Biometric Identification Systems for Welfare Distributions:  
A Case Study of Aadhaar

Caroline Schauder  
Advised by Dr. Rajesh Veeraraghavan

A thesis submitted in partial fulfilment for the requirements for the  
Award of Honors in

Science, Technology, and International Affairs  
Edmund A. Walsh School of Foreign Service  
Georgetown University

May 2020
Acknowledgements

This thesis is a product of two years of research and fieldwork. It was made possible by the help of many different people and entities, and I am grateful to everyone who was a part of this process.

Dr. Veeraraghavan, I reached out to you over email and you agreed to be my advisor without ever having met me. Throughout the last year, you have challenged my thinking and pushed me to make this my best work possible. This process was daunting in many ways, but you have been reassuring and kind, and you have given me confidence in myself and my work. I am so grateful to have worked with you this year, and I sincerely appreciate the time you have dedicated to guiding my thesis.

Irfan, you are the reason that I felt prepared and qualified to pursue this project. You helped me navigate the early stages of the research process and provided me with the resources to make this project happen. Your dedication to your students is inspiring, and I am so appreciative for the opportunity to work with you. I will be forever grateful for your continuous encouragement and support over the last two years.

Thank you to Sneha Varma, who assisted in conducting field work and translated the interviews. This project would not have been possible without you.

To the STIA faculty that made this possible, specifically Professor Mendenhall, thank you for your dedication to the thesis class. You provided us with the resources to produce quality undergraduate research, and I appreciate all of the time that you put into your students.

To the SFS Dean's Office and the Lisa J. Raines scholarship, I am eternally grateful for the financial support which made the project possible. This thesis has significantly influenced my academic trajectory, and I appreciate the resources that you provide to help undergraduates pursue research.

Finally, to my family and friends who supported me in this endeavor, thank you for taking the time to listen when I needed to talk out ideas or simply be distracted from my ideas. Thank you specifically to my mother, who allowed me to go to India independently and pursue this project. I know that this was not easy, and I appreciate your trust in me.
# Table of Contents:

**Acknowledgements**  
2

**Abstract**  
4

**Introduction**  
5

**Literature Review**  
7

**Methodology**  
15
  - Study Setting  
  - About Public Distribution System (PDS)  
  - Data Source  
  - Data Collection  
  - Data Management  
  - Data Analysis

**Analysis**  
19
  - Inclusion  
    - Universal Coverage  
    - Universality/Non-discrimination:  
  - Accessibility  
    - Direct and indirect costs  
    - Information and technology disparities

**Design**  
26
  - Establishing a robust - unique, secure, and accurate - identity  
    - Unique  
    - Secure  
    - Accurate  
  - Interoperable and responsive platform  
    - Responsiveness  
    - Interoperability

**Governance**  
39
  - Data privacy, security, and user rights  
  - Legal and trust frameworks  
  - Adjudication

**Conclusion**  
44

**References**  
46
Abstract

Personal identification is now an essential prerequisite for development in the modern world. Providing proper identification documents improves access to both public and private services for citizens and helps governments to understand and serve their citizens better. In an effort to make identification systems as unique and accurate as possible, states are implementing more robust (unique, secure, and accurate) systems through the integration of biometrics, most commonly fingerprints. While the systems seem to be effective from a government’s large-scale perspective, biometrics-based systems present significant challenges, including universal coverage, accessibility, and implementation challenges. This thesis studies Aadhaar, India’s biometric identification system, as a case study in order to understand how the users perceive the system. As the largest biometric identification system in the world, over one billion individuals are enrolled in the system. India created Aadhaar with the dual intention of providing an identity to those unregistered in the current system and to enable government databases to communicate with each other to ensure that state funds would be delivered directly and only to those in need. Despite incredible enrollment rates, 4.4 percent of Indian residents are excluded from Aadhaar for various reasons (State of Aadhaar, 2018). Because there is no alternative, these individuals are entirely excluded from the welfare services for which they are eligible. Consequently, different scholars have identified Aadhaar as both a success and failure. This study seeks to understand how Mumbai’s urban poor perceive Aadhaar, specifically in regards to the distribution of Public Distribution System (PDS) services. This study will use the World Bank’s Principles on Identification for Sustainable Development: Toward the Digital Age as a guiding framework to organize the analysis. By using the World Bank’s principles as a framework, this study will identify ways in which Aadhaar has performed well and which ways Aadhaar needs to improve. Ultimately, this study found that when Aadhaar worked well for individuals, they expressed neutral or positive sentiments regarding Aadhaar. However, when Aadhaar did not work for individuals, they were completely excluded from the system. This necessitates more effective alternative methods for authentication.
Introduction

