

STATE OF AADHAAR REPORT 2017-18



MAY 2018

SPONSORED BY:  OMIDYAR NETWORK



STATE OF AADHAAR REPORT 2017-18

MAY 2018

Ronald Abraham
Elizabeth S. Bennett
Rajesh Bhusal
Shreya Dubey
Qian (Sindy) Li
Akash Pattanayak
Neil Buddy Shah

Sponsored by



About IDinsight

IDinsight's mission is to help policymakers and practitioners use rigorous data and evidence to make more socially impactful decisions. We carefully tailor a wide range of quantitative tools to help our clients design better public policies, rigorously test those ideas, and take informed action to improve lives at scale.

IDinsight leads learning partnerships across Asia and Africa, working with governments, multilaterals, foundations, social businesses, and innovative NGOs. We have worked with more than 70 clients across 17 states in India and more than a dozen countries. We work across a range of sectors, including digital ID, education, financial access, governance, health, and sanitation.

We have offices in Dakar, Johannesburg, Lusaka, Manila, Nairobi, New Delhi, San Francisco, and Washington, D.C. To learn more, visit www.IDinsight.org, and follow on Twitter @IDinsight.

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 hundreds of millions of lower-income Indians, 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, Rajesh Bhusal, Shreya Dubey, Qian (Sindy) Li, Akash Pattanayak, and Neil Buddy Shah. *State of Aadhaar Report 2017-18*. Report. IDinsight, 2018.

Comments or questions

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 her or his own analysis of any information contained in this report.

While Omidyar Network is pleased to sponsor this report, the conclusions, opinions, or points of view expressed in the report do not necessarily represent the views of Omidyar Network.

PREFACE

In last year's *State of Aadhaar Report*, we drafted a comprehensive, empirical, and structured review of the Aadhaar landscape. This foundational assessment aimed to promote a more fact-based understanding of the ecosystem at-large. And more critically, we used this analysis to identify areas where more research was needed to understand whether and how Aadhaar can advance the welfare of India's residents.

For this year's report, we aimed to dive deeper into key issues in order to contribute primary research on critical topics highlighted in last year's report. After a series of consultations, we decided to conduct state-representative large-scale surveys to understand how individuals interact with and perceive Aadhaar. This allowed us to empirically explore important issues that to date were discussed without the support of rigorous evidence.

The main results of that survey are contained within these pages, supplemented with other independent research and additional data from the government.

During our initial phase of research design we received valuable inputs from a wide range of thought-leaders and researchers, including: Alan Gelb, Anurodh Giri, Avani Kapur, Reetika Khera, Vijay Madan, Anit Mukherjee, Ajay Bhushan Pandey, Vaishnavi Prathap, Malavika Raghavan, Emrys Schoemaker, Ajay Shah, and Janaki Srinivasan. We are thankful for their time and efforts.

This report would not have been possible without our incredible team at IDinsight. We are grateful to Doug Johnson for his thoughtful feedback as well as Ruchika Joshi for her contributions in our efforts to engage in a data-driven discourse. We also appreciate technical input and reviews from Qayam Jetha, Akib Khan, Jeff McManus, Marc Shotland, and Dan Stein – as well as feedback on our questionnaire from Heather Lanthorn.

We are thankful to Adi Raval and Divya Sooryakumar for their contributions to our communications strategy. We also benefited from the support and patience of the entire IDinsight Delhi office as they helped us brainstorm and work through these important issues.

And we appreciate the efforts of Syed Maqbool, Vinod Sharma, and Lalit Nayak who helped to lead our field teams in Andhra Pradesh, Rajasthan, and West Bengal, respectively.

Omidyar Network (ON) has continued to be a supportive thought-partner throughout this entire journey. In particular, we would like to convey our sincere appreciation for the efforts of CV Madhukar, Subhashish Bhadra, Roopa Kudva, Mike Kubzansky, and ON's entire Digital ID team.

The report itself has greatly benefited from the expertise of our design firm, Studio Subu, as well as our editor, Allan R. Gold.

Lastly, for their tireless efforts, we would like to thank our co-authors: Neil Buddy Shah, Qian (Sindy) Li, Rajesh Bhusal, Shreya Dubey, and Akash Pattanayak.

As always, any shortcomings in the report are our own. We hope this report facilitates meaningful dialogue on digital identity – both in India and abroad.

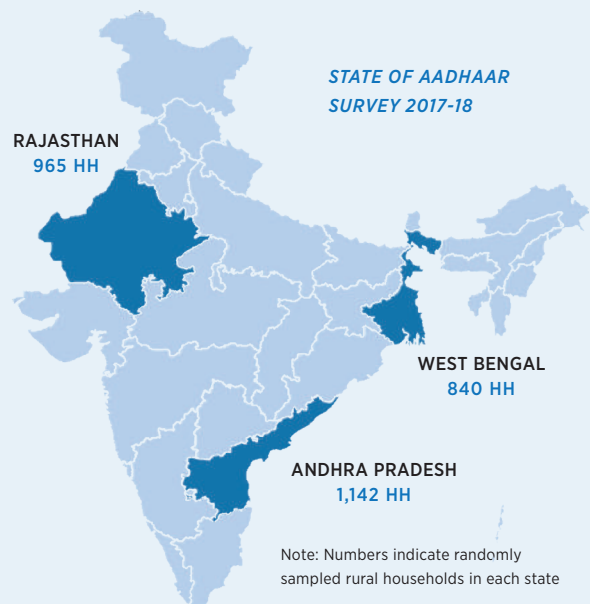
Ron and Elizabeth



EXECUTIVE SUMMARY

Aadhaar provides identification to more than 1.2 billion Indian residents. Its scale, ability to uniquely identify individuals, and digital interface make it a compelling identification platform. These same features also raise questions about privacy, data security, and exclusion. The current debate on Aadhaar is binary in nature: either Aadhaar should be jettisoned or scaled aggressively. However, the facts on the ground—as revealed by our three-state survey on Aadhaar, the largest to date—support a more nuanced approach. Our report's key takeaways explain why.

IDinsight's State of Aadhaar initiative aims to catalyse data-driven discourse and decision-making in the Aadhaar ecosystem. This report, the initiative's flagship output, aims to provide a holistic and empirically grounded assessment of the state of Aadhaar.



KEY TAKEAWAYS

Aadhaar's coverage is widespread, but the quality of the data has room for improvement.

1.5X more self-reported errors in Aadhaar compared to voter IDs
Demographic error-rate in Aadhaar is 8.8% vs. 5.7% for voter ID

A majority of Indians value privacy, but also approve of linking Aadhaar to services.

87% rural residents approve mandatory linking of Aadhaar
Approval for mandatory linking of Aadhaar to government services; for private services, corresponding figure is 77%

Aadhaar's analog version (the letter) is much more widely used to open bank accounts than its digital version (e-KYC).

17% bank a/c holders used Aadhaar e-KYC to open a/c
67% used Aadhaar letter; rest used other IDs; data for most recently opened bank account

Exclusion from food ration (PDS) due to Aadhaar-related factors is significant, but lower than non-Aadhaar factors.

2.2% of food ration recipients in Rajasthan excluded monthly due to Aadhaar-related factors
This extrapolates to ~1.2 million people per month in Rajasthan; non-Aadhaar factors account for 6.5% (or ~ 3.7 million people) of food ration (PDS) recipients excluded per month

Unless specified, all data cited in the executive summary are from our survey and apply to rural areas of Andhra Pradesh, Rajasthan, and West Bengal.

AADHAAR PLATFORM

Aadhaar has rapidly become the foundational identity document of Indian residents. It has achieved near-universality in its coverage and acceptance in India. We review key highlights of what has worked, what has not, and recommended next steps.

1.2 BILLION

residents currently enrolled on Aadhaar platform with over 90% adult saturation in most Indian states (UIDAI 2018)

271 MILLION

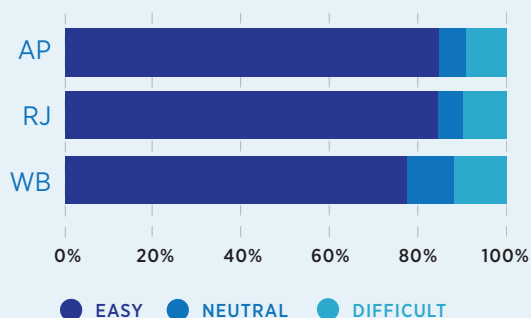
unique individuals used their Aadhaar to digitally authenticate themselves in Feb 2018 (UIDAI 2018). Even more use Aadhaar's analog version (the letter)

1. WHAT HAS WORKED?

Most people have an Aadhaar number and most felt it was easy to enroll

We find no evidence of differences in enrolment by gender, caste, religion, or education level.

USER PERCEPTION OF AADHAAR ENROLMENT PROCESS



In Andhra Pradesh and West Bengal, a relatively small number of people were wrongly charged an enrolment fee. However, in Rajasthan 24% paid a fee.

2. WHAT HAS NOT WORKED?

Aadhaar data has more self-reported errors than the voter ID database

ERROR COMPARISON (VOTER ID VS AADHAAR)

	IN VOTER ID	IN AADHAAR
ANDHRA PRADESH	2.4%	8.0%
RAJASTHAN	2.6%	4.8%
WEST BENGAL	10.4%	12.2%

ERRORS WITHIN AADHAAR

	NAME	ADDRESS	DOB
ANDHRA PRADESH	3.8%	1.2%	2.6%
RAJASTHAN	1.5%	0.7%	2.4%
WEST BENGAL	5.6%	1.7%	3.5%

People also encountered more challenges with the process of updating their Aadhaar, compared to the process of enrolling, such as paying higher-than-required fees.

3. EMERGING POLICY RECOMMENDATIONS

Facilitate updates to correct Aadhaar data

To reduce the number of errors in Aadhaar data, conduct "update campaigns" and set up camps, similar to the enrolment camps that were well-received and worked well in increasing Aadhaar coverage.

Reinforce awareness of fees and processes for enrolment and updates

Of those who paid higher-than-required fees, majority were unaware of the actual cost. Conduct awareness campaign around fees and processes, especially for vulnerable groups. Install a strong grievance redress mechanism.

AADHAAR AND FINANCIAL INCLUSION

The “Jan Dhan” banking scheme, Aadhaar, and mobile (together called “JAM”) are meant to play a pivotal role in the inclusion of unbanked, and underbanked, into the formal financial sector. There are two main channels through which Aadhaar can help increase financial inclusion:

1 Open a bank account with an Aadhaar letter or e-KYC

2 Increase account usage through microATMs & DBTs

48 TO 138 MILLION

increase in e-KYC verifications from FY 2016-17 to 2017-18 (NPCI 2018)

435

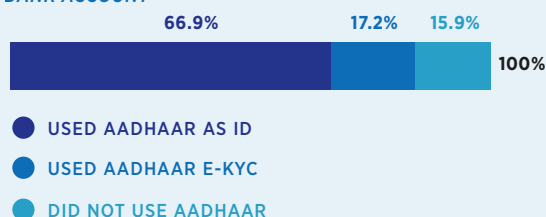
govt. schemes use DBTs to transfers benefits to bank accounts (some via Aadhaar), incentivising account usage

1. WHAT HAS WORKED?

Aadhaar has become a common proof-of-ID for bank account opening

The ubiquity of Aadhaar and its universal acceptance has meant a high proportion of people use it to open a bank account. However, 66.9% used their Aadhaar as an analog, paper ID not e-KYC (used by 17.2%).

USE OF AADHAAR IN OPENING MOST RECENT BANK ACCOUNT



2. WHAT HAS NOT WORKED?

Use of microATMs remains low; e-KYC may not quicken a/c opening

Only 17% of account-holders had recently used a microATM.

No meaningful difference in time reported to open an account with e-KYC vs. traditional KYC.

% OF RESPONDENTS WHO GOT ACCESS TO AN ACCOUNT WITHIN 1 DAY



3. EMERGING POLICY RECOMMENDATIONS

Strengthen business correspondent network

Too few people currently have access to alternatives to brick-and-mortar banks. Ready access to microATMs could change this; however, the network supporting business correspondents (BCs) needs to be strengthened.

Push toward mobile-based financial services

In the absence of a sustainable BC network, there is opportunity for mobile-based financial services to provide greater access to accounts, and help reduce dormancy. These services are able to use Aadhaar as an identity platform.

AADHAAR AND FOOD RATION (PDS)

Aadhaar is envisioned as a key reform in India's social protection programmes for the poor, especially the delivery of food ration subsidies via the Public Distribution System (PDS). Aadhaar's two main uses in PDS have grown steadily over the last year.

1 Aadhaar seeding (aims to remove duplicate and fake entries from databases)

2 Aadhaar-based biometric authentication (aims to prevent access to non-genuine persons)

72% TO 82%

increase in percentage of seeded PDS beneficiary households across all states in India (source in main report)

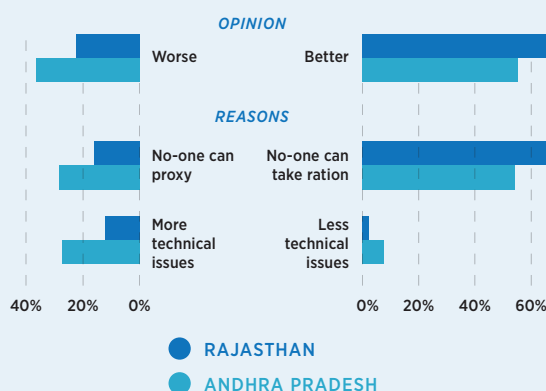
35% TO 57%

increase in percentage of PDS shops using e-PoS devices pan-India (Lok Sabha 2018)

1. WHAT HAS WORKED?

Households feel secure that no one else can take their ration

Majority in Andhra Pradesh and Rajasthan prefer Aadhaar-based PDS delivery as they perceive biometric authentication prevents identity fraud.



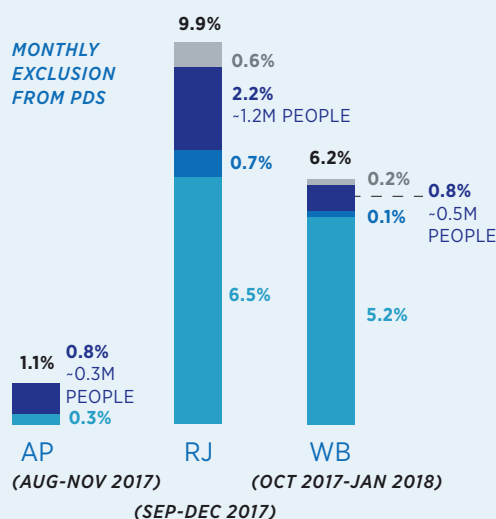
But biometrics is also the reason a quarter of the beneficiaries consider the system worse, as it reduces flexibility to send a proxy to collect ration on one's behalf.

