire.in/wp-content/uploads/2015/06/Enrolment-through-introducer.jpg.

34. As of April 2015, the total Aadhaar numbers generated based on the introducer system were 219,296. Based on available UIDAI estimates, the number of Aadhaar holders in 2015 were about 930 million.
Aadhaar numbers generated based on the introducer system: Ibid.
Number of Aadhaar holders in 2015: “Till Date About 93 Per Cent of the Adult Residents in India Acquired Unique Identity – Aadhaar On Their Own Volition.” Press Release. Ministry of Communications & Information Technology, October 30, 2015.
http://pib.nic.in/newsite/mbErel.aspx?relid=130073.

35. “Resident Enrolment Process Version 2.2.1.” Unique Identification Authority of India, December 12, 2014.
https://uidai.gov.in/images/mou/resident_enrolment_process_ver_2.2.1.pdf.

36. “Role of Biometric Technology in Aadhaar Enrolment.” Unique Identification Authority of India, 2012.
https://uidai.gov.in/images/FrontPageUpdates/role_of_biometric_technology_in_aadhaar_jan21_2012.pdf.

37. Ibid.

38. “FAQs.” Unique Identification Authority of India. Accessed May 16, 2017.
https://uidai.gov.in/your-aadhaar/help/faqs.html.

39. “Frequently Asked Questions: Aadhaar Letter.” Unique Identification Authority of India. Accessed May 7, 2017.
https://uidai.gov.in/your-aadhaar/help/faqs.html.

40. Visual adapted from “Enrolment Process Essentials UIDAI.” NICT- CSC. Accessed May 7, 2017.
http://www.nictcsc.com/images/Aadhaar%20Project%20Training%20Module/English%20Training%20Module/module2_aadhaar_enrolment_process17122012.pdf.

41. UIDAI established two committees in 2009, the Biometric Standards Committee and the Demographic Data Standards and Verification Committee.
“Biometrics Design Standards for UID Applications Version 1.0.” Unique Identification Authority of India Committee on Biometrics, December 2009.
https://uidai.gov.in/images/resource/Biometrics_Standards_Committee_report.pdf.

“Demographic Data Standards and Verification Procedure (DDSVP) Committee Report.” Accessed May 7, 2017. https://uidai.gov.in/images/UID_DDSVP_Committee_Report_v1.0.pdf.

42. “Role of Biometric Technology in Aadhaar Enrolment.” Unique Identification Authority of India, 2012. https://uidai.gov.in/images/FrontPageUpdates/role_of_biometric_technology_in_aadhaar_jan21_2012.pdf.

43. Ibid.

44. “UIDAI Strategy Overview: Creating a Unique Identity Number for Every Resident in India.” Unique Identification Authority of India, April 2010. https://uidai.gov.in/UID_PDF/Front_Page_Articles/Documents/Strategy_Overveiw-001.pdf.

45. “Role of Biometric Technology in Aadhaar Enrolment.” Unique Identification Authority of India, 2012. https://uidai.gov.in/images/FrontPageUpdates/role_of_biometric_technology_in_aadhaar_jan21_2012.pdf.

46. “Training Module on Aadhaar Enrolment Process.” Unique Identification Authority of India. Accessed May 7, 2017. https://uidai.gov.in/images/training/downloads/Module2-Aadhaar_Enrolment_Process-Ver1.0.pdf.

47. Exceptions to this rule are discussed in Appendix 2.1.

48. Aadhaar numbers by gender: “Public Data Portal: Aadhaars by Gender and Age.” Data dashboard. Unique Identification Authority of India. Accessed May 17, 2017. https://portal.uidai.gov.in/uidwebportal/dashboard.do.
Gender composition of India’s population: “Gender Composition.” Office of the Registrar General & Census Commissioner, India. Accessed May 7, 2017. http://censusindia.gov.in/Census_And_You/gender_composition.aspx.

49. UIDAI’s population estimates are based on projected 2015 figures.
“State-Wise Saturation Report,” Unique Identification Authority of India, March 31, 2017. https://uidai.gov.in/beta/enrolment-update/ecosystem-partners/state-wise-aadhaar-saturation.html.

50. Ibid.

51. “Aadhaar Enrolment.” Unique Identification Authority of India. Accessed May 7, 2017. https://uidai.gov.in/enrolment-update/aadhaar-enrolment.html.

52. “UIDAI Strategy Overview: Creating a Unique Identity Number for Every Resident in India.” Unique Identification Authority of India, April 2010. https://uidai.gov.in/UID_PDF/Front_Page_Articles/Documents/Strategy_Overveiw-001.pdf.

53. “List of Valid Documents.” Unique Identification Authority of India. Accessed May 17, 2017. https://uidai.gov.in/images/commdoc/valid_documents_list.pdf.

54. “Role of Biometric Technology in Aadhaar Enrolment.” Unique Identification Authority of India, 2012. https://uidai.gov.in/images/FrontPageUpdates/role_of_biometric_technology_in_aadhaar_jan21_2012.pdf.

55. Ibid.

56. Ibid.

57. Per-day average calculated using daily enrolment data released by the UIDAI. Aadhaar Data Portal, Unique Identification Authority of India. “Aadhaar Generated by State, District.” Accessed May 16, 2017. https://data.uidai.gov.in/uiddatacatalog/getDatsetInfo.do?dataset=UIDAI-ENR-GEOGRAPHY.

58. “Facts about Aadhaar.” Unique Identification Authority of India. Accessed May 7, 2017. https://uidai.gov.in/images/aadhaar_question_and_answers.pdf.

59. “Role of Biometric Technology in Aadhaar Enrolment.” Unique Identification Authority of India, 2012. https://uidai.gov.in/images/FrontPageUpdates/role_of_biometric_technology_in_aadhaar_jan21_2012.pdf.

60. Standing Committee on Finance (2011-12). “Forty Second Report: The National Identification Authority of India Bill, 2010.” Ministry of Planning, December 2011. http://164.100.47.134/lsscommittee/Finance/42%20Report.pdf.

61. “Facts about Aadhaar.” Unique Identification Authority of India. Accessed May 7, 2017. https://uidai.gov.in/images/aadhaar_question_and_answers.pdf.

62. “Authentication Overview.” Unique Identification Authority of India. Accessed May 7, 2017. https://uidai.gov.in/authentication/authentication-overview.html.

63. Ibid.

64. Ibid.

65. “Aadhaar OTP Request API.” Unique Identification Authority of India, 2012. https://uidai.gov.in/images/FrontPageUpdates/aadhaar_otp_request_api_1_5.pdf.

66. “Operating Model.” Unique Identification Authority of India. Accessed May 7, 2017. https://uidai.gov.in/authentication/authentication/operation-model.html.

67. “Aadhaar Authentication Implementation Model.” Unique Identification Authority of India, 2012. https://uidai.gov.in/images/authentication/d3_1_operating_model_v1.pdf.

68. “List of Live AUAs, KUAs and ASAs.” Unique Identification Authority of India. Accessed May 7, 2017.
https://uidai.gov.in/images/list_of_live_asa_aua_ksa_kua.pdf.

69. Visual adapted from “Aadhaar Authentication Overview.” Presentation. Unique Identification Authority of India, 2012.
https://uidai.gov.in/images/aadhaar_authentication_overview.pdf,

70. “Aadhaar Authentication Document for Delivery of Services.” Unique Identification Authority of India, 2016.
https://uidai.gov.in/images/resource/aadhaar_authentication_document_for_delivery_of_services_v1_0.pdf.

71. These were Delhi, Karnataka, Jharkhand, Himachal Pradesh, and Maharashtra.
“Role of Biometric Technology in Aadhaar Authentication”. Unique Identification Authority of India, 2012.
https://uidai.gov.in/images/role_of_biometric_technology_in_aadhaar_authentication_020412.pdf.

72. Ibid.

73. A detailed discussion of this data is presented in Chapter 5, *Social Protection.*

74. “Aadhaar Authentication User Agency (AUA) Handbook - Version 1.0.” Unique Identification Authority of India, January 2014.
https://www.uidai.gov.in/images/aua_handbook_v1.0_final_30012014.pdf.

75. Unique Identification Authority of India. Unique Identification Authority of India (Transaction of Business at Meetings of the Authority) Regulations, 2016. Accessed May 7, 2017.
https://uidai.gov.in/images/regulation_1_to_5_15092016.pdf.

76. “Facts about Aadhaar.” Unique Identification Authority of India. Accessed May 7, 2017.
https://uidai.gov.in/images/aadhaar_question_and_answers.pdf.

77. “Aadhaar Enabled Payment System: Overview.” National Payments Corporation of India. Accessed May 7, 2017.
http://www.npci.org.in/AEPSOverview.aspx.

78. “Aadhaar Enabled Payments.” Authentication Portal, Unique Identification Authority of India. Accessed May 7, 2017.
https://authportal.uidai.gov.in/web/uidai/home-articles?urlTitle=aadhaar-enabled-payments&pageType=authentication.