An employee of the Bombay Municipal Corporation (BMC) used to clock in for work every morning at 8 a.m. for his job as a sanitation worker. He did this everyday preceding his work, like many employees around the world. However, this process changed when the BMC linked the work hour monitoring system to Aadhaar, India’s twelve-digit unique identification card. Aadhaar, which includes biometrics, such as fingerprints and iris scans, is an identification card that India has connected to many public and some private services to create a more accurate and efficient way of authenticating individuals (Das, 2015). With the integration of Aadhaar, this employee must now scan his fingerprint every time he enters work to authenticate himself and to provide a digital time stamp of his arrival. However, with Aadhaar, if he has not registered his arrival by 8 a.m., he is ineligible to receive his pay for that entire day. There are generally long lines of employees waiting to clock in every morning, and with the new system, if he is still waiting in line after 8 a.m., he will not be paid for that day. With this Aadhaar-based system, he has to arrive at work thirty minutes early to ensure that he is able to register before his starting time (Yadav, 2018).

This anecdote exposes one facet of a larger theme of unintended negative consequences that users face within the Aadhaar system. The concept of linking Aadhaar to employee-work-hour monitoring systems makes sense from a company management perspective, in that it standardizes a process, this is one of many examples of digital systems that are created with good intentions but result in significant inconveniences for the users. It is likely that the employer did
not care that linking this system to Aadhaar would inconvenience some users, or even prevent some individuals from receiving the pay for which they worked. Identification systems try to create a process that is applicable and functional to every user. However, it is challenging to find a biometric system that always works for everyone. The more rigid identification systems become, the less able they are to account for exceptions or errors. The ramifications of these errors generally hurt the users, and exclude them from the system that is sold as benefiting them. This emphasizes the importance of understanding the user experience of a digital identification system in order to evaluate its success.

This study seeks to understand how Mumbai’s urban poor perceive Aadhaar, specifically in regards to the distribution of PDS services. This study will use the World Bank’s *Principles on Identification for Sustainable Development: Toward the Digital Age* as a guiding framework to organize the analysis. By using the World Bank’s principles as a framework, this study will identify ways in which Aadhaar has performed well and which ways Aadhaar needs to improve from the perspective of the users.
Literature Review

Formal identification is now an essential prerequisite for development in the modern world (Gelb, A., Clark, J. 2013). Providing proper identification documents not only improves public policies, but ensures access to citizen’s civic and legal rights (Gelb, 2013). It also allows citizens to participate in essential private sector activities, such as education, formal employment, and financial services. Birth certificates are considered the foundation of all other forms of identification, in that they prove age, nationality, and parentage (Gelb, 2013). Wealthy countries exhibit strong identification regimes, with generally over 98 percent of people registered with birth certificates (UNICEF Innocenti Research Centre, 2002). In contrast, poorer countries struggle to include almost all of the population and to provide credible identification services (Gelb, J. 2013). A UNICEF analysis from 2000 estimated that 36 percent of children worldwide and 40 percent of children in the developing world were not registered at birth (UNICEF, 2005; UNICEF Innocenti Research Centre). It also found that even registered individuals found it difficult to access their birth certificates due to poor record keeping, lack of mobility, or corruption (Gelb, 2013).

The World Bank selected ‘legal identification for all’ as one of their Sustainable Development Goals to stress the importance of identity in developing a more inclusive society. They support this claim in their official report by writing:

*The implications of ‘providing legal identity for all, including birth registration’ go beyond individual rights and opportunities: being able to reliably verify the identities of their population is critical for countries to deliver services efficiently, strengthen their ability to raise revenues, and foster growth in the private sector’* (World Bank).
As developing countries aspire to provide more services for their citizens, such as healthcare, education, and welfare benefits, they need robust identification systems to facilitate these services. Countries are employing electronic identification systems as a way to “leapfrog” traditional paper-based systems (Gelb, 2013). Many of these systems include biometric identification technology in an effort to reach all citizens efficiently, to improve accuracy and security, and to create reliable records (Gelb, 2013). However, as of 2019, only 24 percent of developing countries have a digital identity system, and only 3 percent of these countries have a foundational identity system that can be used in both online and offline domains (Mir, U., et al, 2019).

As countries begin to adopt digital identification systems, it is important to understand the academic consensus and questions regarding biometrics. This literature review serves to summarize the current scholarship focusing on biometric identification systems and it presents the most relevant debates in the field. It explores biometric identification systems through three lenses, challenges of standardization, effectiveness and accessibility, and surveillance. The questions posed in this literature review will drive the analysis of this thesis.