For a more comprehensive treatment of these topics, please read the full report. To download the report, the technical appendix with tables, and learn about our research methodology, please visit www.StateofAadhaar.in.

2. WHAT HAS NOT WORKED?

Exclusion from receiving benefits due to Aadhaar-related factors significant

0.8%, 2.2%, and 0.8% of PDS beneficiaries in rural Andhra Pradesh, Rajasthan, and West Bengal, respectively, are excluded from their entitlements due to Aadhaar-related factors. This extrapolates to ~2 million individuals monthly. However, non-Aadhaar reasons, such as ration unavailability, contribute much more to exclusion from PDS.



- NON-AADHAAR REASONS
- AADHAAR AND NON-AADHAAR REASONS
- AADHAAR REASONS ONLY
- UNKNOWN



3. EMERGING POLICY RECOMMENDATIONS

To reduce programme exclusion, re-consider monthly biometric authentication

Explore alternative technologies (e.g., offline authentication) or processes (e.g., annual verification) that provide a similar secure experience, but reduce Aadhaar-related exclusion.

Enforce rules allowing alternate IDs or authentication mechanisms

Mechanisms are in place to ensure benefits are not denied due to Aadhaar; enforce these strongly. Awareness of other authentication means (e.g., mobile OTP) is low: popularise them.

LEGAL HIGHLIGHTS OF THE AADHAAR PLATFORM

In August 2017, the Supreme Court ruled that privacy is a fundamental constitutional right.

An overwhelming majority of Indians care about their right to privacy; more than 96% of respondents stated it is important for them to know how their Aadhaar information is used by the government.

AADHAAR AND TELECOM: QUICK HIGHLIGHTS

77% of respondents approved of the mandatory linking of Aadhaar to services, including mobile

More than 50% of respondents who got a SIM card in late 2016 or after, used e-KYC to do so

TABLE OF CONTENTS

Figures	1
Introduction	2
Aadhaar Platform	4
Aadhaar enrolment	
Aadhaar usage and awareness	
Aadhaar data quality and updating data	
Legal	13
Right to privacy judgement	
Mandatory linking of Aadhaar to services	
Data protection law	
Financial Inclusion	17
Opening a bank account	
Using a bank account	
Social Protection: Food Ration	22
User experience and exclusion	
User perception	
Government Savings	
Emerging Uses: Spotlight on Telecommunications	29
Looking Ahead	30
References	32

FIGURES

- Figure 1.1** Significant Aadhaar developments in Financial Year (FY) 2017-18
- Figure 1.2** State of Aadhaar Survey 2017-18, sample description
- Figure 2.1** Interactions with the Aadhaar system
- Figure 2.2** Comparison of SOA survey data and UIDAI data on enrolment
- Figure 2.3** Comparison of saturation level in Aadhaar and voter ID for adult population
- Figure 2.4** User perception of Aadhaar enrolment process
- Figure 2.5** Different uses of Aadhaar by residents
- Figure 2.6** Aadhaar authentication and unique residents authenticated over time, Apr 2016 – Feb 2018
- Figure 2.7** Proportion of Aadhaar awareness levels among survey respondents
- Figure 2.8** Comparison of errors in Aadhaar and voter ID
- Figure 2.9** Types of error on Aadhaar letters with a demographic error
- Figure 3.1** Importance of knowing how the government uses respondents' data (All three states: Andhra Pradesh, Rajasthan, West Bengal)
- Figure 3.2** Approval ratings on mandatory linking of Aadhaar to services, by entity type (All three states: Andhra Pradesh, Rajasthan, West Bengal)
- Figure 4.1** Proportion of respondents who used Aadhaar for bank account openings, since 2014
- Figure 4.2** Proportion of respondents who possessed other IDs among those who "Used Aadhaar as ID" to open an account, since 2014
- Figure 4.3** Monthly number of successful Aadhaar e-KYC verifications as per NPCI, Apr 2016 – Feb 2018
- Figure 4.4** Proportion of respondents who got access to account within 1 day among those who used e-KYC and those who did not
- Figure 4.5** Monthly transactions of AEPS and APBS, Apr 2016 – Feb 2018
- Figure 4.6** Proportion of respondents who used their bank accounts by whether they receive DBTs or not
- Figure 5.1** Proportion of beneficiaries seeded in India's major social protection programmes
- Figure 5.2** Proportion of fair price shops with e-PoS devices across India, Mar 2017 & Mar 2018
- Figure 5.3** Average monthly exclusion from PDS and role of Aadhaar, Aug 2017 – Jan 2018
- Figure 5.4** Breakdown of monthly exclusion rate by reasons for exclusion, for Rajasthan's PDS, Sep 2017 - Dec 2017
- Figure 5.5** Number of attempts required for successful Aadhaar-based Biometric Authentication in PDS
- Figure 5.6** Opinion on whether use of Aadhaar for PDS delivery is better or worse than previous system and associated reasons
- Figure 5.7** Government of India's savings estimate from Aadhaar, DBT, & other initiatives
- Figure 6.1** Proportion of respondents who used Aadhaar for SIM cards since late 2016
- Figure 6.2** Proportion of respondents got SIM activated in 1 day among those who used e-KYC vs. those who did not use e-KYC (All three states: Andhra Pradesh, Rajasthan, West Bengal)



INTRODUCTION

Aadhaar currently provides identification to more than 1.2 billion Indian residents, or more than 90 percent of India's population. Its scale, ability to uniquely identify individuals, and digital interface make it a compelling identification platform for use by the government, civil society, and private sector. These same features, however, raise questions about privacy, data security, and exclusion of vulnerable populations.

These concerns came to the fore on multiple occasions this past year, one of the most eventful since Aadhaar's inception in 2009. In Figure 1.1, we provide a timeline of these significant events.

Throughout this year, however, the discourse was fractious and polarized. Those challenging Aadhaar contended that it is a tool for surveillance and disempowerment of the poor and called for jettisoning the project. Those in government posited that Aadhaar empowers the poor, saves money for the exchequer, and increases state capacity. Their resulting policy prescription is to aggressively scale the use of Aadhaar.

We at the *State of Aadhaar* initiative believe that instead of this false dichotomy, India requires a more nuanced and empirically grounded discourse and decision-making ecosystem around Aadhaar. We advocate for a careful and case-by-case evaluation of Aadhaar's applications using objective data and evidence, in order to inform whether a given use should be advanced, adjusted, or abandoned.

For the first time in Aadhaar's history, we now have an opportunity to catalyse such a data-rich discourse. In the last one year, more robust and independent evidence on how Aadhaar is working has been generated than in any preceding year. The State of Aadhaar Survey 2017-18 (SOA survey) advances the evidence base with the largest survey on Aadhaar to date. The survey provides data representative of the rural populations of three states in India: Andhra Pradesh, Rajasthan, and West Bengal. Given the three states' varying cultural contexts, governance capacity, and take-up of Aadhaar use-cases, they also provide an indicative understanding of Aadhaar's status quo nationally. This survey, in conjunction with other published research and official data, form the basis for this report.

Our findings suggest that important reforms are required for Aadhaar to realise its potential, while simultaneously limiting the risks it poses. To make genuine progress on the role of Aadhaar within India, we invite a vigorous debate on our findings and their policy implications. We hope this debate advances objective, data-driven discourse and decision-making on Aadhaar, and motivates more independent research to answer questions as they arise. This type of empirical approach, we believe, will best serve the interests of the country's more than 1.3 billion residents.

Figure 1.1. Significant Aadhaar developments in Financial Year (FY) 2017-18

June 1: Ministry of Finance order mandates linking of Aadhaar with bank accounts

June 9: Supreme Court allows Aadhaar-PAN linkage

August 24: Supreme Court upholds the right to privacy as a fundamental right

October 16: Newspaper reports claim a 11-year old dies of starvation as her family was denied food subsidies due to their ration card not being linked to Aadhaar

November 19: Unique Identification Authority of India (UIDAI), in a Right to Information (RTI) reply, stated that 210 government websites disclosed Aadhaar data

November 27: Government of India releases a white paper on "Data Protection Framework for India"

January 4: Journalist for The Tribune reported that she was able to buy unauthorised access to a UIDAI portal enabling her to get demographic details of any individual upon entering a valid Aadhaar number

January 10: UIDAI announced virtual ID, limited e-KYC, and UID token

January 17: Five-judge constitution bench begins hearing 30 petitions challenging Aadhaar

Sources: Supreme Court orders, MeitY notification, newspaper reports

New to Aadhaar?

This report is written assuming a basic understanding of Aadhaar and its uses. If you require a primer, however, we suggest reading our first report: *State of Aadhaar Report 2016-17*.

RESEARCH METHODOLOGY

The *State of Aadhaar Report 2017-18* combines primary data collected from the SOA survey with secondary research that draws on administrative data and published research on Aadhaar.

State of Aadhaar Survey 2017-18

The survey is designed to provide representative state-level estimates of the rural populations of Andhra Pradesh, Rajasthan, and West Bengal. The states were chosen to be geographically distributed across India, representing diverse contexts of culture and state capacity. In addition, these states have varying penetration of Aadhaar in terms of enrolment and linkages to services.

A total of 2,947 households were surveyed in person (see Figure 1.2). The sample size was selected to maximise the precision of the estimates while managing operational constraints. We used the Election Commission's public, online voter ID database to construct the sampling frame. Sample selection used the probability proportional to size (PPS) method to sample districts (stratified by region) and sub-district units. Simple random sampling was used to select households and again to select individual respondents within households.¹

Secondary Research

Other sources for this report include data from various public portals maintained by the central and state governments, government reports and documents, and published independent research. Please see our full list of references at the end of the report.

Figure 1.2: State of Aadhaar Survey 2017-18, sample description

	AP	RJ	WB	ALL 3 STATES
Number of sampled households (and respondents)	1,142	965	840	2,947
Number of sampled household members	4,454	5,430	3,785	13,669
Number of sampled districts	6 (of 13)	8 (of 33)	7 (of 23)	21 (of 69)
Dates of survey	Nov-Dec 2017	Dec 2017 - Jan 2018	Jan-Feb 2018	Nov 2017 - Feb 2018
2017 rural population	34.8m	57.7m	65.9m	158.4m

Note: 2017 rural population estimates calculated using data from UIDAI and Census.
A detailed technical note on the survey methodology is available on www.StateofAadhaar.in.

1. One adult per household was selected to be the respondent. Some survey questions only concern the respondent themselves, while others concern all members of the household, including children.

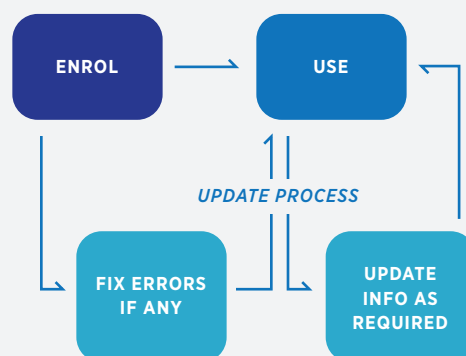


AADHAAR PLATFORM

Aadhaar is the world's largest publicly run digital identity database and it continues to grow. The database contains 1.2 billion enrollees and has facilitated nearly 24 billion digital authentications (Unique Identification Authority of India 2018). This demonstrates phenomenal growth since the first Aadhaar was issued in 2010, yet key questions related to the platform – enrolment and updating processes, usage, and data quality – remain unanswered. As we show in Figure 2.1, these areas comprise the major touchpoints with the Aadhaar system.

With the State of Aadhaar Survey 2017-18 (SOA survey), along with government administrative data, we begin providing initial answers in this section. Specifically, we seek to answer the following critical questions:

Figure 2.1: Interactions with the Aadhaar System



1. What are people's experience with the Aadhaar enrolment process? To what extent are people excluded from the Aadhaar platform itself?
2. How do people use their Aadhaar? What are the most common usages?
3. What is the quality of the demographic data captured by Aadhaar? What are individuals' experiences regarding fixing errors or updating their Aadhaar?

The next subsections discuss our findings related to these questions. This is followed by a discussion on our recommended next steps informed by the findings.

AADHAAR ENROLMENT

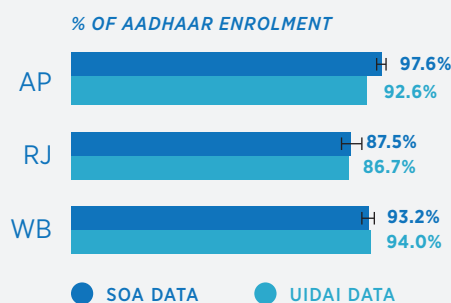
Overall Enrolment Trends in the SOA survey

The enrolment saturation rates from the SOA survey support the UIDAI's saturation data (see Figure 2.2). Beyond the high saturation rate of more than 90 percent, we looked into enrolment by different demographics. We do not find that members of vulnerable communities are less likely to be enrolled.² This is indicative that exclusion from Aadhaar is not only low, but also not systematically biased against the poor or vulnerable.

For those who tried to enrol in the Aadhaar system but were turned away (1 percent of all household members across the three states), we sought to understand why. The most common reason for rejection was "ineligibility due to biometrics" which was 30.9 percent across all three states.^{3,4} Given the centrality of biometric capture to the Aadhaar platform, the UIDAI should look into this issue further to determine root causes and to develop technological or manual solutions.