79. This service can be, and is, provided without the use of Aadhaar as well.

80. “UIDAI Strategy Overview.” Unique Identification Authority of India. Accessed May 7, 2017.
https://uidai.gov.in/images/uidai_strategy_overview_04022016.pdf.

81. Ibid.

82. Ibid.

83. “Frequently Asked Questions - Children.” Unique Identification Authority of India. Accessed May 17, 2017.
https://uidai.gov.in/component/fsf/?view=faq&catid=18.

84. Ibid.

85. “UIDAI Strategy Overview.” Unique Identification Authority of India. Accessed May 7, 2017.
https://uidai.gov.in/images/uidai_strategy_overview_04022016.pdf.

86. “Enrolment Process Essentials UIDAI.” NICT- CSC. Accessed May 7, 2017.
http://www.nictcsc.com/images/Aadhaar%20Project%20Training%20Module/English%20Training%20Module/module2_aadhaar_enrolment_process17122012.pdf.

87. “Authentication Overview.” Unique Identification Authority of India. Accessed May 7, 2017.
https://uidai.gov.in/authentication/authentication-overview.html.

88. “Aadhaar Authentication Document for Delivery of Services.” Unique Identification Authority of India, 2016.
https://uidai.gov.in/images/resource/aadhaar_authentication_document_for_delivery_of_services_v1_0.pdf.

ENDNOTES Chapter 3: Legal and Governance Framework

1. The full title of this Act is Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act 2016.
Ministry of Law and Justice (Legislative Department). The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, Pub. L. No. 18 of 2016 (2016).
https://uidai.gov.in/images/the_aadhaar_act_2016.pdf.

2. These are discussed in Chapters 4 (*Financial Inclusion*), 5 (*Social Protection*) and 6 (*Emerging Uses*) respectively.

3. Planning Commission, Government of India. “Notification No. A.03011/02/2009,” January 28, 2009.
https://uidai.gov.in/images/notification_28_jan_2009.pdf.

4. The evolution (and eventual collation) of disparate identity projects that formed the basis for Aadhaar is discussed in Chapter 2, *Aadhaar Architecture.*

5. Since January 1, 2015, the NITI Aayog has replaced the Planning Commission. Niti Aayog. “Overview.” Accessed May 14, 2017.

http://niti.gov.in/content/overview.

6. "About UIDAI." Unique Identification Authority of India. Accessed May 18, 2017.
https://uidai.gov.in/about-uidai/about-uidai.html.

7. Standing Committee on Finance (2011-12). "Forty Second Report: The National Identification Authority of India Bill, 2010." Ministry of Planning, December 2011.
http://164.100.47.134/lsscommittee/Finance/42 Report.pdf.

8. Ibid.

9. Employment News Weekly, Ministry of Information and Broadcasting. "National Identification Authority of India Bill, 2013." Accessed May 16, 2017.
http://employmentnews.gov.in/NewEmp/AboutUs.aspx.

10. All tax and non-tax revenue received by the Government of India in connection with the conduct of government business is credited to the Consolidated Fund of India. No money can be withdrawn from the fund without Parliament's authorisation.
    Office of Chief Controller of Accounts, Ministry of Commerce and Industry. "Government Accounts." Accessed May 14, 2017.
    http://ccaind.nic.in/govt_accounts.asp.

11. Individuals to whom an Aadhaar number has not been assigned, must make an application for enrolment. These individuals shall be offered alternate and viable means of identification for the delivery of benefits.

12. The Speaker of the Lok Sabha certified this.

13. Ministry of Finance, Department of Revenue, Government of India. "Mandatory Quoting of Aadhaar For PAN Applications & Filing Return of Income." Press Release, April 5, 2017.
http://www.incometaxindia.gov.in/Lists/Press%20Releases/Attachments/611/Press-Release-Aadhaar-5-04-2017.pdf.

14. 2013: Justice K.S. Puttaswamy (Retd) & ANR v. Union of India & ORS, No. Writ Petition (Civil) No (s). 494 (Supreme Court of India 2013).
http://judis.nic.in/temp/494201232392013p.txt.

15. 2014: Unique Identification Authority of India & ANR v. Central Bureau of Investigation, No. Petition for Special Leave to Appeal No. 2524 (Supreme Court of India 2014).
http://courtnic.nic.in/supremecourt/temp/2524201422432014p.txt.

16. 2015: Justice K.S. Puttaswamy (Retd) & ANR v. Union of India & ORS, Supreme Court of India, Writ Petition (Civil) No (s). 494 (2012) and all Transferred Case, Writ and Contempt petitions.
http://judis.nic.in/supremecourt/imgs1.aspx?filename=42841.

17. These refer to The Public Distribution System (PDS) and the Liquefied Petroleum Gas (LPG) subsidy. Ibid.

18. In order of reference: Mahatma Gandhi National Rural Employment Guarantee Scheme (MGNREGS), National Social Assistance Program (NSAP), Pradhan Mantri Jan Dhan Yojana (PMJDY), and Employees' Provident Fund Organisation (EPFO).
    Justice K.S. Puttaswamy (Retd) & ANR v. Union of India & ORS, Supreme Court of India, Writ Petition (Civil) No (s). 494 (2012).
    http://supremecourtofindia.nic.in/FileServer/2015-10-16_1444976434.pdf.

19. Ibid.

20. "Post Matric Scholarship Aadhaar Seeding." Notification. ST & SC Development and Minority Community and Other Backward Class Welfare Department, Government of Odisha. Accessed May 9, 2017.
http://www.stscodisha.gov.in/pdf/Post-matric_Scholarship_Aadhar_Seeding.pdf.

21. Department of Minorities Welfare. "Letter No. A4/731/2015," August 4, 2016.
https://www.nitt.edu/home/iiits/Pre-Matric-Scholarship.pdf.

22. Ministry of Labour and Employment. "Notification." Gazette of India, January 4, 2017.
http://egazette.nic.in/WriteReadData/2017/173488.pdf.

23. "Notification." Gazette of India. Ministry of Rural Development, Government of India, January 3, 2017.
http://nrega.nic.in/netnrega/writereaddata/Circulars/2001173479.pdf.

24. Ministry of Finance, Department of Revenue, Government of India. "Mandatory Quoting of Aadhaar For PAN Applications & Filing Return of Income." Press Release, April 5, 2017.
http://www.incometaxindia.gov.in/Lists/Press%20Releases/Attachments/611/Press-Release-Aadhaar-5-04-2017.pdf.

25. "UIDAI Strategy Overview: Creating a Unique Identity Number for Every Resident in India." Unique Identification Authority of India. Accessed May 17, 2017. https://uidai.gov.in/images/uidai_strategy_overview_04022016.pdf.
https://uidai.gov.in/images/uidai_strategy_overview_04022016.pdf.

26. Delegated legislation refers to the rules created by empowered bodies to implement objectives laid out in primary or parent legislation (in this case the Aadhaar Act 2016).

27. Uncorrected Transcript of Rajya Sabha Debate (2016). Rajya Sabha, Government of India.
http://164.100.47.5/newdebate/238/16032016/Fullday.pdf.

28. "Press Statement 05.03.2017." Unique Identification Authority of India, March 5, 2017.

https://uidai.gov.in/images/news/Press_Statement_06032017.pdf.

29. Ministry of Electronics and Information Technology, Government of India. “Personal Data of Individuals Held by UIDAI Is Fully Safe and Secure.” Press Release. Press Information Bureau, March 5, 2017.
http://pib.nic.in/newsite/PrintRelease.aspx?relid=158849.
30. Unique Identification Authority of India. Twitter Post, April 25, 2017.
https://twitter.com/UIDAI/status/856783508034928640.
31. Ibid.
32. Ibid.
33. An example of such a law is the Telegraph Act, 1885, dealing with conditions under which wiretapping may be permissible. “Indian Telegraph Act 1885.” Department of Telecommunications, Government of India. Accessed May 17, 2017.
http://www.dot.gov.in/actrules/indian-telegraph-act-1885.
34. “Illegal Use of Aadhaar: Unstarred Question No. 5065.” Lok Sabha Question. Ministry of State for Electronics and Information Technology, April 5, 2017.
https://uidai.gov.in/images/loksabha/LS_USQ_5065_answered_on_05042017.pdf.
35. “Registration of FIR by UIDAI: Unstarred Question No. 4469.” Lok Sabha Question. Ministry of State for Electronics and Information Technology, March 29, 2017.
https://uidai.gov.in/images/loksabha/LS_USQ_4469_answered_on_29032017.pdf.
36. Justice K.S. Puttaswamy (Retd) & ANR v. Union of India & ORS, No. Writ Petition (Civil) No (s). 494 (2012) and all Transferred Case, Writ and Contempt petitions (Supreme Court of India 2015).
http://judis.nic.in/supremecourt/imgs1.aspx?filename=42841.
37. Unique Identification Authority of India. Unique Identification Authority of India (Transaction of Business at Meetings of the Authority) Regulations, 2016 (No. 1 of 2016) Page 1-10 (2016).
https://uidai.gov.in/images/regulation_1_to_5_15092016.pdf.
38. Unique Identification Authority of India. Aadhaar (Enrolment and Update) Regulations, 2016 (No. 2 of 2016) – Page 10-41 (2016).
https://uidai.gov.in/images/regulation_1_to_5_15092016.pdf.
39. Unique Identification Authority of India. Aadhaar (Enrolment and Update) (First Amendment) Regulations, 2017 (2017).
https://uidai.gov.in/images/reg_amendment_16022017.pdf.
40. Unique Identification Authority of India. Aadhaar (Authentication) Regulations, 2016 (No. 3 of 2016) - Page 41-67 (2016).
https://uidai.gov.in/images/regulation_1_to_5_15092016.pdf.
41. Unique Identification Authority of India, Ministry of Electronics and Information Technology. “Circular: Amendment in Schedule A of Aadhaar (Authentication) Regulations, 2016,” April 3, 2017.
https://uidai.gov.in/images/resource/amendment_in_Schedule_A_05042017.pdf.
42. Unique Identification Authority of India. Aadhaar (Data Security) Regulations, 2016 (No. 4 of 2016) - Page 67-72 (2016)
https://uidai.gov.in/images/regulation_1_to_5_15092016.pdf.
43. Unique Identification Authority of India. Aadhaar (Sharing of Information) Regulations, 2016 (No. 5 of 2016) – Page 72-77 (2016).
https://uidai.gov.in/images/regulation_1_to_5_15092016.pdf.