“Seeing” citizens

Advocates of identification for development assert that identification systems allow citizens to be represented and served by the government. This follows the assumption that states can govern well only when they ‘see’ their subjects within a uniform administrative format (Sriraman,
2018). James Scott argues that states use methods such as censuses, surveys, and naming and identification practices to make their subjects more visible and legible (Scott, 1998). He refers to these practices as ‘simplifications’ and ‘abstractions’ on account of the reductive and universalizing functions that these practices create (Scott, 1998; Sriraman, 2018). State methods for standardization have varied over time and place, but they include surveys, population registers, the invention of freehold tenure, the standardization of language and legal discourse, the design of cities, and the organization of transportation (Scott, 1998). All of the information taken from these sources helps the state to better “understand” its citizens, and more accurately know where its citizens are located, what they do for a living, and other demographic information. This helps the state target services directly to the people who need them most. Scott advocates that convenient standards are necessary in order to create a modern state. (Scott, 1998, Sriraman, 2018).

However, this assumes that the ‘simplifications’ and ‘abstractions’ are effective in helping the government understand its citizens. If a state simplifies information too much, it could lead the government to make assumptions about its population that are false or problematic (Ceyhan, 2002). Ceyhan cautions against blind acceptance of data from large-scale identification systems (Ceyhan, 2002). He worries that data created from these systems will lead governments or organizations to make certain assumptions about populations (Ceyhan, 2002). Practically, there must be some standardization in order for states to function. But others argue that Scott’s glossing over of critical social factors in an effort to achieve a uniform system does not always achieve its desired goal - to better understand its citizens. Loveman expresses this doubt through
her ethnography studying the civil registration system in Brazil, which she argues failed to build a modern infrastructure of governing subjects (Loveman, 2007). She suggests that the state’s ‘visual acuity’ was devoid of indigenous forms of knowledge, and therefore did not employ local metrics and conditions (Loveman, 2007). This impaired its own goal of making its subjects visible to the state.

Possibly the best example of a state’s prioritization of convenience over understanding its citizens is the Spanish empire’s assignment of last names to Philipino subjects (Scott, 1998). In 1849, the Spanish Governor declared that Philipinos must adopt permanent Hispanic surnames, as a way of imposing Spanish colonial values and rules on the Philipinos. The Governor created a *Catologo*, or a list of personal names, nouns, and adjectives given to villages that could be used as example names. The local enforcers carried this out by assigning the last names to citizens down the Catologo, in alphabetical order (Scott, 1998). This resulted in entire villages having names that started with the same letter. One can still see the effects of this today by looking at a list of names of people residing in one geographical area and noticing a disproportionate amount of names that begin with the same letters. The Spanish implemented this system purely out of convenience and standardization, however, because they did not record the previous names and identifiers used by the Philipinos, it is impossible to trace families and property before the re-naming campaign (Scott, 1998). The prioritization of convenience by the government sacrificed great insights into the Philipino population. For example, it is nearly impossible to trace back land or family lineage prior to the *Catologo*, because the Spanish did not acknowledge their previous identities (Scott, 1998). Scott argues for the importance of standardizing
information in order to better understand, and therefore serve citizens. However, these examples pose the question of whether standardization actually helps states better understand its citizens.

When states implement biometric identification systems, they standardize authentication using biometrics. Biometrics present significant benefits to states in that they are generally more accurate, therefore reducing corruption, and convenient in that they function with a nation-wide, centralized system. However, it is dangerous when the state simplifies an identity to a biometric. It not only assumes that a person has the required biometric, for example fingerprints, but that it will always work properly. There will likely always be exceptions to biometric authentication, and if the state does not acknowledge that a biometric is a simplification of identity, it will prevent certain individuals from being “seen” by the government.

This poses the question of state priorities. Is the exclusion due to biometrics of a minority of individuals justified by the effectiveness of biometrics for the majority? This necessitates greater scholarship to understand this question, and this study will address the accuracy of identification systems in understanding users.

**Effectiveness and Accessibility**

While biometric identification systems promise greater accuracy and effectiveness in authenticating individuals, do they actually work? The ideal biometric system is universal, unique, permanent, and collectable (Yanushkevich, n.d.). Universal means that each individual possesses this characteristic. There will always be exceptions to this, as it is difficult to find one
feature that everyone possesses. For example, if a system uses fingerprints, this must take into account those who do not have fingers or hands. However, the best system will be the most inclusive and require as few as possible exceptions. Additionally, the features must be unique. No two people can share the same characteristic. Fingerprints and iris scans are good examples of features that uniquely identify individuals. The characteristic must also be permanent, in that it should neither change nor be alterable. It must be consistently representative of the individual. Finally, the feature should be collectable. It must be readily and easily presentable to a sensor and realistically quantifiable (Yanushkevich, n.d.).