An important motivation for Aadhaar at the time of its inception was to provide formal identification to those who did not have one. However, in our survey, more than 99 percent of respondents in all three states had at least one other form of ID at the time of enrolment.⁵ This finding is also in line with an RTI response that demonstrated the number of enrolments that used the introducer system accounted for only 0.02 percent of total enrolments (Sharma (RTI) 2015).⁶

Figure 2.2: Comparison of SOA data and UIDAI data on enrolment

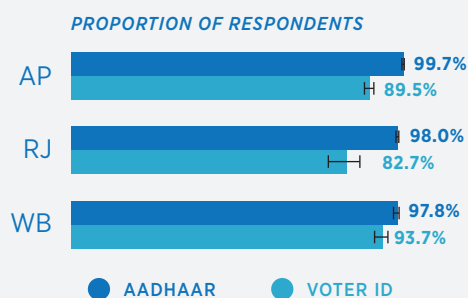


Note: Error bars denote 95% confidence intervals
 Number of observations: AP (4,448); RJ (5,396); WB (3,778)
 Data sources: State of Aadhaar Survey 2017-18;
 UIDAI State-wise Saturation Report, March 31, 2018

The most common forms of identification were ration cards and voter IDs. While both of these IDs are widely accepted, it should be noted that they also have limitations. Ration cards, in most states, are provided at the household level, not the individual level. Voter IDs are restricted to those eligible to vote—meaning eighteen years old and above. Thus, neither form of ID is universal in quite the same way as Aadhaar. A comparison of saturation rates for Aadhaar and voter ID in the three states we surveyed can be seen in Figure 2.3.

2. We tested for differences in the following populations: gender, religion, age, and caste. We found that respondents above the age of 60 are more likely to be enrolled. When conducting hypothesis tests for difference in outcomes between various groups we correct for multiple hypothesis testing using the Bonferroni correction. This applies to all hypothesis tests contained in this report.
3. "Ineligibility due to biometrics" refers to cases where residents were told that their biometrics are not of sufficient quality to enrol in Aadhaar.
4. There was variation across states; however, the number of state-level observations was too small to be able to report on any differences across states.
5. In the survey, we used voter rolls to construct the sampling framework. We are fairly confident that our sample captures households where some members of the household may have been left off the voter roll (as evidenced by the fact that more than 10 percent of adults within the sample did not have a voter ID). However, one limitation of the survey is that we would have been unable to capture households where no single member is on the voter list. For more details about the survey methodology, including limitations, please see www.StateofAadhaar.in.
6. The introducer system is intended to be an avenue of enrolment for individuals unable to provide proofs-of-identity.

Figure 2.3: Comparison of saturation level in Aadhaar and voter ID for adult population



Note: Error bars denote 95% confidence intervals

Number of observations (Aadhaar): AP (3,415); RJ (3,553);

WB (2,810) Number of observations (voter ID): AP (3,399);

RJ (3,553); WB (2,807)

Data source: State of Aadhaar Survey 2017-18

Analysing the enrolment process

The UIDAI has built a sizeable infrastructure for the purposes of enrolment. We describe this infrastructure in the Aadhaar Architecture chapter of the *State of Aadhaar Report 2016-17*. In this year's report we focus on the efficacy of these systems, the resulting user experience, and user perceptions of the enrolment process.

UIDAI regulations state that enrolment in Aadhaar is free and no entity can charge a fee for this service (UIDAI 2016). However, findings from our survey show that this regulation has not always borne out in practice. The

highest incidence of deviation was found in Rajasthan, with 23.7 percent of people stating that they paid to enrol in Aadhaar. Those in Andhra Pradesh and West Bengal experienced this issue as well with 9.0 percent and 5.7 percent of people, respectively, paying to enrol. Those who enrolled in an Aadhaar camp were less likely to have paid for enrolment in all three states.

While many enrollees reported facing inconveniences such as failed enrolment or the charging of unnecessary fees, an overwhelming majority of the respondents in all three states indicated they found the enrolment process to be "easy" (see Figure 2.4).

AADHAAR USAGE AND AWARENESS

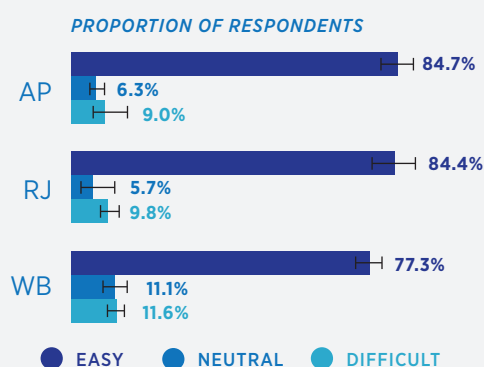
A critical but largely unanswered question is how do people tend to use their Aadhaar. Below, we explore the most common types of uses and look into how many people use each type.

Usage to establish identity

The most common reported use of Aadhaar for establishing identity is providing a photocopy of one's Aadhaar letter.⁷ More than 93 percent of respondents in all three states claimed they have used Aadhaar in this way to establish their identity (see Figure 2.5). The next most common usage is fingerprint authentication. While this use is widespread in Andhra Pradesh (95.4 percent) and Rajasthan (76.7 percent), it is less common in West Bengal (48.8 percent). One probable explanation is the fact that West Bengal's ration system does not currently use Aadhaar-based biometric authentication at a large scale. Iris authentication usage in Andhra Pradesh is much higher than in Rajasthan and West Bengal. This is likely due to the use of iris authentication in the Public Distribution System (PDS) and cash withdrawals from iris-enabled microATMs.

Data from the UIDAI shows that the number of overall Aadhaar authentications is growing steadily. Similarly, the number of unique IDs (UIDs) authenticated continues to trend upward (UIDAI 2018). In February 2018, 271 million individuals used their Aadhaar to authenticate themselves, representing nearly one in four people in possession of an Aadhaar (see Figure 2.6).

Figure 2.4: User perception of Aadhaar enrolment process



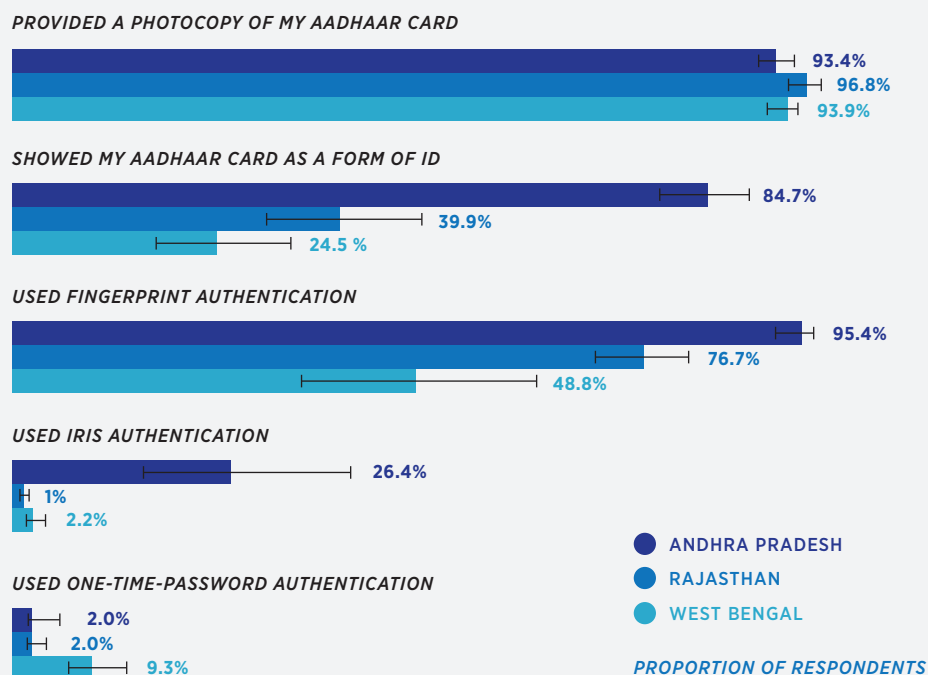
Note: Error bars denote 95% confidence intervals

Number of observations: AP (1,140); RJ (950); WB (826)

Data sources: State of Aadhaar Survey 2017-18

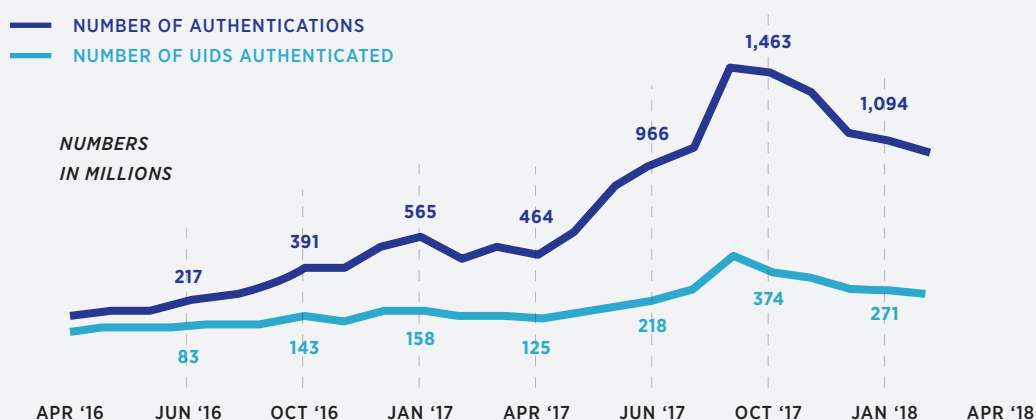
7. The Aadhaar letter – sometimes referred to as an "Aadhaar card" – is issued by the UIDAI. The letter contains one's Aadhaar number, demographic details, and photograph. Throughout this report we refer to the letter as an "analog" or "non-digital" ID to differentiate between the biometrically-enabled aspects of the ID.

Figure 2.5: Different uses of Aadhaar by residents



Note: Error bars denote 95% confidence intervals
 Number of observations: AP (1,142); RJ (952); WB (825)
 Data source: State of Aadhaar Survey 2017-18

Figure 2.6: Aadhaar authentication and unique residents authenticated over time, Apr 2016 – Feb 2018



Data source: UIDAI Dashboard

Awareness

In our survey we asked a series of questions about awareness to understand which features and functionalities people understood regarding Aadhaar.

See Figure 2.7 for an assessment of awareness levels for the three states in our survey. The UIDAI has set up regulations and systems to improve access and also safeguard its end users. However, lack of user awareness has limited the impact of these steps.



EVOLVING FEATURES OF AADHAAR

To try and address growing concerns about privacy and data security, the UIDAI recently launched three features: Virtual ID, Limited KYC, and UID token.

Virtual ID (VID) is a temporary 16-digit random number that can be generated by residents against their Aadhaar numbers. VID, along with one's biometrics, can be used to authenticate oneself. The introduction of VID tackles privacy concerns in two ways. One, it prevents agencies from linking databases using Aadhaar's unique identifier since each agency will only have access to the temporary VID. Two, it allows an individual to have a choice about when (and with whom) they share their Aadhaar number.

Limited Know-Your-Customer (KYC) is being introduced to regulate the storing of Aadhaar numbers in different databases. As per the UIDAI's notification, the authority plans to allow only authentication agencies that are required by law to receive full demographic information along with the Aadhaar number of an individual. The remaining agencies will be subject to Limited KYC and will not be allowed to store Aadhaar numbers upon authentication.

To facilitate uniqueness and security of beneficiaries in the authentication agencies' databases, the UIDAI aims to introduce a system called UID Token. With this system, each individual Aadhaar number is given a unique token ID for an authentication agency. That token is used for each transaction with that agency, but not used anywhere beyond that agency (UIDAI 2018). This too prevents different agencies from linking databases as each agency has a unique token for an individual that cannot be mapped to the token of that individual from another database.

Efforts to advance and evolve security features to better protect residents should be encouraged. However, given low levels of awareness of other security features such as biometric locking, simply offering these features is unlikely to result in sufficient uptake (see Figure 2.7). The government should engage in thoughtful campaigns, targeted toward individual users and institutions requiring Aadhaar for identification to ensure the objectives of these initiatives are met. Finally, these measures, and the processes accompanying them, need careful and rapid testing to ensure they are optimised to provide a seamless and effective layer of protection.

Figure 2.7: Proportion of Aadhaar awareness levels among survey respondents

CATEGORY	ISSUE	AP	RJ	WB	ALL 3 STATES
Authentication Awareness	Awareness of fingerprint authentication	97.8	87.6	71.5	85.1
	Awareness of iris authentication	45.7	15.4	30.8	31.0
	Awareness of OTP authentication	6.1	10.0	13.9	10.1
	Awareness of all three	5.8	7.2	8.7	7.2
UIDAI Regulations	Enrolment is free of cost	40.2	41.0	43.3	41.6
	Updating should cost only ₹15	4.8	11.8	8.0	7.3
Security Features	Aware of biometric locking & unlocking	2.0	3.4	3.9	3.1

Note: The fee charged for updates was ₹15 but has recently been increased to ₹25

Number of observations: The number of observations reported above varies by question and by state. Most questions were asked to all respondents who have an Aadhaar, with variation arising from the removal of “don't know” responses. However, the question on cost of updating was only asked to a relevant subset (275). See the technical appendix on www.StateofAadhaar.in for more details.

Data source: State of Aadhaar Survey 2017-18

AADHAAR DATA QUALITY AND UPDATING DATA

While saturation levels are important, it is equally imperative to ensure that the information collected is accurate. Low data quality would lead to errors in seeding and a less reliable e-KYC process. Through our survey, we wanted to gain a better understanding of the quality of the demographic data captured through Aadhaar. To understand this vital component of Aadhaar, we examined several related indicators, such as the proportion of respondents that self-reported an error in their Aadhaar data, the frequency of updating (due to errors or a need to update information), and the proportion of duplicates in the system. We also wanted to understand people's experience with the updating process.

Data quality

At the peak of the enrolment process, the UIDAI was facilitating enrolment of nearly one million people a day (*State of Aadhaar Report 2016-17*). This raises the question about whether the scale of the enrolment made the exercise vulnerable to data entry errors. When asked, 8.8 percent of people stated that their Aadhaar letter contained an error. The errors are self-reported and there is reason to believe these are a lower-bound estimate for errors.⁸

To interpret the errors compared with the most widely used alternative, we also asked if respondents had errors in their voter ID cards. We see that in Andhra Pradesh and Rajasthan the proportion of respondents with errors in Aadhaar are more than three times and nearly two times higher than for voter IDs, respectively, while in West Bengal the Aadhaar error rate is higher, though the difference is not as extreme (see Figure 2.8).

We also wanted to identify which types of information are most error-prone. The most common source of error in Andhra Pradesh and West Bengal was the name of the respondent, while in Rajasthan date of birth contained the highest number of self-reported errors (see Figure 2.9). The magnitude of error(s) also matters in terms of how the error affects people. Of those who reported an error in their name, about one-third claimed their full name was wrong while two-thirds noted an incorrect spelling. We also asked respondents about the perceived source of the error. Eighty-nine percent reported their error(s) was due to data entry mistakes while 10.3 percent stated a pre-existing error in a source document. The remaining errors were attributed to mistakes made by the respondents themselves.