ENDNOTES Chapter 4: Financial Inclusion

1. Cull, Robert, Tilman Ehrbeck, and Nina Holle. “Financial Inclusion and Development: Recent Impact Evidence.” Focus Note. Consultative Group to Assist the Poor (CGAP), April 2014.
http://www.cgap.org/sites/default/files/FocusNote-Financial-Inclusion-and-Development-April-2014.pdf.
2. “Pradhan Mantri Jan-Dhan Yojana: A National Mission on Financial Inclusion.” Department of Financial Services, Government of India, August 22, 2014.
https://pmjdy.gov.in/files/financial-Literacy/Mission-Document/PDF/English.pdf.
3. “No of Accounts Opened under PMJDY as on 22.02.2017 (Summary).” Dataset. Archive Reports - Accounts Opened & Rupay Cards Issued. Department of Financial Services, February 22, 2017.
https://pmjdy.gov.in/ArchiveFile/2017/2/22.02.2017.pdf.
4. One hundred million is a conservative calculation of the remaining unbanked population in India. The current number of unbanked adults in India is not available. We estimate that as of 2014 there were about 420 million unbanked adults in India.

This figure is calculated using data from the 2014 World Bank Global Findex database with estimates from the 2011 World Bank Global Findex database and a 2014 World Bank Findex Note on South Asia. This specific calculation and related notes can be found here: http://bit.ly/2r41lJg. Sources listed below. We then calculated the current estimate using this 2014 estimate of unbanked individuals in India (420 million) and then subtracted the number of new accounts opened under PMJDY since 2014 (282 million), resulting in 138 million. This calculation assumes that every new account opened under PMJDY was executed by a previously unbanked person; therefore, it is a highly conservative estimate of the number of unbanked persons. The actual estimate is likely much higher.

Demirguc-Kunt, Asli, Leora Klapper, Dorothe Singer, and Peter Van Oudheusden. "The Global Findex Database 2014: Measuring Financial Inclusion around the World." Working Paper. World Bank, April 2015.
http://documents.worldbank.org/curated/en/187761468179367706/pdf/WPS7255.pdf.

Demirguc-Kunt, Asli, and Leora Klapper. *Measuring Financial Inclusion: The Global Findex Database.* Policy Research Working Papers. The World Bank, 2012. doi:10.1596/1813-9450-6025.

Demirguc-Kunt, Asli, Leora Klapper, Dorothe Singer, Peter Van Oudheusden, Saniya Ansar, and Jake Hess. "The Global Findex Database 2014: Financial Inclusion in South Asia." Findex Notes. World Bank, November 2015.
http://pubdocs.worldbank.org/en/312921461702869643/N7-SAsia.pdf.

5. "No of Accounts Opened under PMJDY as on 22.02.2017 (Summary)." Dataset. Archive Reports - Accounts Opened & Rupay Cards Issued. Department of Financial Services, February 22, 2017.
https://pmjdy.gov.in/ArchiveFile/2017/2/22.02.2017.pdf.

6. "Discussion Paper on Aadhaar Based Financial Inclusion." Discussion paper. Unique Identification Authority of India, Government of India, October 2010.
https://uidai.gov.in/images/FrontPageUpdates/discussionpaperonaadhaarbasedfinancialinclusion15oct.pdf.

7. Demirguc-Kunt, Asli, Leora Klapper, Dorothe Singer, and Peter Van Oudheusden. "The Global Findex Database 2014: Measuring Financial Inclusion around the World." Working Paper. World Bank, April 2015.
http://documents.worldbank.org/curated/en/187761468179367706/pdf/WPS7255.pdf.

8. This statistic was calculated by analysing survey data released by the World Bank (see previous citation). A respondent could pick more than one reason why she or he does not have a financial account, including the lack of "necessary documentation (identity card, wage slip, etc.)," which is the statistic represented here.
The full World Bank question on the Global Findex survey reads:

Question 8: "Please tell me whether each of the following is A REASON why you, personally, DO NOT have an account at a bank or another type of formal financial institution. (Read and rotate A-I) Is it… ?
A. Because financial institutions are too far away
B. Because financial services are too expensive
C. Because you don't have the necessary documentation (identity card, wage slip, etc.)
D. Because you don't trust financial institutions
E. Because of religious reasons
F. Because you don't have enough money to use financial institutions
G. Because someone else in the family already has an account
H. Because you cannot get an account
I. Because you have no need for financial services at a formal institution"

9. See sections on Aadhaar Payment Bridge System (APBS) used for digitising Direct Benefit Transfer (DBT) payments; Aadhaar Enabled Payment System (AEPS) used with microATMs that reach rural areas; and the UPI system that provides mobile banking services.

10. Government Of India, Unique Identification Authority of India. "Aadhaar Enabled Payments." *Aadhaar Enabled Payments. Accessed May 15, 2017.*
https://authportal.uidai.gov.in/home-articles?urlTitle=aadhaar-enabled-payments&pageType=authentication.

11. The number of Aadhaar-seeded bank accounts is sourced from the "Aadhaar Numbers in NPCI Mapper" on the NPCI homepage.

National Payments Corporation of India. "National Payments Corporation of India." Homepage. National Payments Corporation of India. Accessed April 12, 2017.
http://www.npci.org.in/.

12. The number of times Aadhaar e-KYC is used to open financial accounts is sourced from the "e-KYC Verification (Successful Txn)" from an NPCI document on retail statistics.

"Retail Payments Statistics on NPCI Platforms." Dataset. National Payments Corporation of India, April 2017.
http://www.npci.org.in/documents/RETAIL_PAYMENTS_STATISTICS.pdf.

13. Reddy, Dr. Y. Venugopal. "Statement by Dr. Y. Venugopal Reddy, Governor, Reserve Bank of India on the Mid-Term Review of Annual Policy for the Year 2005-06." Notification. Reserve Bank of India, October 25, 2005.
https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=2539&Mode=0.

14. Verma, Rajesh. "Financial Inclusion- Access to Banking Services – Basic Savings Bank Deposit Account." Notification. Reserve Bank of India, August 10, 2012.
https://www.rbi.org.in/commonman/English/Scripts/Notification.aspx?Id=989.

15. Basic Savings Bank Deposit Accounts (BSBDAs) were introduced by the RBI in 2012, replacing "no-frills" bank accounts. BSBDAs removed the requirement for minimum balances. They also allow for ATM usage, electronic payments & receipts, and deposits & collection of cheques. The accounts stipulate no limits on number of deposits, but have a maximum of four withdrawals in a month. ATM/debit cards are considered standard under these guidelines. All these features are provided at zero cost to the account holder. Basic savings bank deposit account holders are not eligible to open another savings account at the same bank.

    Verma, Rajesh. "Financial Inclusion- Access to Banking Services – Basic Savings Bank Deposit Account." Notification. Reserve Bank of India, August 10, 2012.
    https://www.rbi.org.in/commonman/English/Scripts/Notification.aspx?Id=989.

16. See endnote 4 for a full explanation of this calculation.

17. Government Of India, Department of Financial Services, Ministry of Finance. "Pradhan Mantri Jan Dhan Yojana (PMJDY)." Pradhan Mantri Jan-Dhan Yojana | Department of Financial Services | Ministry of Finance, n.d.
https://www.pmjdy.gov.in/about.

18. Data is not yet available for the number of BSBDAs opened in fiscal year 2016-2017. However, growth among non-PMJDY BSBDA accounts has been slow since the introduction of PMJDY in 2014. Here we have used the number from 2015-2016.