When evaluating biometric identification systems, it is also important to consider the performance of the system, acceptability by the public, and potential for circumvention (Yanushkevich, n.d.). Firstly, one must consider a biometric identification system’s accuracy, speed, robustness, resource requirements, and operational or environmental factors that affect its accuracy and speed. For example, a signature could be a biometric form of identification; however, it has low accuracy results, and therefore has lower performance than something like fingerprints which is unique to each individual. Additionally, one must consider the extent to which the public is willing to accept a particular method as a biometric identifier in their daily lives. Biometric technologies border on being intrusive, and some people aren’t comfortable with certain methods (Yanushkevich, n.d.). Fingerprints work well because it is realistic to scan a fingerprint each time, whereas eye scans seem a little more intrusive. The final characteristic, circumvention, discusses the likelihood that a method can be fooled through fraudulent methods.
Schauder 13

(Yanushkevich, n.d.). This is important because if a system can easily be manipulated, then it does not fulfill its promise to identify individuals correctly.

While fingerprints perform better than most other forms of biometrics when considering the criteria defined above, there are still significant challenges when implementing fingerprints on a large scale. Primarily, disabilities or everyday life conditions can cause deformations in fingerprints, making them undetectable by the scanners (Biometrics at the Frontiers, 2005). One study estimated that five percent of individuals would not be able to register and produce a detectable fingerprint (Biometrics at the Frontiers, 2005). This is especially important to consider when evaluating state-wide identification systems which include millions, and sometimes billions, of people. Similarly, the US-VISIT program in 2004, with a database of 6,000,000 individuals, had a false match rate of .31% and a missed match rate of 4% (Anderson, 2008). While these studies are from the early 2000s, similar challenges persist today, even with the improvement of technology. Four or five percent of a large population presents a significant concern and necessitates a valid alternative for these individuals. False Match rates (when one is authenticated but they should not be), False Non-Match rates (when someone is not authenticated but they should be), and the inability to detect certain fingerprints, present significant concerns for national identification systems that rely exclusively on fingerprint authentication.

State identification systems often identify universal coverage as one of the main goals in digital identification systems. The World Bank’s Principles on Identification for Sustainable Development identified Universal Coverage as the first factor necessary in establishing an
effective identification system. India’s implementation of Aadhaar, a biometric identification system, similarly established its main goal of documenting the undocumented (Das, 2015). Aadhaar strives to identify every Indian resident, over 1 billion people. India, and other countries work towards universal coverage in an effort to ‘see’ all of their residents, and therefore serve them effectively and efficiently (Das, 2015). This thinking reframes identity as a human right (Das, 2015).

The enrollment of hard-to-reach groups makes sense in theory, as if the state understood these previously unregistered individuals, they would better be able to support them by knowing their location and specific needs. However, this implies that the state is able to reach these deemed “hard-to-reach” groups. Therefore, it is not enough to simply create a digital identification system and expect individuals to enroll. There must be a strategy implemented which ensures inclusion of all individuals and offers proper incentives. Otherwise, the people who were previously unregistered will likely remain that way. The Unique Identification Authority of India (UIDAI) considered this in their creation of an enrollment strategy which strived to be pro-rural and pro-poor (Das, 2015). They tried to reach these populations by linking Aadhaar with government services, such as subsidies and rations, specifically used by these populations. The UIDAI also included a strategy to include traditionally marginalized groups such as the urban poor, children, women, differently abled people, and tribal communities. It offered different initiatives to incorporate these individuals into Aadhaar. Because over 90 percent of India is enrolled in Aadhaar, it seems that this strategy has been fairly effective (State of Aadhaar, 2018). However, there is still a percentage of the population that is not enrolled, and it is unclear if these
are individuals categorized in “hard-to-reach” groups. This questions whether biometric identification systems generally are actually able to reach their intended populations. Or do they continue to exclude those who were previously undocumented by the government?

However, some scholars worry that the push to achieve universal coverage in biometric identification systems actually hurts those who are unable to register even more than previous systems. One study asserts that the more accurate a system becomes, the more people rely exclusively on the system (Biometrics at the Frontiers, 2005). If the system works for 98 percent of individuals, then both the government and the services which are linked to this system will increasingly rely on this system and expect people to be able to use it. However, what happens to the 2 percent of individuals whose fingerprints are not detectable by the machine? Mordini and Petrini argue that when identity systems have wide user scope, and successful outcomes, identity errors and abuse may become less frequent, but when they happen, they could potentially be more dangerous (Mordini, 2007). Mordini argues that the level of exclusion becomes significantly more comprehensive the more effective and accepted the system. This therefore emphasizes not the universality of the system, but instead the existence of an effective exception handling system (Biometrics at the Frontiers, 2005). The European Commission Joint Research Centre advocates for the need of exception handling in biometric identification systems in its statement,

We shall have to consider exception handling processes for individuals who have difficulty with automated processes ... The impact [of disenfranchisement from people excluded] will depend upon how well such factors have been considered in advance, together with the nature and practical delivery of associated exception handling processes (Biometrics at the Frontiers, 2005).
The *Biometrics at the Frontiers* report therefore questions whether universal coverage should be the end goal for biometric identification systems. It is unrealistic to assume that biometrics will always work for everyone, and states should not expect to achieve perfect universal coverage. How do states balance the goal of achieving universal coverage with the reality that exceptions will likely always occur?