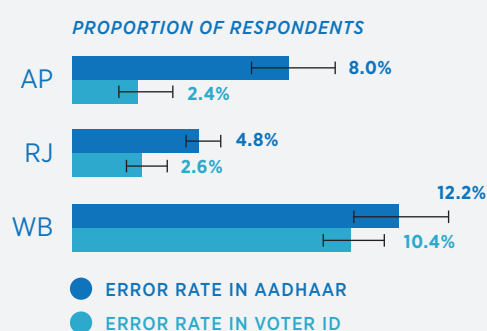
The UIDAI has established processes for the correction of errors in Aadhaar. Most who tried to get their error rectified claimed to be successful. However, only 53.0 percent of those with errors actually reported trying to get the error corrected. An important concern that emerges from the data on the enrolment process is that of the

8. We believe self-reported errors will be lower than externally verified errors. This assumes that respondents are more likely to report an error that has affected their ability to use their Aadhaar or access services, and less likely to report an error if it does not impede any uses. For example, a name may be misspelled or wrongly transliterated from another language into English, but a respondent would likely only report the error if it has led to service denials or other issues. Additionally, respondents who are not literate might not be able to tell if some information is incorrect.

respondents who paid to get the error fixed (82.4 percent), 96.0 percent reported paying more than the designated fee of ₹25.⁹

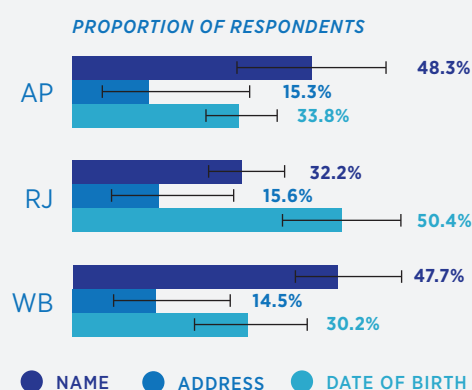
In contrast to the high number of respondents reporting ease in the enrolment process, the proportion is lower for the correction of errors. In Andhra Pradesh and Rajasthan 69.1 percent and 67.0 percent, respectively, stated that they found the process “easy.”¹⁰ In West Bengal, 47.8 percent of those who attempted to fix errors felt the process was “easy.” This indicates that there are challenges or barriers in this process that should be addressed to improve the user experience and to ensure the accuracy of the Aadhaar data.

Figure 2.8: Comparison of errors in Aadhaar and voter ID



Note: Error bars denote 95% confidence intervals
Number of observations (Aadhaar): AP (4,275); RJ (4,669); WB (3,435)
Number of observations (voter ID): AP (2,999); RJ (2,934); WB (2,611)
Data source: State of Aadhaar Survey 2017-18

Figure 2.9: Types of error on Aadhaar letters with a demographic error



Note: Error bars denote 95% confidence intervals
Number of observations: AP (333); RJ (223); WB (410)
Data source: State of Aadhaar Survey 2017-18

Updating data

Updating Aadhaar data will become essential to ensuring accuracy of the information. This primarily involves updating contact details, photographs, and biometric information of children once they turn five and again at age fifteen, per the UIDAI requirements. Some updates are required on an ad hoc basis (updating one's address after a move) while some updates are cyclical (updating one's photo every ten years). The proportion of people that updated their data in cases where their address had changed was low (13.0 percent) amongst the three states. The proportion was higher (25.5 percent) in the case of updating mobile phones numbers.

DISCUSSION

As noted above, people were generally satisfied with the Aadhaar enrolment process. However, they faced greater challenges when fixing mistakes or updating information. Updates will be required as long as the system is in place. Consequently, the UIDAI should examine the successes of the enrolment system and think critically about how to improve the updating process.

As the administrator of the world's largest biometric database, the UIDAI will face significant challenges ensuring Aadhaar data remains current and updated. A system containing errors is likely to cause problems, ranging from minor inconveniences to serious threats of exclusion.

Similarly, some uses of Aadhaar authentication remain low, particularly OTP and iris authentication. Given fairly high rates of mobile penetration, it may be worthwhile for the UIDAI to invest in awareness campaigns aimed at the ease of OTP authentication. This could also provide relief for individuals who struggle to authenticate using their biometrics. Additionally, the overwhelmingly high use of Aadhaar in its analog form necessitates a greater focus on adding security features to the physical copy of Aadhaar as well. As Aadhaar's use as an identity platform continues to increase, it is vital for the underlying quality of its database to improve, along with well-established processes to continuously stay up to date. Having achieved exemplary scale, a renewed focus toward quality and updating processes may be important next steps for the UIDAI.

9. The fee charged for updates was ₹15 but has recently been increased to ₹25.

10. The number of respondents who answered this question was less than fifty in Andhra Pradesh and Rajasthan.

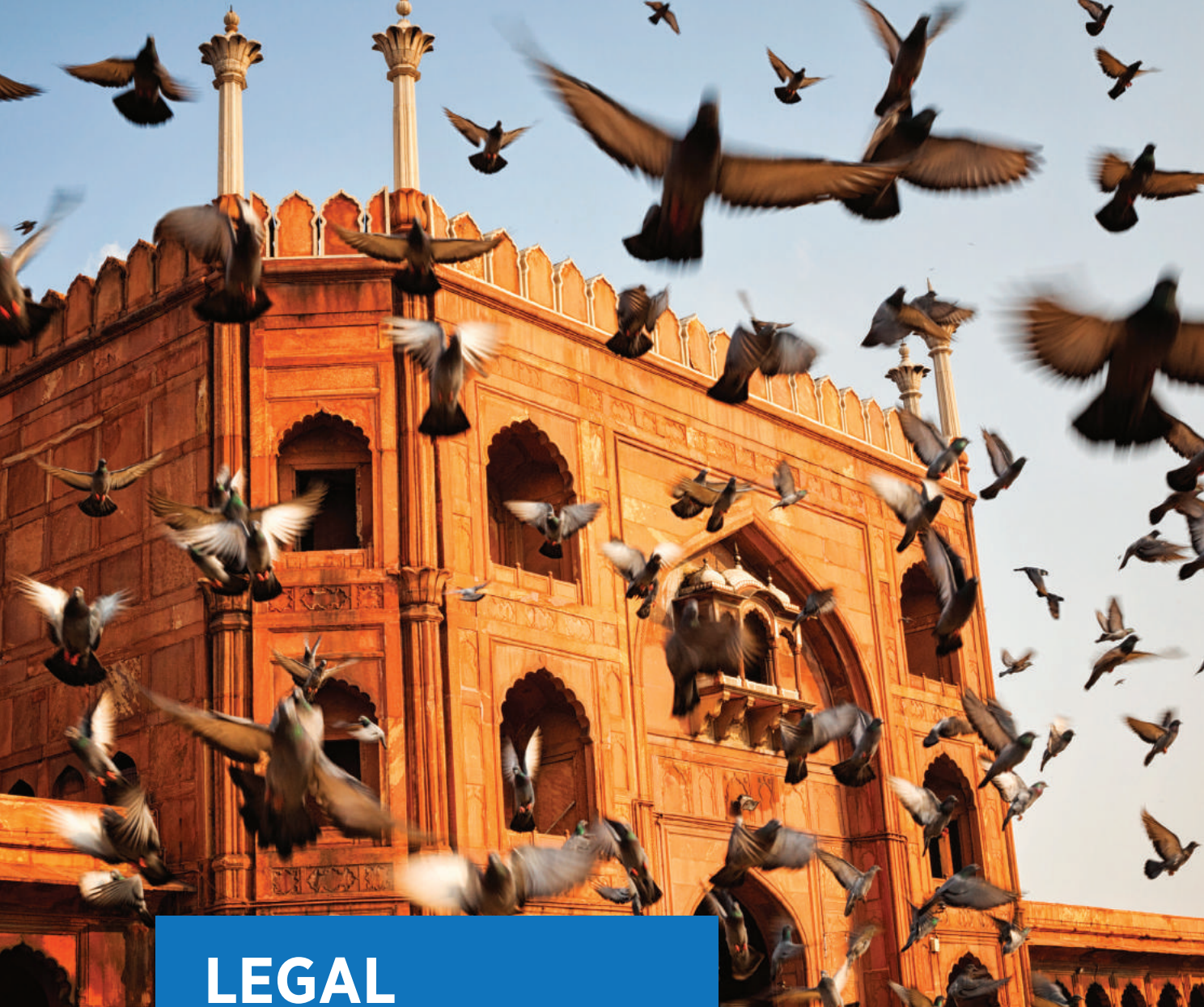
DUPLICATE AADHAAR "CARDS"

One of the strongest arguments in favour of Aadhaar is the ability to create a database free of duplicate entries. The unique 12-digit number combined with individuals' unique biometric information is meant to create a system in which each individual is only entered once.

Our survey data suggests this is mostly true; however, we found three cases in which individuals possessed two Aadhaar letters—containing matching name and demographics but with a distinct unique ID number. At 0.1 percent of our sample, this represents a small but meaningful number.¹¹

Based on UIDAI's performance data, the false acceptance rate was expected to be 0.035 percent (*State of Aadhaar Report 2016-17*). However, given different estimation methods and the low incidence in our sample, we cannot strictly compare these two statistics.

11. A direct extrapolation of this number would be equivalent to 71,300 duplicates across the rural population of all three states. The 95 percent confidence interval around this estimate ranges from 3 to 213,900, meaning there is a wide variance on our estimate for how many duplicates may exist. However, we may want to think of this number as a lower-bound considering that anyone who intentionally obtained a second Aadhaar (for nefarious purposes) would likely not have shared this information with our survey team. Note that we confirmed that these were indeed duplicate Aadhaars and not the respondent mistaking their temporary enrollment ID to an Aadhaar number.



LEGAL

As we write this report, a five-judge constitution bench of the Supreme Court of India is hearing 30 petitions challenging the legality of Aadhaar. The Court is expected to answer foundational questions about the digital identify platform. Is the 2016 Aadhaar Act, passed as a Money Bill, constitutional? Is Aadhaar's use of biometrics in conformity with our newly codified right to privacy? Are the burdens borne by Indian residents due to the use of Aadhaar justified by the potential gains?

In answering these questions, the Supreme Court can play a crucial role in shaping our institutions and ability to manage risks in a fast-paced digital world. In August 2017, its landmark judgement on the right to privacy served as confirmation of this role. In addition, the Government of

India has also set in motion a consultative process regarding the framing of a much-needed data protection law (Ministry of Electronics and Information Technology [MeitY] 2017).

In this chapter, we provide a brief overview of these legal developments in the Aadhaar ecosystem over the last year. We do not discuss the current set of petitions being heard in the Supreme Court as the matter has not concluded at the time of sending this report to print.

RIGHT TO PRIVACY JUDGEMENT

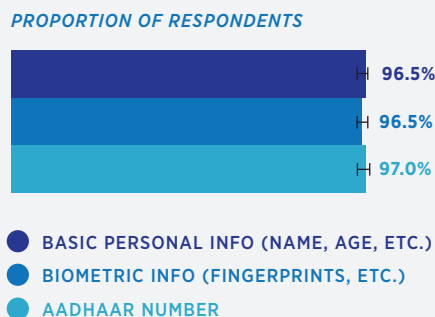
A nine-judge bench of the Supreme Court of India passed a landmark judgement recognizing our fundamental right to privacy as emanating from Article 21 (right to life and personal liberty) and other rights guaranteed under Part III of India's Constitution. The judgement came in light of a series of individual petitions linked to Aadhaar combined with the writ petition filed by retired High Court Justice K.S. Puttaswamy challenging various aspects of the Aadhaar project, especially its potential violations of individual privacy.

Whether India's constitution allows a right to privacy remained unsettled before this judgement. While there were two- or three-judge benches that ruled that it was a right (Gobind vs State of Madhya Pradesh 1975; Malak Singh 1980), the Union of India argued against a blanket right to privacy, citing larger Supreme Court benches (M P Sharma 1954; Kharak Singh 1962).

Privacy was deemed an undeveloped and elitist concept in the proceedings (Justice K S Puttaswamy (Retd.) and Anr versus Union of India and Ors 2017). Findings from the SOA survey do not support this view. To a question asking SOA survey respondents whether they consider it important (or not) to know how the government uses their information, more than 96 percent of respondents in the three surveyed states contended that it was indeed important, for all three types of information shown in Figure 3.1. These findings are in line with qualitative interviews conducted with low-income individuals in a collaborative effort between Dalberg, CGAP, and Dvara Research. One of their key insights was that respondents were "highly protective" of their personal information, including their Aadhaar numbers (Privacy on the Line 2017).

The dimensions of privacy discussed in the judgement include an individual's right to seclusion, autonomy over fundamental personal choices, and the right to control dissemination of personal information. Similar to other fundamental rights, the judgement maintained that the right to privacy can be subject to reasonable restrictions where such an invasion must be justified by law and a legitimate state aim, including preserving scarce resources.

Figure 3.1: Importance of knowing how the government uses respondents' data (All three states: AP, RJ, WB)



Note: Error bars denote 95% confidence intervals
 Number of observations (for basic personal information): AP (1,135); RJ (939); WB (836)
 Number of observations (for biometric information): AP (1,137); RJ (932); WB (829)
 Number of observations (for Aadhaar number): AP (1,129); RJ (924); WB (820)
 Data source: State of Aadhaar Survey 2017-18

MANDATORY LINKING OF AADHAAR TO SERVICES

Using Section 7 of the Aadhaar Act 2016, central and state governments have required beneficiaries of 252 schemes (as of December 2017) to authenticate themselves using Aadhaar (Rajya Sabha Question 2018).

One of these uses, put forward by the Department of Telecommunications in March 2016, asks for Aadhaar-based verification of all existing mobile phone subscribers.¹² Similarly, an order in June 2017 by the Supreme Court upheld a move allowing the linking of Aadhaar to each individual's PAN (Binoy Viswam versus Union of India & Ors 2017).

We asked respondents in the SOA survey whether they approved or disapproved of the decision to mandatorily link Aadhaar to services offered by the government and the private sector. Approximately 87 percent of people approved of the government's mandatory use of Aadhaar, while 76.9 percent approved Aadhaar's mandatory use by the private sector. See Figure 3.2.