19. "No of Accounts Opened under PMJDY as on 22.02.2017 (Summary)." Dataset. Archive Reports - Accounts Opened & Rupay Cards Issued. Department of Financial Services, February 22, 2017. https://pmjdy.gov.in/ArchiveFile/2017/2/22.02.2017.pdf.

20. "Spreading JAM across India's Economy." Annual Survey Report. Economic Survey. Ministry of Finance, Government of India, 2016.
http://indiabudget.nic.in/es2015-16/echapvol1-03.pdf.

21. World Bank Group. Global *Financial Development Report 2014: Financial Inclusion.* Vol. 2. World Bank Publications, 2013.

22. Demirguc-Kunt, Asli, Leora Klapper, Dorothe Singer, and Peter Van Oudheusden. "The Global Findex Database 2014: Measuring Financial Inclusion around the World." Working Paper. World Bank, April 2015.
http://documents.worldbank.org/curated/en/187761468179367706/pdf/WPS7255.pdf.

23. World Bank Group. *Global Financial Development Report 2014: Financial Inclusion.* Vol. 2. World Bank Publications, 2013.

24. According to the Ministry of Finance, 73 percent of villages are more than five kilometers from the nearest bank branch. Note: This statistic was calculated by taking the inverse of the statement in *Spreading JAM across India's Economy* that stated in rural India "only 27 percent of villages have a bank within 5km."

    "Spreading JAM across India's Economy." Annual Survey Report. Economic Survey. Ministry of Finance, Government of India, 2016.
    http://indiabudget.nic.in/es2015-16/echapvol1-03.pdf.

25. Demirguc-Kunt, Asli, Leora Klapper, Dorothe Singer, and Peter Van Oudheusden. "The Global Findex Database 2014: Measuring Financial Inclusion around the World." Working Paper. World Bank, April 2015.
http://documents.worldbank.org/curated/en/187761468179367706/pdf/WPS7255.pdf.

26. As of February 2017, 25 percent of all bank accounts opened under PMJDY had a balance of zero rupees. Further, a 2014 survey found that 43.3 percent of those with bank accounts had not deposited or withdrawn money from them in the previous year.

    "No of Accounts Opened under PMJDY as on 22.02.2017 (Summary)." Dataset. Archive Reports - Accounts Opened & Rupay Cards Issued. Department of Financial Services, February 22, 2017.
    https://pmjdy.gov.in/ArchiveFile/2017/2/22.02.2017.pdf.

27. The Reserve Bank of India (RBI) initially adopted know-your-customer (KYC) norms for banks in 2002 for the purposes of identifying and flagging suspicious transactions. In 2004, with recommendations from the Financial Action Task Force (FATF) on Anti-Money Laundering (AML) standards and on Combating Financing of Terrorism (CFT), RBI strengthened its KYC requirements by providing a specific list of acceptable identity and address documents for account openings by individuals. In July 2013, the letter from the UIDAI containing Aadhaar details was included as an acceptable document for proof of identity and address. In September 2013, RBI incorporated the use of Aadhaar e-KYC as an acceptable KYC measure, predicated upon banks having the necessary equipment and infrastructure in place to conduct the consent-based authentication per the UIDAI guidelines.

    Muralidharan, C. R. Circular from the Reserve Bank of India (RBI). "Guidelines on 'Know Your Customer' Norms and 'Cash Transactions.'" Circular from the Reserve Bank of India (RBI), August 16, 2002.
    https://rbi.org.in/scripts/NotificationUser.aspx?Id=819&Mode=0.
    Saran, Prashant. Circular from the Reserve Bank of India (RBI). "Know Your Customer (KYC) Guidelines – Anti-Money Laundering Standards." Circular from the Reserve Bank of India (RBI), November 29, 2004.
    https://www.rbi.org.in/commonman/English/Scripts/Notification.aspx?Id=79.

Sahoo, Prakash Chandra. Circular from the Reserve Bank of India (RBI). "Master Circular – Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) Standards/Combating of Financing of Terrorism (CFT)/Obligation of Banks under PMLA, 2002." Circular from the Reserve Bank of India (RBI), July 1, 2013.
https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=8179&Mode=0#f10.
Sahoo, Prakash Chandra. Circular from the Reserve Bank of India (RBI). "KYC Norms/AML Standards/Combating Financing of Terrorism (CFT)/Obligation of Banks under PMLA, 2002 - E-KYC Service of UIDAI – Recognising on-Line Aadhaar Authentication to Be Accepted as an 'Officially Valid Document' under PML Rules." Circular from the Reserve Bank of India (RBI), September 2, 2013.
https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=8357&Mode=0.

28. According to the UIDAI, financial services entities have authorised the use of Aadhaar e-KYC as a legal KYC document, which includes: Reserve Bank of India, Insurance Regulatory and Development Authority, Pension Fund Regulatory and Development Authority, and Securities and Exchange Board of India.
"Frequently Asked Questions (FAQs) – UIDAI's Electronically Know Your Customer (E-KYC) Service." Frequently Asked Question (FAQ) document. Unique Identification Authority of India, Government of India. Accessed April 5, 2017.
https://uidai.gov.in/images/commdoc/FAQs-EKYC.pdf.

29. "Frequently Asked Questions (FAQs) – UIDAI's Electronically Know Your Customer (E-KYC) Service." Frequently Asked Question (FAQ) document. Unique Identification Authority of India, Government of India. Accessed April 5, 2017.
https://uidai.gov.in/images/commdoc/FAQs-EKYC.pdf.

30. Desai, Manish. "Aadhar E-KYC : Fast, Secure & Cost Effective." Press Release. Press Information Bureau, August 23, 2013.
http://www.pib.nic.in/newsite/mbErel.aspx?relid=98437.

31. Public sector banks are defined here as "Nationalised Banks," "SBI and its Associates," and "Other Public Sector Banks."

32. National Payments Corporation of India. "Banks/Entities Live in eKYC Production." National Payments Corporation of India. Accessed March 29, 2017.
http://www.npci.org.in/ekyc.aspx.

33. "Press Statement 05.03.2017." Press Release. Unique Identification Authority of India, Government of India, March 5, 2017.
https://www.uidai.gov.in/images/news/Press_Statement_06032017.pdf.

34. An individual would also need to give the name of the bank where she or he held an account.
National Payments Corporation of India. "Aadhaar Enabled Payment System Overview." National Payments Corporation of India. Accessed March 15, 2017.
http://www.npci.org.in/AEPSOverview.aspx.

35. The Business Correspondent model was initiated by the RBI in 2006 to extend banking services to areas where bank branches may not be present. Business correspondents (BCs) were initially limited to employees of NGOs, microfinance institutions, and post-offices; however, in late 2010, the RBI allowed banks to enter an agreement with any individual to become a BC. The RBI has stated that a "fundamental principle" of the model is that a BC should be a resident of the area she or he is serving. Per RBI guidelines, a BC is allowed to provide the following services: awareness promotion of banking products and financial literacy; processing of loan applications; provision of micro-credits; collection of interests and deposits; sale of financial products, including micro-insurance, mutual funds, pension products; accepting and disbursal of remittances and other payments; and the distribution of cash.
Bhaskar, P. Vijaya. Circular from the Reserve Bank of India (RBI). "Financial Inclusion by Extension of Banking Services - Use of Business Facilitators and Correspondents." Circular from the Reserve Bank of India (RBI), January 25, 2006.
https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=8357&Mode=0.
Bhaskar, P. Vijaya. Circular from the Reserve Bank of India (RBI). "Financial Inclusion by Extension of Banking Services – Use of Business Correspondents (BCs)." Circular from the Reserve Bank of India (RBI), November 29, 2009.
https://rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=5390.
Bhaskar, P. Vijaya. Circular from the Reserve Bank of India (RBI). "Financial Inclusion by Extension of Banking Services – Use of Business Correspondents (BCs)." Circular from the Reserve Bank of India (RBI), April 26, 2010.
https://rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=5630.
Sahoo, Prakash Chandra. Circular from the Reserve Bank of India (RBI). "Financial Inclusion by Extension of Banking Services - Use of Business Correspondents for Distribution of Banknotes and Coins - Alternative Avenues." Circular from the Reserve Bank of India (RBI), September 2, 2013.
https://rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=8361.

36. While we do not have comprehensive data on microATMs, we do have some coverage data from government sources. The DBT Mission coordinated a village-wise mapping exercise, along with NIC and other departments. They found, "...only 174,691 out of 640,947 lakh villages (27%) have been covered by either Bank Branch, Bank Mitra, ATM, Post Office or Common Service Centre (CSC)"—meaning many villages (and therefore people) remain uncovered.
"The Direct Benefit Transfer." Government report. DBT Mission, Government of India, March 18, 2016.
https://dbtbharat.gov.in/data/documents/REPORT-ON-DBT.pdf.

37. In so much as a BC is unlikely to possess two microATM devices.

38. This number may be less meaningful given India's high population density (Kenya's population is more sparsely distributed and therefore may need more BCs—and thus a smaller ratio—to achieve adequate coverage). A better metric may be the number of BCs within a given unit of geography or the spatial density. Unfortunately, the spatial density of BCs within India is still only 17 percent of the Kenyan ratio.