**Surveillance**

Other scholars worry about the role of biometric identification systems in establishing state surveillance systems. The root of surveillance lies in the state’s desire to ensure security (Scott, 1998; Lispschutz, Rowe, 2005). Scott’s *Seeing Like a State* discusses the role of identification, specifically last names, in asserting control and order (Scott, 1998). Lipschutz also explores the concept of security by asserting that “security demands certainty” (Lipschutz, Rowe, 2005). By this, he means that in order to secure systems and ecosystems, a government or people must be certain of what is happening and how individuals will respond. If true, it implies that states will try to become as secure as possible by monitoring as much as they can. However, Ceyhan argues that ensuring certainty cannot ensure success, and therefore states will never be completely secure (Ceyhan, 2002). Ceyhan questions the validity and justification of identification systems, as they may not achieve their intended goal.

The concept of surveillance has evolved significantly with the advancement of technology. Foucault described his panopticon theory of surveillance as centralized state surveillance that derives from one unified source (Foucault, 1977). However, other authors argue that this does
not apply today. Gilles Deleuze and Felix Guattari propose that modern-day surveillance is not centralized surveillance, but instead a system that operates as a “surveillant assemblage” (Giddens, n.d.). Patton defines an assemblage as a multiplicity of heterogeneous objects whose unity comes solely from the fact that these items function together, that they “work” together as a functional entity (Patton, 2009). Therefore, instead of surveillance coming from one specific source, it is now an amalgamation of information and resources from many different sources. Ceyhan supports this theory, arguing that contemporary surveillance functions through a network of public, private, and transactional databases (Ceyhan, 2002). He asserts that surveillance occurs with neither surveillant nor surveilled fixedness to single places, and seems to be the convergence of some discrete systems (Ceyhan, 2002). Bozbeyoğlu relates this concept to electronic IDs in reference to Turkey’s case specifically, by discussing the ways in which the identification document is linked to all spheres of society - public, political and commercial (Bozbeyoğlu, 2011). Because countries are connecting identification systems to all aspects of life, electronic identification systems create a unified system from many different sources - both commercial and public (Bozbeyoğlu, 2011). As national identification systems become more complex and connected to public and private services, will they give the government greater power in controlling and monitoring activity? Furthermore, if a state’s goal is to understand its citizens better in order to serve them more effectively, where is the line drawn? How much information is too much information, and when does it become a breach of privacy?

The current literature explores the ways in which biometrics enforce surveillance. Finn asserts that fingerprinting and photography bring all bodies (criminal and non-criminal) under
surveillance (Finn, 2005). Fingerprints were originally used as a replacement to photos in order to identify criminals after a crime was committed (Finn, 2005). Previously, law enforcement organizations used photos to document criminal identity (Finn, 2005). They used Bertillon’s anthropometric system of identification, which recorded specific identification data in a standardized form and allowed the police to process more records than was previously possible (Finn, 2005). However, over time, the galleries grew so much that they accumulated massive collections. In this case, the determination of a criminal or innocent citizen preceded the taking of the photo. Therefore, only criminals’ pictures were taken. However, Finn asserts that with the collection of fingerprints, the use of the camera precedes the identification of someone as a criminal or non-criminal (Finn, 2005). The police transitioned to capturing fingerprints because they take up less space than photos and they are a literal trace of a person (Finn, 2005). In this capacity, Finn claims that “fingerprints can be collected independently of the presence and knowledge of the body to which they attest and independent of traditional spatial and temporal constraints” (Finn, 2005, p. 28). It was still used on an offender-basis, but it gave rise to new police practice and a new mode of state surveillance based on the aggregate collection of identification data (Finn, 2005). Finn believes this has resulted in the collection of fingerprint data on known and unknown bodies, which has expanded the scope of law enforcement from the individual criminal body to a larger, abstract social body (Finn, 2005, p. 29).

Law enforcement uses fingerprint data because these methods allow them to collect identification material without the physical presence or consciousness of individuals (Finn, 2005). This proposes the idea that states are collecting information about people without their
consent, but what happens when individuals do consent or are coerced into consenting to national identification systems? Does voluntary enrollment mean that governments can use individual’s biometrics how they want? This also raises the question of whether these systems are voluntary at all, or if individuals are coerced into these programs. This gap calls for more scholarship focusing on the role of surveillance in established government identification systems for which people consent.

This literature review combines concepts from multiple different disciplines in order to summarize the current scholarship, present themes, and guide the questions that will be explored throughout this thesis. The major themes identified in this literature review are universal access, state-sponsored standardization, and privacy.