12. The Supreme Court order that led to this notification, however, was more tentative in language on what types of mobile subscribers should be covered and whether Aadhaar should be used exclusively in the verification process (State of Aadhaar Blog 2017).

DATA PROTECTION LAW

With an ever-growing digital economy and the right to privacy judgement, discussion about the need for a data protection law intensified this past year. The MeitY constituted an expert committee led by Justice B.N. Srikrishna to identify data protection issues in India and draft a bill addressing these concerns. The committee released a white paper in November 2017 to seek public views to define the contours of a data protection law in India. The paper outlines seven principles for data protection in India—technology agnosticism, holistic application, informed consent, data minimisation, controller accountability, structured enforcement, and deterrent penalties (MeitY 2017). It draws on existing international laws—such as the European Union’s General Data Protection Regulation (2016) as well as South Africa’s Protection of Personal Information Act (2013)—and raises questions on subject matters ranging from potential definition of different types of data, the territorial scope, extent of exemptions, existence of a data protection authority, and the model of regulatory approach that must be adopted.

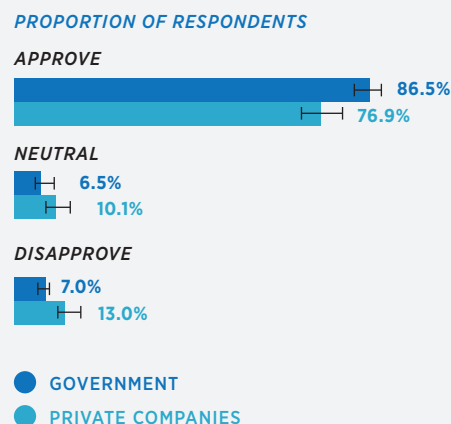
DISCUSSION

The Supreme Court judgement on privacy, the mandatory linking of services, and the forthcoming data protection law all pivot around the central question of whether and how Aadhaar can be a tool for infringement of privacy.

We believe that Aadhaar, if unregulated, can be a tool that erodes our fundamental right to privacy. However, it is only a tool and other public and private digital platforms are also capable of invading our privacy. Therefore, as we do with any tool in the public domain, we need to take advantage of its benefits while managing its risks.

More fundamentally, the threat of privacy infringement highlights the need for a strong data protection law backed by an independent, competent, and fully authorised data protection regulator to enforce it. Currently, UIDAI acts as both a data controller of Aadhaar demographic and biometric information and regulator to ensure the appropriate use of that information. This can be ineffective given the dual purpose for a single

Figure 3.2: Approval ratings on mandatory linking of Aadhaar to services, by entity type (All three states: Andhra Pradesh, Rajasthan, West Bengal)



Note: Error bars denote 95% confidence intervals
 Number of observations (for government services): AP (1,136); RJ (945); WB (828)
 Number of observations (for private services): AP (1,103); RJ (935); WB (823)
 Data source: State of Aadhaar Survey 2017-18

organisation, raises potential conflicts, and is not ideal given the complexity of regulatory requirements.

With the past and forthcoming Supreme Court judgements and the establishment of the Srikrishna Committee to actively look into data protection, the government has the opportunity to institute a strong data protection law and regulator to manage risks posed by Aadhaar and other digital tools, an opportunity we hope it seizes.

AADHAAR DATA DISCLOSURE

While there has been no unauthorised data disclosure of enrolment data within the UIDAI's Central Identities Data Repository, Aadhaar numbers and demographic details have been disclosed on other public portals.

A report released by the Centre for Internet and Society reported that Aadhaar numbers and demographic details of 135 million residents were disclosed on four government portals due to lack of stringent IT measures (Sinha and Kodali 2017). The MeitY further reported that, as per the UIDAI, 210 government websites had revealed details of Aadhaar and other personal data (Lok Sabha Question 2018).

Name, address, bank account details, and Aadhaar numbers of more than a million beneficiaries of an old age pension scheme in Jharkhand were published on a website maintained by the Jharkhand Directorate of Social Security in July 2017 (Sethi, Bansal, and Saurav 2017).

A journalist for the Tribune reported a data breach in which she was able to buy access to a UIDAI portal. With this access, one could enter a person's Aadhaar number and obtain personal demographic data (Khaira 2018).



FINANCIAL INCLUSION

Access to formal financial services is pivotal to the economic progress and development of the poor and their communities (Cull, Ehrbeck, and Holle 2014). While banking access has increased rapidly over the past few years, 20 percent of Indian adults continue to be excluded from the formal financial system.¹³ According to a recent study by the World Bank, India's unbanked population is 190 million, accounting for more than 10 percent of the global unbanked population (Demirgüç-Kunt et al 2018).

Over the last year, the Government of India has continued its focus on financial inclusion through programmes such as Pradhan Mantri Jan Dhan Yojana (PMJDY or "Jan Dhan").¹⁴ As of March 2018, 313 million bank accounts have been opened through Jan Dhan (PMJDY 2018). However, nearly 40 percent of bank account owners have not made a deposit or withdrawal in the past twelve months (Demirgüç-Kunt et al 2018).

As discussed in the *State of Aadhaar Report 2016-17*, the government contends Aadhaar can play an important role in financial inclusion, both in the initial stage of opening a bank account and then in facilitating the active usage of the account. Until recently there was insufficient data to

examine these claims. While data gaps remain, we use the State of Aadhaar survey from rural Andhra Pradesh, Rajasthan, and West Bengal, along with other recent research and administrative data to begin to understand the role of Aadhaar in promoting financial inclusion.

To this end, we seek to answer the following two questions in this section:

1. Has Aadhaar aided unbanked individuals (or households) in opening a bank account? If so, to what extent?
2. Has Aadhaar made bank accounts easier to use — and thus does it result in fewer dormant (or inactive) accounts

In the next two subsections, we discuss our findings related to the above questions. This is followed by a discussion on the implications of the findings for expanding financial inclusion within India.

¹³. According to the World Bank's Global Findex, in 2011, 35.2 percent of Indian adults had access to a financial institution account. In 2014, that number grew to 52.8 percent; in 2017 it was 79.8 percent.

¹⁴. The goal of PMJDY, launched in April 2014, is to ensure every household in India possesses a bank account.

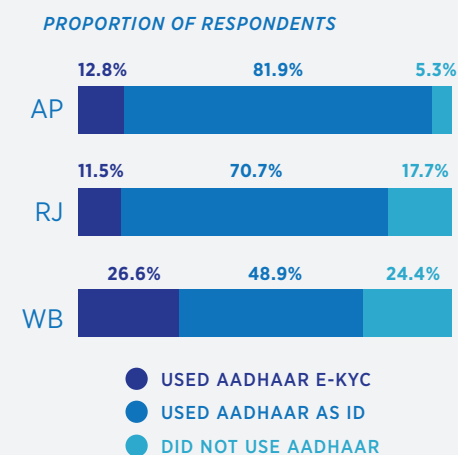
OPENING A BANK ACCOUNT

The promise of Aadhaar in enabling the opening of a bank account is two-fold: first, it can serve as a legitimate identity document and second it can be used to verify a customer's identity and securely share her or his demographic details via Aadhaar-enabled e-KYC.

Use of Aadhaar as an identity document

Starting in July 2013, the Reserve Bank of India (RBI) allowed the use of Aadhaar as a means of identification to open a bank account (Sahoo 2013).¹⁵ According to our survey data, among those who opened a bank account in the last three years, a large majority of respondents used Aadhaar as an analog identity document in Andhra Pradesh (81.9 percent) and Rajasthan (70.7 percent) and nearly half in West Bengal (48.9 percent) (see Figure 4.1). However, the extent to which having an Aadhaar exclusively enabled these respondents to open a bank account – compared to the counterfactual of not having an

Figure 4.1: Proportion of respondents who used Aadhaar for bank account openings, since 2014



Number of observations: AP (479); RJ (431); WB (350)
Data source: State of Aadhaar Survey 2017-18

Aadhaar – is unknown. We estimate that nearly 90 percent of the respondents who used Aadhaar as an identification document to open a bank account also had another legitimate proof-of-identity document before securing an Aadhaar.¹⁶ Almost all also had a legitimate proof of address (see Figure 4.2).¹⁷ That being said, the high usage of Aadhaar as an identity document for opening an account demonstrates the benefits of having a universal ID – one document that can serve as proof of identity and address and that is widely recognized by both customers and service-providers.

Use of Aadhaar e-KYC

As previously noted, Aadhaar can also facilitate the opening of a bank account through e-KYC. Usage of e-KYC

Figure 4.2: Proportion of respondents who possessed other IDs among those who “Used Aadhaar as ID” to open an account, since 2014

PROPORTION OF RESPONDENTS

PROOF OF IDENTITY



PROOF OF ADDRESS



● ANDHRA PRADESH
● RAJASTHAN
● WEST BENGAL

Note 1: We gathered data on the IDs respondents possessed when they applied for an Aadhaar. In this analysis, legitimate proofs-of-identity document for bank accounts include: NREGA job card, voter ID, driving license, PAN card, letter from an official government authority/panchayat, and passport. Legitimate proofs-of-address document for bank accounts include: ration card, an existing bank statement, and letter from official government authority/panchayat.

Note 2: Error bars denote 95% confidence intervals
Number of observations: AP (400); RJ (293); WB (171)
Data source: State of Aadhaar Survey 2017-18

15. As previously noted, the Aadhaar letter is issued by the UIDAI. The letter includes the name, address, and photograph of a customer, as required by the know-your-customer (KYC) rules established by the Reserve Bank of India (RBI).

16. The RBI defines a legitimate proof-of-identity document for bank accounts as: passport, PAN card, voter ID, driving license, NREGA job card, Aadhaar letter issued by the UIDAI, an identity card of the bank's satisfaction, and letter from an official government authority / panchayat. In our analysis, legitimate proofs-of-identity document (not including the Aadhaar letter) for bank accounts include: NREGA job card, voter ID, driving license, PAN card, letter from an official government authority / panchayat, and passport.

17. A legitimate proof-of-address document for bank accounts includes: telephone bill, bank account statement, letter from an official government authority / panchayat, electricity bill, ration card, letter from employer deemed satisfactory by the bank, and rent agreement registered with a recognized authority. In our analysis, legitimate proofs of address (not including the Aadhaar letter) include: ration card, an existing bank statement, and letter from official government authority / panchayat.

Figure 4.3: Monthly number of successful Aadhaar e-KYC verifications as per NPCI, Apr 2016 – Feb 2018

Note 1: Note: FY 2017-18 data does not include March 2018

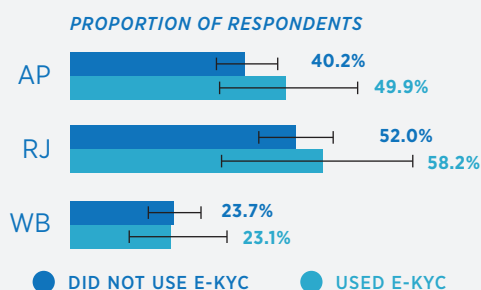
Note 2: E-KYC verifications data is released by the NPCI. Data points may be for opening new bank accounts and for other financial services products as well. The data is only pertaining to the usage of e-KYC for financial transactions and is representative of financial entities that are registered with the NPCI to offer e-KYC services.

Data source: National Payments Corporation of India

to open financial accounts increased significantly over the last year compared with the previous year (NPCI 2018). As seen in Figure 4.3, the number of successful e-KYC verifications has nearly tripled in FY 2017-18 compared with FY 2016-17.¹⁸ As for the prevalence of e-KYC in the opening of bank accounts in rural settings, our data suggests uptake is fairly low. According to our survey results, for those who opened an account in the last three years, e-KYC usage was 12.8 percent and 11.5 percent in Andhra Pradesh and Rajasthan, respectively. Uptake was higher in West Bengal, with 26.7 percent of accounts opened within the last three years using e-KYC. These results can also be seen in Figure 4.1. The gap between the proportion of people who used Aadhaar as a means of

identification and those who used e-KYC may be explained in part by the lack of a differentiation factor of e-KYC in the opening of bank accounts. In our survey data, using Aadhaar e-KYC is not correlated with a higher likelihood of accessing one's bank account within one day of opening. Thus, we have no evidence that e-KYC expedited the process of opening an account, which is contrary to the stated benefits. This held true for all three states (see Figure 4.4).

USING A BANK ACCOUNT

Figure 4.4: Proportion of respondents who got access to account within 1 day among those who used e-KYC and those who did not

Note: Error bars denote 95% confidence intervals

Number of observations (did not use e-KYC): AP (409);

RJ (341); WB (240)

Number of observations (used e-KYC): AP (55);

RJ (53); WB (95)

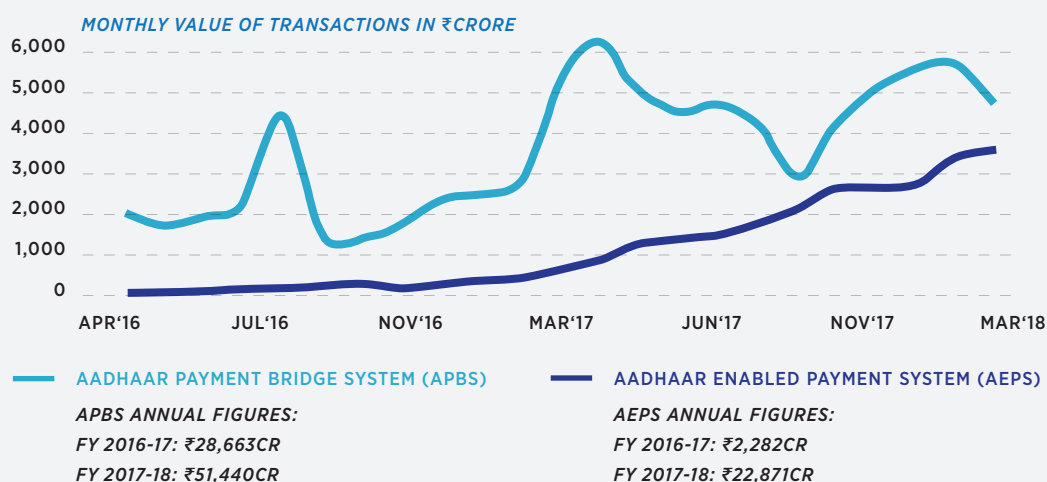
Data source: State of Aadhaar Survey 2017-18

To experience the full benefits of the formal financial sector, individuals must have ready access to their bank accounts, as well as a full understanding of their utility. Said in another way, customers need reasons to keep using their accounts. According to our data, more than 90 percent of respondents in Andhra Pradesh and Rajasthan and nearly 80 percent in West Bengal had access to a bank account. Despite growing access to bank accounts among Indian adults, we found only a subset of accounts are actively in use: 66.6 percent in Andhra Pradesh, 58.1 percent in West Bengal, and 44.9 percent in Rajasthan. The next major challenge in financial inclusion is active participation in the financial ecosystem. There are two ways in which Aadhaar may help to facilitate increased usage of bank accounts: first, Aadhaar serves as the foundational layer for use of microATMs through the Aadhaar Enabled Payment System (AEPS) and second, direct benefit transfers (DBTs) can be paid using an Aadhaar-based infrastructure known as Aadhaar Payment Bridge System (APBS).¹⁹

18. This figure also includes the use of e-KYC by non-bank financial entities and payments banks, such as mobile wallet companies.