"Spreading JAM across India's Economy." Annual Survey Report. Economic Survey. Ministry of Finance, Government of India, 2016.
http://indiabudget.nic.in/es2015-16/echapvol1-03.pdf.

39. "Unstarred Question No. 6308 Aadhaar Enabled Payment." Lok Sabha Questions, April 12, 2017.
http://164.100.47.190/loksabhaquestions/annex/11/AU6308.pdf.

40. "The Direct Benefit Transfer." Government report. DBT Mission, Government of India, March 18, 2016.
https://dbtbharat.gov.in/data/documents/REPORT-ON-DBT.pdf.

41. APBS payments are tied to one's Aadhaar number and her or his bank identification number. The usual form of electronic transfer, National Electronic Funds Transfer, or NEFT, requires three data points: name, bank account number, and an 11-digit alphanumeric code (IFSC) of the bank branch. Some bank account numbers do not have a standardised number of digits. By contrast, Aadhaar always has 12 digits, and the last digit can be used to verify the remaining 11 (see Chapter 2).

"Frequently Asked Questions (FAQs) By Customers Aadhaar Payment Bridge (APB) System." Frequently Asked Question (FAQ) document. National Payments Corporation of India. Accessed December 15, 2016.
http://www.npci.org.
in/documents/FAQs_on_APBS_for_Customers1.pdf.
Government Of India, Reserve Bank of India. "FREQUENTLY ASKED QUESTIONS NEFT System." *Reserve Bank of India – Frequently Asked Questions,* July 24, 2015.
https://rbi.org.in/Scripts/FAQView.aspx?Id=60.

42. National Payments Corporation of India. "National Payments Corporation of India." Homepage. National Payments Corporation of India. Accessed April 12, 2017.
http://www.npci.org.in/.

43. Demirguc-Kunt, Asli, Leora Klapper, Dorothe Singer, Peter Van Oudheusden, Saniya Ansar, and Jake Hess. "The Global Findex Database 2014: Financial Inclusion in South Asia." Findex Notes. World Bank, November 2015.
http://pubdocs.worldbank.org/en/312921461702869643/N7-SAsia.pdf.

44. Government Of India, Unique Identification Authority of India. "Aadhaar Enabled Payments." A*adhaar Enabled Payments.* Accessed May 15, 2017.
https://authportal.uidai.gov.in/home-articles?urlTitle=aadhaar-enabled-payments&pageType=authentication.

45. Four types of transactions are possible with AEPS: balance check, cash deposit, cash withdrawal, and Aadhaar-to-Aadhaar Fund Transfer.

National Payments Corporation of India. "Aadhaar Enabled Payment System Overview." National Payments Corporation of India. Accessed March 15, 2017.
http://www.npci.org.in/AEPSOverview.aspx.

46. National Payments Corporation of India. "UPI FAQs." Unified Payments Interface (UPI) Frequently Asked Questions. National Payments Corporation of India. Accessed May 5, 2017.
http://www.npci.org.in/UPI_FAQs.aspx.

47. Government Of India, Cashless India. "Bharat Interface for Money (BHIM)." *Cashless India.* Accessed May 25, 2017.
http://cashlessindia.gov.in/bhim.html.

48. "MINISTRY OF FINANCE (Department of Economic Affairs) NOTIFICATION." Gazette of India. Ministry of Finance, Government of India, November 8, 2016.
http://egazette.nic.in/WriteReadData/2016/172713.pdf.

49. "Retail Payments Statistics on NPCI Platforms." Dataset. National Payments Corporation of India, April 2017.
http://www.npci.org.in/documents/RETAIL_PAYMENTS_STATISTICS.pdf.

50. "BHIM Application Launched on 30th December 2016: Salient Features Include Instant Money Transfer at All Times among Others." Press Release. Press Information Bureau, February 3, 2017.
http://www.pib.nic.in/newsite/mbErel.aspx?relid=158028.

51. "BHIM Product Overview." National Payments Corporation of India. Accessed May 15, 2017.
http://www.npci.org.in/BHIM_Product_Overview.aspx.

52. "BHIM Analytics." Data dashboard. National Payments Corporation of India, May 7, 2017.
http://www.npci.org.in/BHIM-Analytics.aspx.

53. Government Of India, Cashless India. "Bharat Interface for Money (BHIM)." *Cashless India.* Accessed May 25, 2017.
http://cashlessindia.gov.in/bhim.html.

54. "BHIM Product Overview." National Payments Corporation of India. Accessed May 15, 2017.
http://www.npci.org.in/BHIM_Product_Overview.aspx.

ENDNOTES Chapter 5: Social Protection

1. "Taking On Inequality, Poverty And Shared Prosperity." The World Bank, 2016. https://openknowledge.worldbank.org/bitstream/handle/10986/25078/9781464809583.pdf.
2. This calculation is of the largest social protection programmes of the Government of India that include an income augmenting cash transfer to the poor or a subsidy for the basic needs of food and housing: PDS, urea and nutrient subsidy, MGNREGS, LPG subsidy, ICDS, Pradhan Mantri Awas Yojana, mid-day meals, and NSAP. This is a lower bound estimate. Calculations use 2015-16 actual budget expenditure from the Ministry of Finance.
3. The total budget of 2015-16 is ₹17.9 lakh crore ($267 billion). Social protection expenditure was more than 17.6 percent of this total. Calculations use 2015-16 actual budget expenditure from the Ministry of Finance.
4. "*Economic Survey 2016-17*." Department of Economic Affairs, Ministry of Finance, Government of India, 2017. http://finmin.nic.in/indiabudget2017-2018/es2016-17/echapter.pdf.
5. "Aadhaar Enabled Service Delivery." Unique Identification Authority of India, 2012. https://uidai.gov.in/images/resource/whitepaper_aadhaarenabledservice_delivery.pdf.
6. Ibid.
7. Ibid.
8. "Advancing the Development Agenda with Aadhaar." Unique Identification Authority of India, 2014. https://uidai.gov.in/images/Aadhaar-English.pdf.
9. For instance, Aadhaar seeding varies across schemes with only 19% seeding for scholarship schemes and about 80% for MGNREGS and LPG (PAHAL) as of December 2016. The percentage of beneficiaries seeded has been increasing. In MGNREGS, seeding rose from about 52% in September 2015 to about 81% as of February 2017.
10. This calculation is of the major social protection programmes identified by us that are using Aadhaar. Of the eight programmes, the schemes using Aadhaar are: PDS, MGNREGS, LPG Subsidy, ICDS, NSAP and Mid-day meals. These account for ₹2.4 lakh crore of the ₹3.3 lakh crore spent on social protection.
11. Direct Benefit Transfer Mission, Government of India. "DBT Saving." Accessed May 16, 2017. https://dbtbharat.gov.in/page/frontcontentview/?id=ODM=.

    "Statement by Shri Ravi Shankar Prasad, Minister of Electronics & IT and Law & Justice." Press Release. Unique Identification Authority of India, January 27, 2017. https://uidai.gov.in/images/news/on_111_crore_aadhaar_31012017.pdf.
12. "FP Shops Left Over Beneficiaries Report." Society for Social Audit, Accountability and Transparency, 2015. http://www.socialaudit.ap.gov.in/SocialAudit/LoadDocument?docName=Fair%20Price%20Work%2%20Shops%20(Ration%20Card%20Holders)%20-%20Beneficiaries%20Report.pdf&type=application.
13. Reasons for authentication failures for beneficiaries of NTR Bharosa, a pensions programme, in Andhra Pradesh, and MGNREGS and SSP (another pensions programme) in Telangana and Andhra Pradesh, are presented in Figure 5.6.
14. PDS alone accounts for 667 million beneficiaries (see Figure 5.3). This estimate is calculated using data from state government PDS portals and census data. As per the Ministry of Consumer Affairs, Food and Civil Supplies Department there are a total of 232 million ration cards.
15. The government spends more than ₹2 lakh crore on the four programmes that form the focus of this Chapter, out of total annual spending of more than ₹3 lakh crore on social protection.
16. "Annual Report 2016-17." Ministry of Consumer Affairs, Food and Public Distribution, Government of India, December 2016. http://dfpd.nic.in/writereaddata/images/annual-140217.pdf.
17. Open Budgets India. "Union Budget (2017-18) - Department of Food and Public Distribution." Dataset. Department of Food and Public Distribution, Government of India. Accessed April 15, 2017. https://openbudgetsindia.org/dataset/department-of-food-and-public-distribution-2017-18.
18. Open Budgets India. "Union Budget (2017-18) - Department of Rural Development." Dataset. Department of Rural Development, Government of India. Accessed April 15, 2017. https://openbudgetsindia.org/dataset/department-of-rural-development-2017-18.
19. Open Budgets India. "Union Budget (2017-18) - Ministry of Petroleum and Natural Gas." Dataset. Ministry of Petroleum and Natural Gas, Government of India. Accessed April 15, 2017. https://openbudgetsindia.org/dataset/ministry-of-petroleum-and-natural-gas-2017-18.
20. "National Social Assistance Programme Guidelines. " Ministry of Rural Development, 2014. http://www.nsap.nic.in/Guidelines/nsap_guidelines_oct2014.pdf.