Universal access continuously appears in the existing literature as an essential priority for biometric identification systems. However, some scholars suggest that making universal access the end goal of identification systems more intensely excludes the small minority that are unable to participate in the system. The debate regarding universal access frames this paper’s discussion of accessibility within Aadhaar. Additionally, the literature presents contradicting opinions towards the effectiveness of state-sponsored standardized systems in their ability to understand and serve citizens. This study analyzes survey data from users to explore whether individuals feel “seen” through Aadhaar. Finally, the literature discusses surveillance and privacy extensively. It generally addresses the topic from an academic point of view, and this thesis questions whether users express similar concerns as those posed in the literature. This study
builds upon the existing literature to derive insights regarding how Mumbai’s urban poor perceive Aadhaar.
Methodology

Study Setting

The UIDAI literature identified the urban poor as a “hard-to-reach” demographic due to high proportions of migrant workers with temporary or seasonal jobs (Das, 2015). Mumbai, a city of over 18 million people, has the largest slum population in India. Six percent of Maharashtra’s population lives in the slums of the state capital, Greater Mumbai (Risbud, n.d.). This study selected Mumbai as the study site because it sought to understand the user experience of Aadhaar by the urban poor. This study involved 99 individuals interviewed from four different neighborhoods in Mumbai — Dharavi (n=26), Ambedkar Nagar in Colaba (n=25), Cuffe Parade fishing village (n=23), and residencies in Mumbai Central (n=24). Each of these localities are low-income, highly concentrated urban settlements in the heart of Mumbai, the financial capital of India. These localities were selected in an effort to collect a diverse sample in different areas of Mumbai. The image below details the geographic locations of these urban zones.
This study seeks to understand the role of Aadhaar in user’s collection of Public Distribution Services, and therefore, the interviews were conducted in or near ration shops. The Public Distribution System (PDS) is India’s government welfare system that provides food and fuel to the poor (Das, 2015). It has a network of more than 462,000 fair price shops, established in each town and city, which distribute government subsidized food and fuel (Das, 2015). It is the largest distribution network of its kind in the world (Das, 2015). India’s Unique Identification Authority (UIDAI) established Aadhaar with the goal of making India’s Public Distribution System (PDS) more effective. Therefore, the government connected the PDS system to Aadhaar. Presently, in order for individuals to receive the government rations for which they are eligible, they must first be registered in the Aadhaar system. They must then go to a ration shop, present their Aadhaar card and their government-issued ration book, and scan their fingerprint to authenticate their
identity. If the individual cannot complete any of these steps, then they cannot receive their rations.

Data Source

Aadhaar was created with the intention of streamlining the PDS process, making the system more flexible and transparent, and enabling the government to fulfill the objective of food security in times of crises (Das, 2015). This study analyzes whether biometric identification systems deliver on their claims to improve access for those who need the services most. Therefore, this study targeted individuals who use and benefit from government PDS rations, in an effort to understand the effects of implementation of biometric identification systems on the users.

This study involved a survey conducted with ration shop customers. The study facilitators began the survey collection at ration shops, and then often were directed or led to other homes to speak with neighbors and friends about their experiences with Aadhaar. The participants answered and discussed a brief, 9-question survey, regarding their thoughts about the utility of Aadhaar. The survey did not collect data regarding the socio-economic status of the participants. However, because the participants were recruited at ration shops or from neighbors, the study participants were largely low-income recipients of government benefits such as rations, subsidies, and various government schemes. People were given the choice to participate, and this study was approved by the Georgetown University Institutional Review Board.
Data Collection

All of the interviews were conducted by myself and Sneha Varma, a Master’s student at St. Xavier’s College, who helped translate the interviews as they were conducted. The most common languages spoken were Marathi, Hindi, and Tamil. As a white American woman, I noticed differences in the ways in which the subject participants interacted with me, and I recognize that this could bias the data. Some individuals seemed uncomfortable speaking with me. Others seemed to express more critical opinions of Aadhaar possibly because they were confident that I was not associated with the Indian government, and therefore their responses would not have implications for their rations. Others seemed to be more positive towards Aadhaar, which could have been an effort to present a good image of India to a foreigner. I tried to mitigate this by working with a Master’s student from India. Still, conducting this survey as an outsider likely had varying effects and biases in the data that I could not control.

This study was conducted from June to July 2018. The interview began by asking the individual for verbal consent to participate. Then, a series of questions were asked and the results were recorded by notes in a notebook. The nine general questions are listed below. Occasionally they were adapted depending on the response.

1. Do you have an Aadhaar card?
2. If so, which schemes have you linked it to (ration, gas subsidy, SIM, bank, etc)
3. How long have you had an Aadhaar card for?
4. How did you find out that you needed to link your benefits with Aadhaar?