19. To read more about these systems and how they work, please read the financial inclusion chapter of the *State of Aadhaar Report 2016-17*.

Figure 4.5: Monthly transactions of AEPS and APBS, Apr 2016 – Feb 2018



Note 1: FY 2017-18 data does not include March 2018

Note 2: APBS is an Aadhaar-based payment system that facilitates government subsidies and benefits, such as direct benefit transfers (DBTs).

AEPS is an Aadhaar-based payment system that facilitates the use of microATMs.

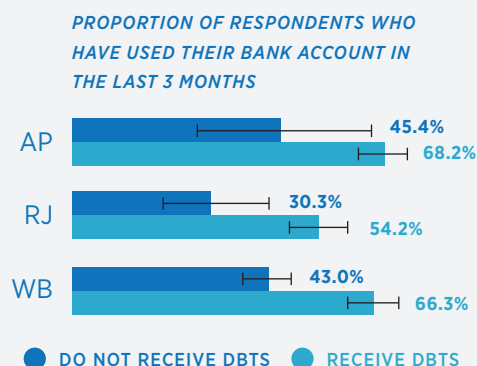
Data source: National Payments Corporation of India

Use of microATMs

According to research by InterMedia, fewer than half of all adults in India know of a microATM within a kilometer of their home (2017). Aadhaar-enabled microATMs, portable devices equipped to authenticate biometrics and generally accessed through business correspondents (BCs), can offer financial services to individuals who do not live close to a brick-and-mortar bank. These microATMs can help lower barriers to accessing a bank account and thus lead to more active usage. Data from NPCI demonstrates an almost tenfold increase in the value of transactions conducted using AEPS, which includes microATM transactions, in FY 2017-18 compared with the previous year (see Figure 4.5).²⁰ The average size of a transaction has also grown significantly—from ₹1,400 (\$22) a month in FY 2016-17 to ₹2,527 (\$39) a month in FY 2017-18 (NPCI 2018).²¹

In addition, the number of BCs in rural areas has been slowly increasing, with the total number growing by 2 percent between 2016 and 2017 (from 531,229 to 543,472) (RBI 2017). About half of the BCs (53 percent) use microATMs to conduct transactions (Mehrotra et al. 2018). Although transactions and the number of BCs have been increasing, our data indicates that utilization rates are still low in the three states where we conducted our survey.

Figure 4.6: Proportion of respondents who used their bank accounts by whether they receive DBTs or not



Note: Error bars denote 95% confidence intervals

Number of observations (no DBT): AP (74); RJ (319); WB (221)

Number of observations (DBT): AP (964); RJ (547); WB (433)

Data source: State of Aadhaar Survey 2017-18

In Andhra Pradesh, 33.4 percent of respondents who used their bank account in the last three months reported having used a microATM. In West Bengal and Rajasthan, it was 14.7 percent and 5.1 percent, respectively.

²⁰ AEPS allows for biometric authentication of transactions by individual users; microATMs use AEPS to facilitate transactions such as withdrawals, deposits, and mini-statements. APBS allows government agencies to transfer funds to citizens using only their Aadhaar number and bank name. This system is used in government subsidy and social protection programmes.

²¹ The figure for FY 2017-18 does not include data from March 2018.

Low usage levels may be rooted in implementation gaps rather than the design of the microATM platform. Our data implies that microATMs offer a better user experience compared with banks. Of those who used microATMs in the last three months, 78.4 percent in Andhra Pradesh and 81.6 percent in West Bengal reported that using them is easier than transacting at a bank.^{22,23} Respondents in both states cited shorter distances, decreased lines, and speed of transactions.

However, a recent study by MicroSave highlighted issues that may be leading many to continue to transact at a bank. Sixty-five percent of BCs who carry a microATM experienced service downtimes in the previous month, which was higher than those who do not use a microATM (50 percent). In addition, uncertainty of a successful transaction with a BC was higher. An overwhelming majority of BCs (94 percent) currently do not offer services to customers of other banks (i.e., those who do not have an account with the specific bank employing the BC); 76 percent reported having faced problems in maintaining liquidity (Mehrotra et al. 2018). If the usage of BCs and microATMs is to be encouraged, reliability of the branchless network must improve.

Aadhaar seeding and direct benefit transfers

The mandatory seeding of Aadhaar to bank accounts has been widely discussed over the past year. Before the recent regulatory push for seeding of bank accounts, it was originally introduced to route government-to-citizen direct benefit transfers (DBTs) through APBS (NPCI n.d.). The benefits of APBS in disbursing DBTs compared with other electronic payment mechanisms, such as National Electronics Funds Transfer System (NEFT), are unclear. However, the DBT Mission has indicated that it seeks to maximize DBT payments made via APBS (DBT Mission 2016). As seen in Figure 4.5, the value of transactions made over APBS has almost doubled in FY 2017-18 compared with a year ago (NPCI 2018).

Research suggests that receiving DBTs into one's bank account can increase account usage; not having a bank balance is a key contributor to account dormancy (Demirgüç-Kunt et al. 2015). Our survey data suggests a possible relationship between receiving DBTs and active account usage. We find that the likelihood of active usage of one's bank account is significantly higher among those who receive DBTs (see Figure 4.6).

DISCUSSION

The Government of India — in particular RBI, NPCI, and the UIDAI — have laid strong foundations for the integration of Aadhaar into the financial ecosystem. A major part of this foundation focuses on the digital aspects of the Aadhaar infrastructure. However, we find that in the rural areas of our three surveyed states, Aadhaar's digital usage for financial inclusion (e-KYC) has had a limited reach, while its analog version (the letter) has been an enabler of inclusion, particularly in opening bank accounts. Nevertheless, the possession of an Aadhaar number could play a larger role in promoting the continued usage of accounts. According to our data, microATMs may offer a better experience than banks and could potentially enhance the reach of formal financial services. For this to materialise, however, implementation issues regarding BC networks discussed above will need to be addressed.

In addition to strengthening BCs, another Aadhaar-related channel for improving access to accounts is mobile payment systems, such as mobile money accounts. Mobile-based systems can leverage Aadhaar for payer authentication (though they do not need to exclusively use Aadhaar). Research from the World Bank estimates that only 2 percent of Indian adults have a mobile money account. However, that same survey claims that 100 million unbanked adults in India own a mobile phone (Demirgüç-Kunt et al 2018). Identifying ways for the public or private sector to make mobile money accounts and payment systems more prevalent in rural areas could be an important step in expanding financial inclusion.

Similarly, given that receiving DBTs is correlated with active bank account usage, the role of DBTs in financial inclusion requires more consideration. Insofar as it is the government's aim to maximize DBT payments over APBS, possession of Aadhaar and Aadhaar-seeded bank accounts could be policy tools to encourage bank account usage. We recommend further research to analyse any causal impacts DBTs have on account usage, and the role of Aadhaar and Aadhaar-seeded bank accounts. The initial evidence suggests additional efforts may be needed to fully realize Aadhaar's potential for financial inclusion, especially the digital aspects of the identity platform. Designing and implementing these efforts require tailored and rigorously tested solutions that build on the existing foundations. Doing so could help mainstream millions of India's unbanked or underbanked poor and empower them to augment their savings and financial stability.

22. For those who used a microATM to withdraw NREGA wages, the time frame for this question on microATM usage was defined as a five-month period (from March to June 2017) as opposed to the "last 3 months."

23. We do not present results from Rajasthan, as the number of respondents who answered this question was too low.



SOCIAL PROTECTION: FOOD RATION

India's social protection programmes are an essential lifeline for its poor. However, these programmes – providing subsidised food, employment guarantees, pensions, and other benefits – suffer from significant leakages (Economic Survey 2016-17).²⁴

While digitisation, near-universalisation of food subsidies, and other reforms are improving this status quo (World Bank 2017), the Government of India envisions the use of Aadhaar as a key reform to improve social protection delivery. It posits that Aadhaar can remove duplicate and fake beneficiaries from programme muster rolls and prevent fraudulent transactions.²⁵

To this end, the use of Aadhaar in India's social protection programmes is steadily increasing.

Aadhaar seeding of beneficiaries in India's major social protection programmes increased over the last financial year.²⁶ See Figure 5.1. During the same period, of the half-million fair price shops in India, the proportion using electronic point-of-sale (e-PoS) devices, primarily used to facilitate Aadhaar-based biometric authentication (ABBA),

increased from 35 to 57 percent.²⁷ See Figure 5.2 for the 2017 and 2018 state-wise distribution.

While Aadhaar seeding and authentication for social protection programmes are rising, various reports emerged this year of these processes leading to denial of benefits to genuine beneficiaries, combined with other inconveniences (Khera 2017).

Therefore, the main issue that emerges is whether the scale-up of Aadhaar as an identity platform for India's social protection is justified. Until recently, there was insufficient data to answer this question. While data gaps remain, we use the SOA survey, along with other recent research and administrative data to begin providing answers. Given data availability, we will focus largely on the Public Distribution System (PDS), a food subsidy scheme and India's largest social protection programme. In addition, much of the discussion will revolve around Andhra Pradesh and Rajasthan, two states that have scaled up the use of ABBA for PDS.²⁸ West Bengal only uses Aadhaar for seeding purposes.

²⁴. "Leakages" refers to the fact that the full proportion of benefits do not reach genuine beneficiaries and instead "leak" out of the system due to corruption and other inefficiencies.

²⁵. Please read the Social Protection chapter of the *State of Aadhaar Report 2016-17* for an overview of these impact channels.

²⁶. Aadhaar seeding refers to linking names of beneficiaries to their Aadhaar details in programme muster rolls. This helps maintain programme databases to be free of fake and duplicate entries.

²⁷. Fair price shops are the delivery point for food subsidies from the Public Distribution System.

²⁸. Twenty-seven states and Union Territories use e-PoS devices for PDS delivery, many of which are Aadhaar-enabled.

Figure 5.1: Proportion of beneficiaries seeded in India's major social protection programmes*PROPORTION OF BENEFICIARIES***LPG (PAHAL)****MGNREGS****NSAP****PDS**

● MAR 2017-18 ● MAR 2016-17

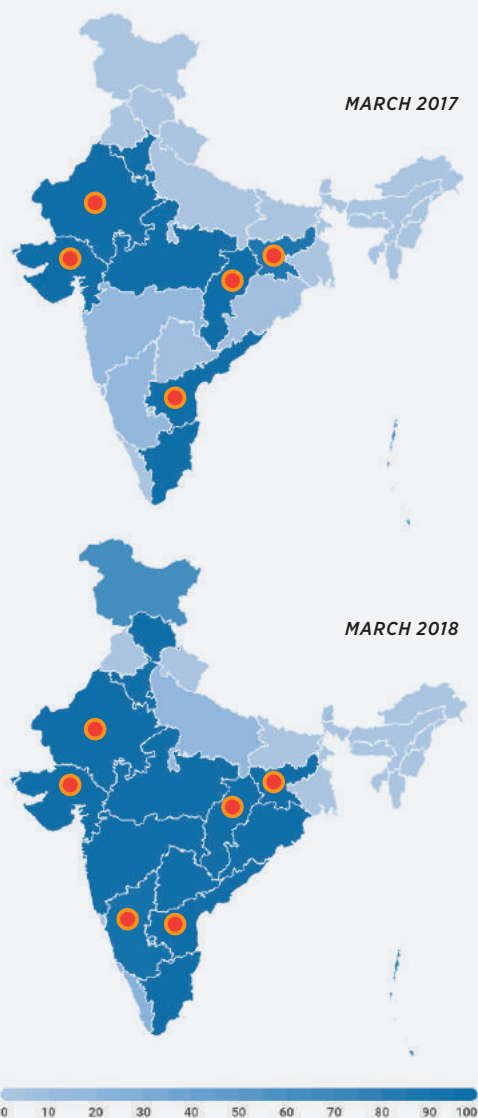
Note: Data for LPG for 2017-18 is updated as of August 2017. Data for MGNREGS, NSAP and PDS for 2017-18 is updated as of March 2018.

Data sources: LPG: DBT Bharat Monthly Reports; PDS: Annual Report of the Food and Civil Supplies Department 2016-17 and Lok Sabha Un-starred Question No. 5786 (3.04.2018); MGNREGS: DBT Bharat Monthly Reports (March 2017) and NREGA MIS Portal; NSAP: DBT Bharat Monthly Reports (March 2017) and NSAP Portal

Specifically, we seek to answer three questions related to Aadhaar's impact on PDS delivery in India:²⁹

1. What is the user experience of employing Aadhaar in PDS delivery? Whether and to what extent has Aadhaar contributed to the exclusion of genuine beneficiaries?
2. What is the user perception of employing Aadhaar in PDS delivery? Are users in favour or against the use of Aadhaar and why?
3. With regard to governance, has Aadhaar delivered on its potential to curb leakages and increase government savings?

The next subsection addresses our findings related to the above questions. This is followed by a discussion on implications and policy recommendations from the findings.