21. "Report of the Expert Group to Review the Methodology for Measurement of Poverty." Planning Commission, Government of India, 2014.
http://planningcommission.nic.in/reports/genrep/pov_rep0707.pdf.

22. Open Budgets India. "Union Budget (2017-18) - Department of Rural Development." Dataset. Department of Rural Development, Government of India. Accessed April 15, 2017.
https://openbudgetsindia.org/dataset/department-of-rural-development-2017-18.

23. The full title of this Act is Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016.

24. "Notification." Gazette of India. Ministry of Rural Development, Government of India, January 3, 2017.
http://nrega.nic.in/netnrega/writereaddata/Circulars/2001173479.pdf.
"Notification." Gazette of India. Ministry of Consumer Affairs, Food and Public Distribution, Government of India, February 8, 2017.
http://dfpd.nic.in/writereaddata/Portal/Magazine/Document/1_211_1_aadhaar-notification.pdf.

25. "Economic Survey 2016-17." Department of Economic Affairs, Ministry of Finance, Government of India, 2017.
http://finmin.nic.in/indiabudget2017-2018/es2016-17/echapter.pdf. 199-200.

26. "Ghost" beneficiaries refer to individuals who have passed away, but continue to be on the beneficiary list of a programme.

27. "Aadhaar Enabled Service Delivery." Unique Identification Authority of India, 2012.
https://uidai.gov.in/images/resource/whitepaper_aadhaarenabledservice_delivery.pdf.

28. Ibid.

29. "MNREGA Dashboard: At a Glance." Ministry of Rural Development, Government of India. Accessed May 9, 2017.
http://mnregaweb4.nic.in/netnrega/all_lvl_details_dashboard_new.aspx.

30. "Aadhaar Enabled Service Delivery." Unique Identification Authority of India, 2012.
https://uidai.gov.in/images/resource/whitepaper_aadhaarenabledservice_delivery.pdf.

31. Ibid.

32. Ibid.

33. "Envisioning a Role for Aadhaar in the Public Distribution System." Working Paper. Unique Identification Authority of India, June 24, 2010.
https://uidai.gov.in/images/resource/Circulated_Aadhaar_PDS_Note.pdf.

34. Direct transfer of cash benefits to bank accounts are portable as bank accounts can be accessed across India. DBTs are covered in more detail below.

35. "Aadhaar: Dynamics Of Digital Identity." Unique Identification Authority of India, 2015.
https://uidai.gov.in/images/news/aadhaar_dynamics_of_digital_identity_19082016.pdf.

36. "Aadhaar Enabled Service Delivery." Unique Identification Authority of India, 2012.
https://uidai.gov.in/images/resource/whitepaper_aadhaarenabledservice_delivery.pdf.

37. It is important to note that in most cases Aadhaar seeding does not weed out individuals who physically exist but are legally not entitled to a particular social protection programme. For example, food subsidies are higher for those below the poverty line. If someone above the poverty line is listed as being below it, Aadhaar isn't able to correct this. As a rule, Aadhaar doesn't collect socioeconomic data. The *Economic Survey 2016-17* reports that about 40 percent of listed beneficiaries are not entitled to their benefits.

38. "The Direct Benefit Transfer." DBT Mission, Cabinet Secretariat, 2015.
https://dbtbharat.gov.in/data/documents/REPORT-ON-DBT.pdf.

39. Ibid.

40. Seeding figures for DBT (LPG, MGNREGS and NSAP):
"DBT Monthly Report Send to Prime Minister's Office." Dataset. DBT Mission, Cabinet Secretariat, Government of India, December 2016. https://dbtbharat.gov.in/data/documents/DBT_MPR__Dec_2016.pdf. Seeding figures from PDS:
"Annual Report 2016-17." Ministry of Consumer Affairs, Food and Public Distribution, Government of India, December 2016.
http://dfpd.nic.in/writereaddata/images/annual-140217.pdf.

41. "Annual Report 2016-17." Ministry of Consumer Affairs, Food and Public Distribution, Government of India, December 2016.
http://dfpd.nic.in/writereaddata/images/annual-140217.pdf.

42. Seventy-two percent of the PDS beneficiary households have at least one member seeded to Aadhaar.
"DBT Saving." Dataset. Direct Benefit Transfer Mission, Government of India. Accessed May 19, 2017.
https://dbtbharat.gov.in/page/frontcontentview/?id=ODM=.

43. Value of savings in rupees: Ibid. Number of Duplicates: Unique Identification Authority of India. "Aadhaar, Gateway to DBT." presented at the Direct Benefit Transfer Event. Accessed May 17, 2017.
https://dbtbharat.gov.in/data/events/Aadhaar_Imphal.pdf.

44. Report of The Comptroller and Auditor General Of India On Implementation Of PAHAL (DBTL) Scheme. Compliance Audit of Ministry Of Petroleum And Natural Gas. Comptroller and Auditor General of India. 2016.
http://www.cag.gov.in/sites/default/files/audit_report_files/Union_Commercial_Compliance_Full_Report_25_2016_English.pdf.

45. Source for figure on total beneficiaries: “Over 1.20 Crore Bogus Rations Cards Deleted During The Last Three Years.” Press Release. Ministry of Consumer Affairs, Food and Public Distribution, Government of India, December 8, 2015.
http://pib.nic.in/newsite/mbErel.aspx?relid=132754.
Source for figure on duplicates removed by Aadhaar: “Report on Aadhaar Enabled De-Duplication & Verification Exercise.” Unique Identification Authority of India, August 2014.
https://uidai.gov.in/images/resource/bangalore_analysis_report_v_1.1_26052015.pdf.

46. “Envisioning a Role for Aadhaar in the Public Distribution System.” Working Paper. Unique Identification Authority of India, June 24, 2010.
https://uidai.gov.in/images/resource/Circulated_Aadhaar_PDS_Note.pdf.

47. Ibid.

48. “PoS Devices in Fair Price Shops: Answer to Unstarred Question Question 6046.” Lok Sabha Question. Ministry of Consumer Affairs, Food and Public Distribution, Government of India, April 11, 2017.
http://164.100.47.190/loksabhaquestions/annex/11/AU6046.pdf.

49. “Disbursal of Fertilizer Subsidy: Answer to Unstarred Question 539.” Lok Sabha Question. Ministry of Chemicals and Fertilizers, Department of Fertilizers, Government of India, May 11, 2017.
http://164.100.47.190/loksabhaquestions/annex/11/AS539.pdf.

50. “Aadhaar Authentication User Agency (AUA) Handbook - Version 1.0.” Unique Identification Authority of India, January 2014.
https://www.uidai.gov.in/images/aua_handbook_v1.0_final_30012014.pdf.

51. The three categories have been grouped from 86 error codes provided by the UIDAI for authentication failures. “API ErrorHandling.” Unique Identification Authority of India Authentication Portal. Accessed May 7, 2017.
https://authportal.uidai.gov.in/web/uidai/developer.

52. Standing Committee in Finance (2011-12). “Forty Second Report: The National Identification Authority of India Bill, 2010.” Ministry of Planning, December 2011.
http://164.100.47.134/lsscommittee/Finance/42%20Report.pdf.

53. “API Error Handling.” Unique Identification Authority of India Authentication Portal. Accessed May 7, 2017.
https://authportal.uidai.gov.in/web/uidai/developer.

54. Calculation was done using authentication attempts analysis data from three portals: NTR Bharosa portal, APOnline portal, and TSOnline portal. Error codes provided by UIDAI were used to categorise the errors into three types. Weighted average was calculated using the number of authentication failures for each scheme.
“Authentication Success Ratio.” 2017. Benefit Disbursal Portal Telangana. Accessed March 17, 2017.
http://tspost.aponline.gov.in/PostalWebPortal/UserInterface/Portal/Reports/Aadhaar/AadhaarAuthAttemptWiseSummaryHOWise.aspx?SC=T
“Authentication Success Ratio.” 2017. NTR Bharosa Portal AP. Accessed March 17, 2017.
http://abdg.aponline.gov.in/NTRBharosa/UserInterface/Portal/Reports/Aadhaar/AadhaarAuthAttemptWiseSumaryDistrictWise.aspx.
“Authentication Success Ratio.” 2017. Benefit Disbursal Portal AP. Accessed March 17, 2017.
http://appost.aponline.gov.in/PostalWebPortal/UserInterface/Portal/Reports/DoP/DopAuthSuccessRatio_New.aspx?SC=AP.

55. Ibid.

56. Ibid.

57. “Role of Biometric Technology in Aadhaar Authentication”. Unique Identification Authority of India, 2012.
https://uidai.gov.in/images/role_of_biometric_technology_in_aadhaar_authentication_020412.pdf

58. “Annual Report 2016-17.” Ministry of Consumer Affairs, Food and Public Distribution, Government of India, December 2016.
http://dfpd.nic.in/writereaddata/images/annual-140217.pdf.