5. Has Aadhaar worked for you?

6. Have you noticed a difference in the delivery of your welfare benefits?

7. Has the linking been successful, did it help you receive the benefits you are eligible for?

8. Are you concerned that the government has access to your data?

9. Overall, do you like Aadhaar? Why or why not?

During this time, 99 individuals were interviewed from the four neighborhoods in Mumbai. The sample size of participants was principally determined by my time constraints. The study did not target specific demographic groups, and did not record factors such as gender, age, caste, and economic status. Instead the study interviewed individuals who were available to participate at the given time. Each interview was approximately ten to twenty minutes long, depending on how much the study participant elaborated upon the questions in the survey. This specifically involved a section that was open-ended, in order for study participants to describe more in detail about how they felt about or experienced Aadhaar.

Data Management

The survey results and field notes were transcribed, and later converted into an excel document. The survey results were then analyzed. Question 5 - “Has Aadhaar worked for you?” generated the longest responses and therefore was coded based on themes present in the response. The possible codes were “Inconvenient”, “Convenient”, “Secure”, “Consistent”, “Linking”, “Fingerprint”, “Enrollment”, “Connection”, and “Migration”. Responses could have multiple
codes depending on the content. The codes helped organize question 5’s data and provide a more thorough analysis. All notes were recorded in English.

Data Analysis

The World Bank published a declaration, *Principles on Identification for Sustainable Development: toward the Digital Age* which identifies a set of common Principles “fundamental to maximizing the benefits of identification systems for sustainable development while mitigating many of the risks” (Principles on Identification, 2017). Essentially, the World Bank and supporting organizations compiled a list of standards that identification systems should meet in order to establish an effective identification system which promotes development. It establishes ten principles, divided into three categories, inclusion, design, and governance (Principles on Identification, 2017):

Inclusion:

1. Ensuring universal coverage for individuals from birth to death, free from discrimination
2. Removing barriers to access and usage and disparities in the availability of information and technology.

Design:

3. Establishing a robust—unique, secure, and accurate—identity.
4. Creating a platform that is interoperable and responsive to the needs of various users.
5. Using open standards and ensuring vendor and technology neutrality.
6. Protecting user privacy and control through system design.
7. Planning for financial and operational sustainability without compromising accessibility.

Governance:

8. Safeguarding data privacy, security, and user rights through a comprehensive legal and regulatory framework.

9. Establishing clear institutional mandates and accountability.

10. Enforcing legal and trust frameworks through independent oversight and adjudication of grievances.

This study uses these Principles as an objective, third party set of standards which identification systems should achieve. The Principles will serve as a framework to organize and analyze the data collected through the survey, and ultimately address the questions posed in the literature review. This study seeks to analyze the ways in which Aadhaar meets the expectations from the Principles on Identification, from the perspective of and information provided by the Aadhaar users. This paper will analyze the data as it relates to each principle. Due to this study’s focus on the user’s response to Aadhaar, it does not have the scope to provide an analysis of high level systematic design principles. Therefore, this study will focus on Principles 1, 2, 3, 4, 8 and 10.
Analysis

Inclusion

The World Bank’s *Principles on Identification for Sustainable Development: Toward the Digital Age*, first focuses on inclusion of individuals in identification systems. It states, “Identification systems should strive for continuous universal coverage from birth to death, free from discrimination and accessible to all individuals” (Principles on Identification, 2017). It divides inclusion into two categories, universal coverage and accessibility.

Universal Coverage

The World Bank defines universal coverage as covering individuals from birth to death, free from discrimination (Principles on Identification, 2017). The first principle of universal coverage is divided into two criteria (1) universality and (2) non-discrimination (Principles on Identification, 2017). First, the report asserts that systems must be universal, in that all residents, not just citizens, from birth to death, should be able to enroll in the system (Principles on Identification, 2017). Second, systems must be non-discriminatory, in that legal, procedural and social barriers to enroll in and use identification systems should be identified and mitigated, with special attention to poor people and groups who may be at risk of exclusion for culture, political, or other reasons (Principles on Identification, 2017). Additionally, identification systems should not be used as a tool for discrimination or infringe on individual or collective rights. This section
will use the World Bank’s definition of universal coverage to analyze Aadhaar’s efforts in enrolling all Indian residents.

Universality/Non-discrimination:

Nandan Nilekani, the co-founder of Infosys Technologies, and the chief programmer of the Aadhaar programme, created Aadhaar, a universal identification document for every Indian resident, with the stated intention of improving delivery of public services and targeting those public services more accurately (Das, 2015). He also saw Aadhaar as a means to ensure a basic right - the right to ‘an acknowledged existence’ in India (Das, 2015). Nilekani believed that without an identity, many of the nation’s poor would be nameless and ignored, and governments could draw a veil over large-scale poverty and destitution (Das, 2015). By officially acknowledging the existence of each citizen, the state is compelled to improve the quality of services, and citizens are provided better access to state-sponsored benefits. He asserted that the recognition would provide all individuals a greater understanding and awareness of their rights, entitlements, and their duties (Das, 2015). Other government agencies had proposed a universal ID for India in that past, however Nilekani’s idea was different in that it framed the identification for each citizen as a human right and emphasized its capacity to benefit India’s poor. This idea passed, and India established the Unique Identification Authority of India (UIDAI) as a government agency to bring Nilekani’s idea to fruition.