Figure 5.2: Proportion of fair price shops with e-PoS devices across India, Mar 2017 & Mar 2018*% OF PDS SHOPS USING E-POS DEVICES*

Note: Not all e-PoS devices are Aadhaar-enabled. Data currently not available for all states to make the distinction. However, where information is available, states that predominantly use Aadhaar-enabled e-PoS device are marked with a red dot. Data sources: Lok Sabha questions dated 11.04.2017 and 03.04.2018

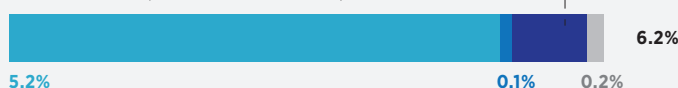
²⁹ An important benefit of using Aadhaar is to enable portability of social protection benefits within and across states. However, this has not yet materialised and hence is not explored here. In an answer to Lok Sabha unstarred question no. 5786, the government stated its plans to roll out portability features by 2019.

Figure 5.3: Average monthly exclusion from PDS and role of Aadhaar, Aug 2017 – Jan 2018**PROPORTION OF RESPONDENTS****ANDHRA PRADESH (AUG - NOV 2017)**

0.3% 0.8% (~0.3M PEOPLE)

RAJASTHAN (SEP - DEC 2017)

6.5% 0.7% 2.2% (~1.2M PEOPLE) 0.6%

WEST BENGAL (OCT 2017 - JAN 2018)

5.2% 0.1% 0.2%

Note 1: A PDS beneficiary household (one which has a valid ration card) is considered "excluded" for a particular month when it reports not getting their food ration entitlement for that month. This question was asked to each PDS beneficiary household with regards to the previous three months' ration provision. This was thereafter converted to a monthly average exclusion rate. Care was taken to not count households as "excluded" if there was a genuine reason for them not getting their ration in a particular month (such as the family being away during ration distribution and picking up their ration in the next month).

Note 2: Aadhaar-related reasons include: Aadhaar seeding, Aadhaar authentication failures, non-availability of PoS-able member and e-PoS connectivity/electricity issues. Non-Aadhaar related reasons include: non availability of ration and other reasons such as dealer not being present. Number of observations: AP (1026); RJ (854); WB (763)

Data sources: Exclusion rate: State of Aadhaar Survey 2017-18; Population numbers: Authors' calculations; see technical appendix available online for details.

USER EXPERIENCE AND EXCLUSION

Role of Aadhaar in exclusion from entitlements

In PDS, Aadhaar-related exclusion is low in percentage terms but affects many in absolute numbers. In rural Andhra Pradesh, Rajasthan, and West Bengal, about 0.8, 2.2, and 0.8 percent genuine beneficiary households, respectively, are excluded from receiving their food subsidy owing to Aadhaar-related factors.³⁰ We extrapolate this to be about 2 million individuals being excluded from their PDS entitlements every month from the rural regions of all three states. In Rajasthan and West Bengal, the overall monthly exclusion rate is significantly high; this is mainly driven by non-Aadhaar factors. The extent of exclusion and contribution of Aadhaar and non-Aadhaar factors for PDS can be seen in Figure 5.3.

Aadhaar-related points of failure

Beneficiaries experience different points of failure, related to Aadhaar and non-Aadhaar factors, while accessing their benefits. In Figure 5.4, we list the main points of failure that beneficiaries face that can lead to exclusion from accessing their food subsidy. While the data in the figure is for Rajasthan, the specific reasons for Aadhaar-related points of failure are similar across geographies.³¹

In the case of Rajasthan, the predominant reason for exclusion is the non-availability of ration, which is an issue unrelated to Aadhaar.

Biometric authentication failures are often cited as a reason for exclusion. In Rajasthan, 1.2 percent of all PDS beneficiaries face exclusion due to Aadhaar authentication failures. Note that the incidence of biometric authentication failure is much higher as revealed by UIDAI's own data. Since fair price shop owners are supposed to use a manual override mechanism for genuine beneficiaries, exclusion due to authentication failures should technically be zero.

³⁰. From a separate study of PDS in Jharkhand, we estimate the comparable metric of exclusion owing to Aadhaar-related factors to be about 5 percent (lower-bound estimate) (Drèze et al. 2017).

³¹. Data on the breakdown of Aadhaar-related reasons for exclusion for PDS in Andhra Pradesh and West Bengal is not presented. For Andhra Pradesh, we had an insufficient sample size due to an overall low exclusion rate. For West Bengal, "Aadhaar seeding" is the only Aadhaar-related reason for exclusion as they have not adopted the use of e-PoS devices.

Figure 5.4: Breakdown of monthly exclusion rate by reasons for exclusion, for Rajasthan's PDS, Sep-Dec 2017

PROPORTION OF RESPONDENTS

AADHAAR AUTHENTICATION FAILURES



AADHAAR SEEDING



E-POS CONNECTIVITY OR ELECTRICITY ISSUES



NO POS-ABLE MEMBER AVAILABLE



NO RATION AVAILABLE



OTHER REASONS



AADHAAR RELATED REASONS

NON-AADHAAR RELATED REASONS

Note 1: The total monthly PDS exclusion rate for Rajasthan is 9.9%. The percentages of each reason add up to more than 9.9% because respondents can select multiple reasons for exclusion.

Note 2: "No PoS-able member available" refers to a household where no member who can successfully authenticate themselves using biometrics was available in a particular month to collect ration (e.g. he or she was sick or away).

Number of observations: 854

Data source: State of Aadhaar Survey 2017-18

Figure 5.5: Number of attempts required for successful Aadhaar-based biometric authentication in PDS

PROPORTION OF RESPONDENTS

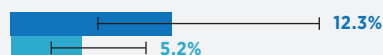
ONE ATTEMPT



TWO ATTEMPTS



THREE ATTEMPTS



MORE THAN THREE ATTEMPTS



ANDHRA PRADESH

RAJASTHAN

Note: Error bars denote 95% confidence intervals

Number of observations: AP (1,012); RJ (546)

Data source: State of Aadhaar Survey 2017-18

However, our data reveals the intersection of biometric failure and the manual override (incorrectly) not being employed, leading to exclusion. Of those who are able to successfully authenticate themselves, 1.9 and 3.0 percent of PDS beneficiaries in Andhra Pradesh and Rajasthan, respectively, required more than three attempts to do so.

In both states, however, more than 80 percent were able to authenticate themselves in two attempts or less. See Figure 5.5.

USER PERCEPTION

The majority of beneficiaries approve of Aadhaar's use to deliver PDS, but a significant minority oppose it. In Andhra Pradesh and Rajasthan, about 55.3 and 67.4 percent PDS beneficiaries say that the new system of PDS delivery using Aadhaar is better than the previous one without Aadhaar. However, a significant minority of 36.5 and 22.2 percent of beneficiaries in these two states respectively claim the new system is worse (See Figure 5.6).³² A study by the Center for Global Development and MicroSave (CGD & MS) in Rajasthan asked a similar question about PDS. In that study, 41 percent of respondents said that the new system is better, 12 percent said that it is worse, and the remaining said that they were indifferent or did not have an opinion (Center for Global Development 2017).³³

Those who feel the Aadhaar system is better favour it mainly because they felt secure that no one else can take

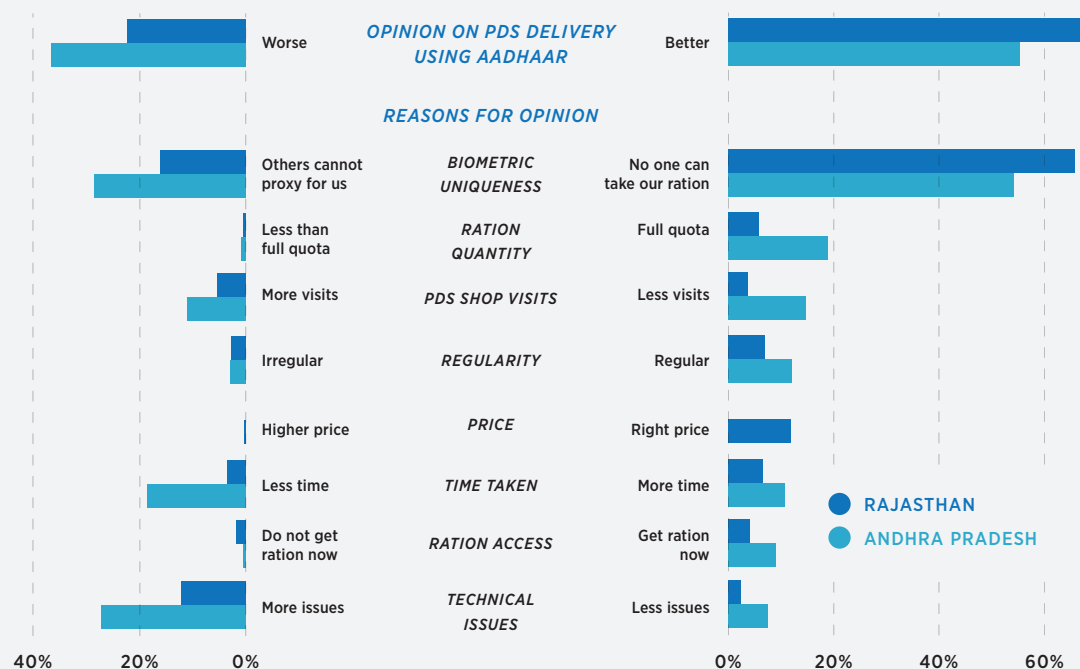
their ration (since non-family members will not have the required biometrics). The study by CGD & MS also found the same result in Rajasthan. In Andhra Pradesh, in addition to this security, many preferred the new system due to the regular availability of foodgrain at the right price and quantity, even though these benefits are not attributable to Aadhaar.

Interestingly, the exclusivity provided by biometrics also explains why many think the new system is worse. The use of biometric authentication prevents ration card holders from sending a proxy (say, their neighbour or relative) to collect their ration. This can be a liability for the elderly, differently-abled, or others who cannot travel easily.

The other important reason for those stating the Aadhaar system is worse includes facing technical issues (discussed above) and the process of obtaining the ration taking more time or requiring more visits.

Figure 5.6: Opinion on whether use of Aadhaar for PDS delivery is better or worse than previous system and associated reasons

PROPORTION OF RESPONDENTS



Note: In this question, respondents could tick multiple options for why they thought the system was better or worse.

Number of observations: AP (1,082); RJ (609)

Data source: State of Aadhaar Survey 2017-18

³² This data is not available for West Bengal because Aadhaar is only used for seeding and not biometric authentication in the state.

³³ While the direction of the CGD & MS survey results is similar to the State of Aadhaar Survey 2017-18, the difference in magnitudes may be a result of half of their sample coming from urban areas, differences in how the question was asked, and/or their focus on Rajasthan's household identity system, Bhamashah.

GOVERNMENT SAVINGS

The Government of India states that ₹83,000 crore (\$12.5 billion) has been saved in four years from FY 2014-15 to FY 2017-18 because of Aadhaar, DBT, digitisation, and other initiatives. The main source for savings is deletion of fake, duplicate, or ineligible accounts. For a breakdown of the savings figure, along with data on the corresponding number of non-genuine programme beneficiaries deleted, see Figure 5.7.

This estimate, however, suffers from three lacunae. One, the government has not provided the underlying data backing the number of non-genuine beneficiaries claimed to be deleted. Two, there is no clarification provided on whether the number of deletions excludes genuine beneficiaries and how that figure was calculated. Finally, no evidence is provided regarding Aadhaar's specific contribution to the deletion of non-genuine beneficiaries, which is valuable to ascertain the precise cost-benefit of Aadhaar's use to plug leakages.

DISCUSSION

Aadhaar's performance in social protection delivery is more mixed than the usual narrative prevalent today. Aadhaar is not an unbridled tool for the empowerment of the poor as evidenced by its role in the exclusion of many PDS beneficiaries. However, the focus on Aadhaar as the lead contributor to exclusion is also not supported by facts. Non-Aadhaar reasons for exclusion tend to be significantly higher in general and therefore worthy of more policy and civil society attention than they are currently receiving. Similarly, while a majority in both Andhra Pradesh and Rajasthan support the new system of Aadhaar for PDS delivery, more than a quarter find the new system worse. That is a significant minority whose grievances need to be addressed and mitigated. Many of the issues related to Aadhaar in social protection originate in the repeat use of biometrics for authentication on e-PoS devices. Three of four main Aadhaar-related points of failure shown in Figure 5.4 are related to biometric authentication (all except Aadhaar seeding). Two immediate policy considerations emerge from this trend.

Figure 5.7: Government of India's savings estimate from Aadhaar, DBT, & other initiatives

SCHEME	YEAR	SAVINGS ESTIMATE IN ₹CRORE	DELETION OF NON-GENUINE BENEFICIARIES
PAHAL	2014-15	14,672	38.5M fake & duplicate connections
	2015-16	6,912	
	2016-17	8,185	
	2017-18	9,105	
PDS	2016-17	14,000 [^]	27.5M fake & duplicate ration cards
	2017-18	12,792	
MGNREGS	2014-15	3,000	10% savings on wages (# of deletion not provided)
	2015-16	4,633	
	2016-17	4,108	
	2017-18	3,633	
NSAP	2015-16	249 [^]	154,000 fake, duplicate & ineligible names
	2016-17	150	
	2017-18	27	
SCHOLARSHIPS	2017-18	397	704,000 fake & duplicate names
OTHERS	2016-17	1,120 [^]	
TOTAL SAVINGS		82,986	

[^] Includes savings upto the year indicated

Data sources: Parliamentary questions, RTIs, and DBT Bharat Portal



One, the use of biometric authentication for each PDS transaction and delivery of other benefits should be reconsidered. Alternatives should be explored and tested. These should provide the same benefits of online biometric verification: comfort for users and governments against threat of identity fraud. At the same time, alternatives should not suffer from the current system's shortcomings: dependence on decent quality fingerprints and a combination of technologies (electricity, Internet, and servers) working simultaneously. Alternatives may include shifting to a less frequent verification cycle and exploring the combination of Aadhaar with other technologies, including offline authentication.

Two, the provision of alternative identification mechanisms if one's biometric authentication fails should be better enforced and widely advertised. While such processes exist on paper, the fact that denials are still happening points to a clear implementation gap that needs to be addressed. A regular, independent, sample-based assessment of exclusion and contributing reasons by the state government's programme implementation bodies may help. This can aid in identifying shop owners who refuse to use the manual override system and refer them to authorities for appropriate action. In addition, an intensive campaign to increase awareness of alternate options when biometrics fail may also prove to be effective.

In addition to countering the issue of biometric failures, a concerted drive to identify and include the remaining small percentage of unseeded individuals or households should be undertaken. The benefits of such an effort could lead to a significant drop in monthly exclusion rates.