59. “Aadhaar Enabled Service Delivery.” Unique Identification Authority of India, 2012.
https://uidai.gov.in/images/resource/whitepaper_aadhaarenabledservice_delivery.pdf.

60. Ibid.

61. “The Direct Benefit Transfer.” DBT Mission, Cabinet Secretariat, 2015.
https://dbtbharat.gov.in/data/documents/REPORT-ON-DBT.pdf.

62. Babu. A. “Disbursement of Pensions through JAM Based.” Direct Benefit Transfer Mission, Government of India, November 1, 2016.
https://dbtbharat.gov.in/successstory/view?id=T0E9PQ==.

63. “The Direct Benefit Transfer.” DBT Mission, Cabinet Secretariat, 2015.
https://dbtbharat.gov.in/data/documents/REPORT-ON-DBT.pdf.

64. This is called the Institution Identification Number (IIN). Ibid.

65. “The Direct Benefit Transfer.” DBT Mission, Cabinet Secretariat, 2015.
https://dbtbharat.gov.in/data/documents/REPORT-ON-DBT.pdf.

66. "Aadhaar Enabled Benefit Disbursement." Andhra Pradesh Benefit Disbursement Portal, February 12, 2013.
http://appost.aponline.gov.in/PostalWebPortal/Documents/APOnlineAEPS.pdf.

67. Annual Report 2016-17. Ministry of Consumer Affairs, Food and Public Distribution, Government of India, December 2016.
http://dfpd.nic.in/writereaddata/images/annual-140217.pdf.

68. Open Budgets India. "Union Budget (2017-18) - Department of Food and Public Distribution." Dataset. Department of Food and Public Distribution, Government of India. Accessed April 15, 2017.
https://openbudgetsindia.org/dataset/department-of-food-and-public-distribution-2017-18.

69. "Ration Cards and Fair Price Shops: Answer to Starred Question 170." Lok Sabha Question. Ministry of Consumer Affairs, Food and Public Distribution, Government of India, March 14, 2017.
http://164.100.47.190/loksabhaquestions/annex/11/AS170.pdf

70. "Subsidized Foodgrains from Fair Price Shops: Answer to Unstarred Question 3073." Lok Sabha Question. Ministry of Consumer Affairs, Food and Public Distribution, Government of India, March 21, 2017.
http://164.100.47.190/loksabhaquestions/annex/11/AU3073.pdf

71. "Notification." Gazette of India. Ministry of Consumer Affairs, Food and Public Distribution, Government of India, February 8, 2017.
http://dfpd.nic.in/writereaddata/Portal/Magazine/Document/1_211_1_aadhaar-notification.pdf.

72. "Computerization of Fair Price Shops: Answer to Unstarred Question 3172." Lok Sabha Question. Ministry of Consumer Affairs, Food and Public Distribution, Government of India, March 21, 2017.
http://164.100.47.190/loksabhaquestions/annex/11/AU3172.pdf

73. Two union territories, Chandigarh and Pondicherry, have introduced Direct Benefits Transfer under PDS wherein the subsidy amount is directly deposited in the beneficiaries' bank accounts. Another union territory, Dadra and Nagar Haveli, has done so partially.

74. Open Budgets India. "Union Budget (2017-18) - Department of Rural Development." Dataset. Department of Rural Development, Government of India. Accessed April 15, 2017.
https://openbudgetsindia.org/dataset/department-of-rural-development-2017-18.

75. MGNREGA Public Data Portal (report on total persons worked in FY 2016-17 generated). Ministry of Rural Development, Government of India, accessed 17 June 2017.
http://mnregaweb4.nic.in/netnrega/dynamic2/dynamicreport_new4.aspx

76. Mahatma Gandhi NREGA e-FMS Manual: Volume 1. Ministry of Rural Development, Government of India. 2012.
http://mgnrega.nic.in/Netnrega/Data/eFMS%20Manual_ritesh_V5_10may2012.pdf

77. "LPG Coverage Ratio: Answer to Unstarred Question 2063." Lok Sabha Question. Ministry of Petroleum and Natural Gas, Government of India, November 28, 2016.
http://164.100.47.190/loksabhaquestions/annex/10/AU2063.pdf

78. "LPG Connections: Answer to Unstarred Question 2990." Lok Sabha Question. Ministry of Petroleum and Natural Gas, Government of India, March 20, 2017.
http://164.100.47.190/loksabhaquestions/annex/11/AU2990.pdf

79. "LPG Subsidy: Answer to Unstarred Question 5945." Lok Sabha Question. Ministry of Petroleum and Natural Gas, Government of India, April 10, 2017.
http://164.100.47.190/loksabhaquestions/annex/11/AU5945.pdf

80. Ibid.

81. "Time Limit for Transfer of LPG Subsidy: Answer to Unstarred Question 19." Lok Sabha Question. Ministry of Petroleum and Natural Gas, Government of India, July 18, 2016.
http://164.100.47.190/loksabhaquestions/annex/9/AU19.pdf

82. Ibid.

83. Ibid.

ENDNOTES Chapter 6: Emerging Uses

1. APIs are a tool for building software applications. APIs are defined as a "set of functions and procedures that allow the creation of applications which access the features or data of an operating system, application, or other service."
"Definition of API in English." *Oxford English Dictionary*. Oxford University Press. Accessed May 26, 2017.
https://en.oxforddictionaries.com/definition/api.

2. "What Is India Stack?" Informational website. *About - IndiaStack*. Accessed April 1, 2017. https://indiastack.org/about/.

3. "Dedicated Repository (Push) API Specification Version 1.7." API technical specifications. DigiLocker, July 2016. https://img1.digitallocker.gov.in/assets/img/digital_locker_dedicated_repository_(push)_API_specification_v1_7_2.pdf.

4. "Pull API Specification Version 1.3." API technical specifications. DigiLocker, July 2016. https://img1.digitallocker.gov.in//assets/img/digital_locker_pull_API_specification_v1_3.pdf.

5. "Requester Specification Version 2.1." API technical specifications. DigiLocker, July 2016. https://img1.digitallocker.gov.in/assets/img/digital_locker_requester_API_specification_v2_1.pdf.

6. Issuers must have an individual's Aadhaar details in their databases in order to be able to push documents into her or his locker.

7. "DigiLocker National Statistics." Data dashboard. DigiLocker | Dashboard. Accessed May 26, 2017. https://digilocker.gov.in/public/dashboard.

8. Government Of India, DigiLocker. "How Users Can Get Their Digital Driving License & Vehicle Registration from DigiLocker." Slideshare, September 15, 2016. https://www.slideshare.net/digilocker_ind/how-users-can-get-their-digital-driving-license-vehicle-registration-from-digilocker-66061579.

9. "DigiLocker National Statistics." Data dashboard. DigiLocker | Dashboard. Accessed May 20, 2017. https://digilocker.gov.in/public/dashboard.

10. This number was calculated by multiplying the percentage of Internet users (26%) by a recent India population estimate (1.32 billion).

    "Individuals Using the Internet (% of Population)." Data Dashboard. International Telecommunication Union, World Telecommunication/ICT Development Report and Database. World Bank. Accessed May 9, 2017. http://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=IN&view=chart.

    "UNdata | Country Profile | India." Data Dashboard. World Statistics Pocketbook. United Nations. Accessed May 9, 2017. http://data.un.org/CountryProfile.aspx?crName=INDIA.

11. "DigiLocker National Statistics." Data dashboard. DigiLocker | Dashboard. Accessed April 9, 2017. https://digilocker.gov.in/public/dashboard.

12. Digital India is an initiative by the Government of India with the key goals of: "Infrastructure as Utility to Every Citizen," "Governance and Service on Demand," and "Digital Empowerment of Citizens." It was approved by the Cabinet on August 2014. Digital Locker is part of the Digital India programme.

    "Digital India – A Programme to Transform India into Digital Empowered Society and Knowledge Economy." Press Release. Press Information Bureau, August 20, 2014. http://pib.nic.in/newsite/PrintRelease.aspx?relid=108926.

    "Unstarred Question No. 382 Digital India." Lok Sabha Questions, July 22, 2015. 164.100.47.190/loksabhaquestions/annex/5/AU382.docx.

13. Digital Locker Authority (DLA), set up by the Ministry of Electronics and Information Technology, is responsible for overseeing the Digital Locker system. The aim of the digital locker is to store information for users in a way that facilitates efficient service delivery.

    "About Us." *About Us | Digital Locker Authority*. Accessed May 18, 2017. http://dla.gov.in/?q=about.

14. "Digital Locker Licensing Advertisement." Advertisement. Digital Locker Authority, Government of India, March 2017. http://meity.gov.in/writereaddata/files/digital-locker-licensing-advertisement.pdf.

15. Government Of India, Ministry of Electronics and Information Technology. "eSign – Online Electronic Signature Service." Department information page. eSign | CCA. Accessed April 12, 2017. http://cca.gov.in/cca/?q=eSign.html.

16. IndiaStack. "About eSign API." *About eSign API - IndiaStack*. Accessed May 18, 2017. https://indiastack.org/esign/.

17. "DigiLocker National Statistics." Data dashboard. DigiLocker | Dashboard. Accessed April 9, 2017. https://digilocker.gov.in/public/dashboard.

18. "Request for Expression of Interest (REOI) for 'Design, Development, Integration, Deployment, Implementation and Maintenance of Integrated Health Information Platform (IHIP).'" Request for expression of interest. Ministry of Health and Family Welfare, Government of India, August 11, 2016. https://www.nhp.gov.in/NHPfiles/Expression%20of%20Interest_IHIP_11_08_2016_v4_1.pdf.

19. Government Of India, Ministry of Electronics and Information Technology. "Online Registration System." ORS Patient Portal. Accessed May 15, 2017. http://ors.gov.in/index.html.

20. "Assistance to Beneficiaries Registered under Janani Suraksha Yojna (JSY)." Press Release, August 11, 2015. http://pib.nic.in/newsite/PrintRelease.aspx?relid=124763.

21. "DBT Progress Report for March 2017." Data Dashboard. DBT Mission, Government of India. Accessed May 15, 2017.
https://dbtbharat.gov.in/data/documents/mpr_March_2017.pdf.

22. "Starred Question No. 422 Linking of Child Development Schemes with Aadhaar." Lok Sabha Questions, December 12, 2016.
http://164.100.47.190/loksabhaquestions/annex/10/AS422.pdf.

23. "Register Aadhaar Card." Registration information. Register Aadhaar Card | National AIDS Control Organization | MoHFW | GoI, December 19, 2016.
http://www.naco.gov.in/register-aadhaar-card.

24. "Aadhaar Based Smart Cards Containing Health Details for Senior Citizens to Be Introduced." Press Release. Press Information Bureau, n.d.
http://pib.nic.in/newsite/PrintRelease.aspx?relid=157862.

25. "DigiLocker National Statistics." Data dashboard. DigiLocker | Dashboard. Accessed April 9, 2017.
https://digilocker.gov.in/public/dashboard.

26. Marksheets (or "marks statement") is a statement issued by the Central Board of Secondary Education for those who have appeared in an examination administered by the Board. Migration certificates provides certification to facilitate any future enrollment in education courses.

27. "Ministry of Human Resource Development, Department of School Education and Literary, Notification." Gazette of India. New Delhi: Ministry of Human Resource Development, Government of India, March 2, 2017.
http://mhrd.gov.in/sites/upload_files/mhrd/files/SSA_AADHAR.pdf.

28. "Ministry of Human Resource Development, Department of School Education and Literary, Notification." Gazette of India. New Delhi: Ministry of Human Resource Development, Government of India, February 28, 2017.
http://mdm.nic.in/Files/Aadhar/Aadhar_mdm.pdf.

29. "Unstarred Question No. 5863 Aadhaar Card for Mid Day Meal Scheme." Lok Sabha Questions, April 10, 2017
http://164.100.47.190/loksabhaquestions/annex/11/AU5863.pdf.

30. Assam, Meghalaya, and Jammu & Kashmir are exempted from the notification because of overall low Aadhaar enrolment.

31. "Ministry of Human Resource Development, Department of School Education and Literary, Notification." Gazette of India. New Delhi: Ministry of Human Resource Development, Government of India, February 28, 2017.
http://mdm.nic.in/Files/Aadhar/Aadhar_mdm.pdf.

32. "Unstarred Question No. 4156 Aadhaar Card for JEE." Lok Sabha Questions, December 12, 2016.
http://164.100.47.190/loksabhaquestions/annex/10/AU4156.pdf.

33. "Starred Question No. 511 Aadhaar Card for NEET Examination." Lok Sabha Questions, April 4, 2017.
http://164.100.47.190/loksabhaquestions/annex/11/AS511.pdf.

34. As above, Assam, Meghalaya, and Jammu & Kashmir are exempted from the notification because of overall low Aadhaar enrolment.

35. Pre-matric stands for pre-matriculation, and post-matric for post-matriculation. Matriculation generally refers to successfully completing the tenth grade exam. Merit-cum-means scholarships generally refer to the scholarships provided to students of merit from a lower socioeconomic background.

36. "Unstarred Question No. 900 Aadhaar Card for School Benefits." Lok Sabha Questions, November 21, 2016
http://164.100.47.190/loksabhaquestions/annex/10/AU900.pdf.

37. Sandhu, Jaspal S. "University Grants Commission Letter on Ensuring Aadhaar-Linked DBT Payments for All Scholarship/Fellowships," July 20, 2016.
http://www.ugc.ac.in/pdfnews/6606505_UGC-letter-reg-Scholarships--Fellowships-(1).pdf.

38. See Chapter 4 and Chapter 5 to learn more about Direct Benefit Transfers (DBTs) and the Aadhaar Payment Bridge System (APBS).

39. Government Of India, Ministry of Electronics and Information Technology. "E-District." Ministry information page. *E-District | Ministry of Electronics and Information Technology, Government Of India*. Accessed April 12, 2017.
http://meity.gov.in/content/e-district.

40. "DigiLocker National Statistics." Data dashboard. DigiLocker | Dashboard. Accessed April 9, 2017.
https://digilocker.gov.in/public/dashboard.

41. According to the CSC website, "Common Services Centres (CSC) are a strategic cornerstone of the Digital India programme. They are the access points for delivery of various electronic services to villages in India, thereby contributing to a digitally and financially inclusive society."

Government Of India, Ministry of Electronics and Information Technology. "About Common Services Centres Scheme." Accessed May 18, 2017.
https://www.csc.gov.in/.

42. MCTS is a tracking system that monitors access to maternal and child health services with an aim toward increasing access and improving service delivery.

Government of India, Ministry of Health and Family Welfare. "Mother & Child Tracking System." *Mother & Child Tracking*

System | Government of India. Accessed May 18, 2017.
http://nrhm-mctsrpt.nic.in/Home.aspx.
Government of Uttarakhand, India, Uttarakhand Health & Family Welfare Society. “Mother & Child Tracking System (MCTS).” *Welcome to Uttarakhand Health & Family Welfare Society*. Accessed May 18, 2017.
http://www.ukhfws.org/details.php?pgID=mn_2563.

43. “Aadhaar Linked Birth Registration of New Born Child.” Registrar General of India, Government of India. Accessed May 16, 2017.
http://yamunanagar.nic.in/g/DwD/Digital_India/ALBR%20.pdf.

44. Government Of India, Unique Identification Authority of India. “Easy Verification for Your Mobile Sim with Aadhaar Based E-KYC. Read More about It from DoT Here -Https://Goo.gl/xVig8y #BenefitsOfAadhaar.” Twitter, October 24, 2016.
https://twitter.com/UIDAI/status/790533909494702080.

45. Tirkey, A. K. “Instructions on Verification of New Mobile Subscribers (Pre-Paid & Postpaid),” August 9, 2012.
http://www.dot.gov.in/sites/default/files/Instructions%20on%20Verification%20of%20New%20Mobile%20Subscribers%20%281%29.PDF?download=1.

46. “Highlights of Telecom Subscription Data as on 31st October, 2016.” Press Release. Telecom Regulatory Authority of India, Government of India, January 9, 2017.
http://www.trai.gov.in/sites/default/files/Telecom%20Sub_Eng_pr.03_09-01-2017_0.pdf.

47. Banzal, Sanjeev. “Verification of Existing Mobile Subscribers through Aadhaar Based E-KYC Services,” January 20, 2017.
http://www.trai.gov.in/sites/default/files/E_KYC_services_Rec_20_01_2017.pdf.

48. Verma, Prashant. “Implementation of Order of Hon’ble Supreme Court Regarding 100% E-KYC Based Re-Verification of Existing Subscribers,” March 23, 2017.
http://www.dot.gov.in/sites/default/files/Re-verification%20instructions%2023.03.2017.pdf.

49. IndiaStack. “About Aadhaar AUTH API.” *About Aadhaar AUTH API – IndiaStack*. Accessed May 14, 2017.
https://indiastack.org/aadhaar/.

ENDNOTES Chapter 7: Looking Ahead

1. Rodrigues, Jeanette. “PM Modi’s Aadhaar Program Wins World Bank Praise Amid Big Brother Fears.” UIDAI.gov.in, March 16, 2017.
https://uidai.gov.in/images/news/pm_modis_aadhaar_program_wins_world_bank_praise_amid_big_brother_fears_17032017.pdf.

2. We only request datasets that can lawfully be shared and for which individual identities can be made anonymous by our researchers.

Designed by

subū

studiosubu.com

IDinsight India

24/1, 3rd Floor, Hauz Khas Village
New Delhi 110 016, India

StateofAadhaar@IDinsight.org
IDinsight.org

IDinsight India is a Private Limited Company
CIN: U74140DL2013FTC252591