The policy considerations mentioned above are currently not at the forefront of the agenda for either side of the Aadhaar debate. The facts compel us to go beyond the false policy dichotomy of scaling Aadhaar aggressively or discarding the whole project. Instead, a granular approach, where each use of Aadhaar is carefully considered and scaled, adjusted, or dropped, is what we believe can maximise the potential for providing essential social protection to India's poor.

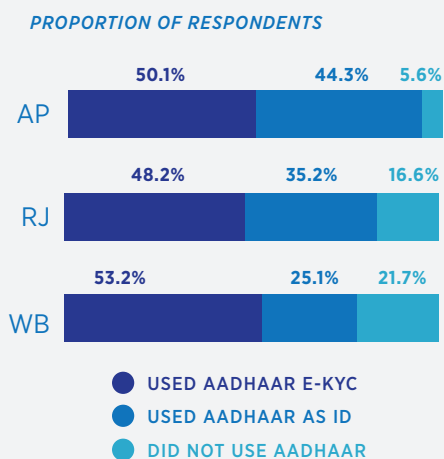
EMERGING USES

SPOTLIGHT ON TELECOMMUNICATIONS

In this spotlight, we look into how telecommunications companies have been using Aadhaar. The main benefit of Aadhaar within the telecom industry has been the use of e-KYC. E-KYC was officially recognized as a valid proof of identity and address starting in late 2016 (Banzal 2017). Our data shows that among respondents who received their SIM cards in late 2016 or after, about half used e-KYC in all three states (see Figure 6.1). Additionally, there appears to be a positive relationship between the use of e-KYC in the issuing of SIM cards and a better user experience. In an analysis of our three states combined, we find that use of e-KYC was positively correlated with same-day SIM card activation (see Figure 6.2). However, this relationship should be explored further. When using conservative corrections for multiple hypothesis testing, the correlation is no longer significant.

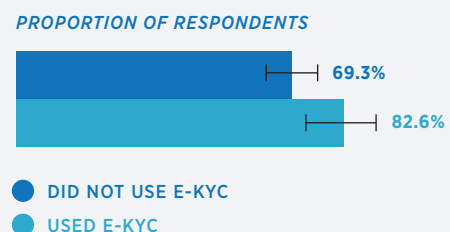
With increasing usage of Aadhaar by the private sector, it is important to ensure that companies prioritize strong data security and protection frameworks. Our survey data indicates that an overwhelming majority of individuals in the three states felt that it was important to know how the information they share with private companies will be used. This signals the importance individuals place on their personal data, underlining the need for transparency when requesting customer information and processes on obtaining informed consent. As uses in the private sector continue to grow, companies have an obligation to develop strong data protection measures for their customers as well as to build responsible consent mechanisms regarding the gathering or sharing individuals' data.

Figure 6.1: Proportion of respondents who used Aadhaar for SIM cards since late 2016



Number of observations: AP (115); RJ (149); WB (145)
Data source: State of Aadhaar Survey 2017-18

Figure 6.2: Proportion of respondents who got SIM activated in 1 day among those who used e-KYC vs. those who did not use e-KYC (All three states: Andhra Pradesh, Rajasthan, West Bengal)



Note: Error bars denote 95% confidence intervals
Number of observations: All three states (388)
Data source: State of Aadhaar Survey 2017-18

LOOKING AHEAD

The past year has been an unprecedented one for the Aadhaar programme. While more than 250 government schemes require Aadhaar for service delivery purposes, the Supreme Court has been hearing 30 petitions weighing the legality of those requirements.

With our recently completed SOA survey, we sought to better understand the experiences and opinions of rural residents in three key states, each representing a different perspective. One motivation for the survey was to gain an on-the-ground understanding of how Aadhaar is used by residents around the country – to ask what they think about the ID system, what motivated them to enrol, if and how they use the ID in their everyday life, and if they think Aadhaar has improved their experience of various services and social protection programmes.

We hope that the *State of Aadhaar Report 2017-18* will significantly add to the current understanding of what is working well with Aadhaar and what is not. However, there is still a critical need for further research to measure the impact of Aadhaar in other areas of interest.

In addition to the generation of more evidence regarding Aadhaar, we need to catalyse an ecosystem that engages with such research and Aadhaar's complexities rather than paint them in overly positive or negative hues. We hope this report is a step in that direction and we look forward to working constructively within the Aadhaar ecosystem to facilitate a more data-driven discourse and help motivate evidence-informed decision-making.



REFERENCES

"Aadhaar Authentication History." Unique Identification Authority of India. Accessed April 4, 2018. <https://resident.uidai.gov.in/notification-aadhaar>.

"Aadhaar mandatory linking: SC's Constitution bench to hear case today," Livemint, 2017. <https://www.livemint.com/Politics/8B7rty2oDrocrb6JSdVw6M/Aadhaar-mandatory-linking-SCs-Constitution-bench-to-hear-c.html>

Abraham, Ronald. 2017. "Aadhaar Needs a Privacy Law." Livemint, November 15, 2017.

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

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.

Binoy Viswam versus Union of India & Ors. 2017. Supreme Court of India.

Business Today. 2018. "UIDAI's Virtual ID, Limited KYC Does Little to Protect Aadhaar Data Already Collected, Say Critics," January 12, 2018. <https://www.businesstoday.in/current/economy-politics/uidais-virtual-id-limited-kyc-little-protect-aadhaar-data-collected-critics/story/267924.html>.

"Clearing the air on Aadhaar data breach," Livemint, 2018. <https://www.livemint.com/Opinion/MUPJK28VMeoCzI1whSBrJ/Clearing-the-air-on-Aadhaar-data-breach.html>

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/les/FocusNote-Financial-Inclusion-and-Development-April-2014.pdf>.

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

DBT Mission. "DBT Report (for July 2017)." Dataset. DBT Mission, Government of India, June 2017. https://dbtbharat.gov.in/data/documents/PMO_report_July_2017.pdf.

"Details of over a million Aadhaar numbers published on Jharkhand govt website," Hindustan Times, 2017 <https://www.hindustantimes.com/india-news/in-massive-data-breach-over-a-million-aadhaar-numbers-published-on-jharkhand-govt-website/story-EeFIScg5Dn5neLyBzrkwl.html>.

Demirgüç-Kunt, Asli, Leora Klapper, Dorothe Singer, Saniya Ansar, and Jake Hess. "The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution." Report. World Bank, April 2018. <https://openknowledge.worldbank.org/bitstream/handle/10986/29510/9781464812590.pdf>.

Demirgüç-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-ASia.pdf>.

DigiLocker. "DigiLocker." Cloud-storage platform. DigiLocker | Free, Secure, Flexible and easy-to-use application, April 2018. <https://digilocker.gov.in/>.

Drèze, Jean, and Reetika Khera. "Understanding Leakages in the Public Distribution System." Economic and Political Weekly 50, no. 7 (February 14, 2015). <http://www.epw.in/journal/2015/7/insight/understanding-leakages-public-distribution-system.html>.

Drèze, Jean, Reetika Khera, Anmol Somanchi, and Nazar Khalid. "Aadhaar and Food Security in Jharkhand Pain without Gain?" LII, no. 50 (December 16, 2017). <http://www.epw.in/journal/2017/50/special-articles/aadhaar-and-food-security-jharkhand.html>.

“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>.

Gobind vs State Of Madhya Pradesh And Anr. 1975. Supreme Court of India.

Gupta, Komal, and Remya Nair. “UIDAI Rolls out Virtual ID for Aadhaar,” April 8, 2018. <https://www.livemint.com/Politics/HEd324d2qsTk8u3yRhQj1O/UIDAI-rolls-out-virtual-ID-for-Aadhaar.html>.

“Information Security Practices of Aadhaar (or Lack Thereof): A Documentation of Public Availability of Aadhaar Numbers with Sensitive Personal Financial Information.” Centre for Internet and Society, May 16, 2017. <https://cis-india.org/internet-governance/files/updated-aadhaar-report.pdf>.

InterMedia. “India Wave 4 Report: FII Tracker Survey.” FII Tracker Survey. InterMedia, June 2017. http://finclusion.org/uploads/file/reports/India%20Wave%204%20Report_8-Jun-2017.pdf.

“Household Perception: Impact of Bhamashah & Digital Governance Reforms in Rajasthan.” Centre for Global Development and MicroSave, December 2017. http://www.microsave.net/files/pdf/171212_Household_Perception_Impact_of_Bhamashah_Digital_Governance_Reforms_in_Rajasthan.pdf.

Justice K S Puttaswamy (Retd.) and Anr versus Union of India and Ors. 2017. Supreme Court of India.

Khaira, Rachna. “Rs 500, 10 Minutes, and You Have Access to Billion Aadhaar Details.” The Tribune, January 3, 2018. <http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html>.

Kharak Singh versus The State of U.P & others. 1962. Supreme Court of India.

Khera, Reetika. “Impact of Aadhaar in Welfare Programmes” (September 29, 2017). Available at SSRN: <https://ssrn.com/abstract=3045235>

“Lock/Unlock Biometrics.” Unique Identification Authority of India. Accessed April 4, 2018. <https://resident.uidai.gov.in/biometric-lock>.

Lok Sabha Question. 2018. “Breach of Aadhaar Data.” <http://164.100.47.190/loksabhaquestions/annex/13/AU2582.pdf>.

Lokniti foundation vs Union of India, Supreme Court of India, 2017

Malak Singh Etc vs State Of Punjab & Haryana & Ors. 1980. Supreme Court of India.

Mehrotra, Aakash, Akhand Tiwari, M. P. Karthick, Mimansa Khanna, and Vivek Khanna. “MicroSave’s ANA India 2017 Report.” MicroSave, February 2018. http://www.microsave.net/files/pdf/Agent_Network_Accelerator_Research_Country_Report_India.pdf.

Ministry of Electronics and Information Technology. 2017. “White Paper of the Committee of Experts on a Data Protection Framework for India.” http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf.

Mittal, Priyanka. 2017. “Aadhaar Mandatory Linking: SC’s Constitution Bench to Hear Case Today.” Livemint, December 14, 2017. <https://www.livemint.com/Politics/8B7rty2oDrocrb6JSdVw6M/Aadhaar-mandatory-linking-SCs-Constitution-bench-to-hear-c.html>.

M.P. Sharma and Others versus Satish Chandra, District Magistrate, Delhi, and others. 1954. Supreme Court of India.

NPCI. “Retail Payments Statistics on NPCI Platforms.” Dataset. National Payments Corporation of India, March 2018. https://www.npci.org.in/sites/default/files/RETAIL%20PAYMENTS%20STATISTICS%20ON%20NPCI%20PLATFORMS_Mar%202018.xlsx.

NPCI. "Aadhaar Payments Bridge (APB) System Standard Operating Procedure." Standard Operating Procedure. National Payments Corporation of India. Accessed March 15, 2017. https://www.npci.org.in/sites/all/themes/npcl/images/PDF/APB_Standard_operating_procedure.pdf.

"Privacy on the Line." Report. Dalberg, CGAP, and Future of Finance. November 2017. <http://foundation.ifmr.co.in/wp-content/uploads/2017/11/Privacy-On-The-Line.pdf>.

PMJDY. "Bank Categorywise Report as on 14/03/2018." Dataset. Department of Financial Services, March 14, 2018. <https://www.pmjdy.gov.in/Archive>.

Rajya Sabha Question. 2018. "Notifications Regarding Schemes under Aadhaar." <http://164.100.158.235/question/annex/245/As82.pdf>.

RBI. "Reserve Bank of India Annual Report 2016-17." Annual Report. Reserve Bank of India, August 30, 2017. https://rbidocs.rbi.org.in/rdocs/AnnualReport/PDFs/RBIAR201617_FE1DA2F97D61249B1B21C4EA66250841F.PDF.

"Response to RTI by Ujjainee Sharma," n.d. <https://i0.wp.com/thewire.in/wp-content/uploads/2015/06/Enrolment-through-introducer.jpg>.

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>.

Sethi, Aman, Samarth Bansal, and Roy Saurav. 2017. "Details of over a Million Aadhaar Numbers Published on Jharkhand Govt Website." Hindustan Times, July 19, 2017. <https://www.hindustantimes.com/india-news/in-massive-data-breach-over-a-million-aadhaar-numbers-published-on-jharkhand-govt-website/story-EeFlScg5Dn5neLyBzrkwl1.html>.

Sinha, Amber, and Srinivas Kodali. 2017. "Information Security Practices of Aadhaar (or Lack Thereof): A Documentation of Public Availability of Aadhaar Numbers with Sensitive Personal Financial Information." Centre for Internet and Society. <https://cis-india.org/internet-governance/information-security-practices-of-aadhaar-or-lack-thereof-a-documentation-of-public-availability-of-aadhaar-numbers-with-sensitive-personal-financial-information-1>.

State of Aadhaar. 2017. "5 Unanswered Questions about Linking Aadhaar and SIM Cards." [www.stateofaadhaar.in](http://stateofaadhaar.in/5-unanswered-questions-about-linking-aadhaar-and-sim-cards/). October 30, 2017. <http://stateofaadhaar.in/5-unanswered-questions-about-linking-aadhaar-and-sim-cards/>.

"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>.

World Bank. 2017. "The Public Distribution System in India. Policy Evolution and Program Delivery Trends." The 1.5 Billion Question. September 2017. <http://pubdocs.worldbank.org/en/901801506434971394/Chapter-2.pdf>.

Unique Identification Authority of India. Aadhaar (Enrolment and Update) Regulations, 2016 (No. 2 of 2016) - Page 10-41 (2016). <https://uidai.gov.in/legal-framework/acts/regulations.html>.

Unique Identification Authority of India. Circular. "Circular 1 of 2018: Enhancing Privacy of Aadhaar Holders - Implementation of Virtual ID, UID Token and Limited KYC." Circular, January 10, 2018. https://uidai.gov.in/images/resource/UIDAI_Circular_11012018.pdf.

Unique Identification Authority of India. "Information W.r.t. RTI Application of Shri Ujjainee Sharma," April 7, 2015. <https://i0.wp.com/thewire.in/wp-content/uploads/2015/06/Enrolment-through-introducer.jpg>.

Designed by

studiosubū

IDinsight India

24/1, 3rd Floor, Hauz Khas Village
New Delhi 110 016, India

StateofAadhaar@IDinsight.org
IDinsight.org

ID Insight India Private Limited
CIN: U74140DL2013FTC252591