Therefore, from the beginning Aadhaar prioritized inclusion of all citizens, but especially targeted the poor. In 2010, the UIDAI first began enrolling Indian residents in Aadhaar, and in the span of less than ten years, 1.2 billion residents have enrolled in Aadhaar, nearly 90 percent
of all adults throughout India (State of Aadhaar, 2018). The UIDAI achieved this high level of reach by setting up a strong and thorough enrollment strategy. Due to the scale and diversity of the population of India, creating a system that is non-discriminatory, intentional or unintentional, presents a challenging task.

The enrollment ecosystem of Aadhaar used a tiered model of Registrars and Enrollment Agencies. The UIDAI partnered with various Registrars, entities recognized for the purpose of enrolling residents. Often these were government agencies, such as welfare distribution agencies, central or state governments, banks, or public sector organizations (State of Aadhaar, 2017). The Registrars then contracted Enrollment Agencies to facilitate the actual enrollment process. In May 2017, there were 113 Registrars and 482 Enrollment Agencies (State of Aadhaar, 2017).

The UIDAI claims its approach to enrollment through Aadhaar is pro-rural and pro-poor (Das, 2015). By partnering with specific government agencies with large rural networks and significant bases among the poor, such as MGNREGS, PDS, and social security pension schemes, the UIDAI was able to reach the individuals that benefit from these services. The UIDAI also created a specific agenda to incorporate “hard-to-reach” groups such as the urban poor, often cited as the most ignored and disadvantaged demographic in India (Das, 2015). This is largely because the urban poor often consists of migrant workers with temporary or seasonal jobs. They addressed this by collaborating with heads of family or businesses who employ co-residents (maids, drivers, or workers), financial institutions, and NGOs. They presented similar initiatives for children, women, differently abled people, and tribal populations (Das, 2015).
The 2017-2018 State of Aadhaar Report, which analyzes data from Rajasthan, Andhra Pradesh, and West Bengal, found that Aadhaar not only had a low exclusion rate, less than ten percent, but that it also was not systematically biased against the poor or vulnerable (State of Aadhaar, 2018). This demonstrates the general success of the enrollment strategy, in that it seems to have largely achieved its goals.

This study surveyed 99 individuals, all of whom would be classified as urban poor, and 95 of those participants were enrolled in Aadhaar. This demonstrates a high successful enrollment rate. When asked where they learned about enrollment for Aadhaar (they could indicate multiple sources of information): 52 participants heard about Aadhaar from the enrollment camps in their localities, 39 from neighbors and the community, 30 from Whatsapp groups and messages, 15 from the news and radio, 8 from their work, 7 from government benefits, and 7 from schools. These results emphasize the influence of the community and word of mouth in dispersing the knowledge and awareness of Aadhaar. The enrollment camps that came to localities had significant reach into the community, and second to the camps was information from family, neighbors, and friends through WhatsApp.

Despite the high enrollment rate, four individuals were unable to enroll, and therefore completely excluded from the system. Three of these individuals indicated specific challenges in accessing the enrollment camps, and were consequently unable to participate in Aadhaar. These inhibitors came in the form of individual and situational circumstances. One woman was illiterate, and she
was therefore unable to enroll for Aadhaar on her own. Her husband works and thus he was unable to go with her to help her get enrolled during the workday. They also had a baby, and she said it was too inconvenient for her to leave during the day. Her husband had an Aadhaar card, so it is unclear why she could not have gone with him when he originally enrolled. The couple did not seem concerned about her lack of an Aadhaar card, so maybe it was simply not a priority for their family. Because the woman did not have an Aadhaar card, the husband picked up the rations every week, as the rations are distributed on a per-family basis.

Two individuals could not enroll due to mobility restrictions. One woman was elderly and she lived with her family. Due to her physical state, she felt it was too hard to go to the camp to enroll in Aadhaar. Because she lives with her family, they are able to collect her rations for her. The fact that she does not have an Aadhaar card makes her entirely reliant on her family to take care of her. In her case, she was able to rely on her family to take care of her, however those without families do not have another option with Aadhaar. Another woman was elderly, and she was interviewed on a chair in the hallway of her apartment building where she was encountered. She was unable to move well, and her neighbor helped her to participate in the study. She lived on the third floor of her apartment building and was unable to get to the enrollment camp to register for Aadhaar. However, even if she had been able to register, she could not individually go shopping for herself to get her rations. Her neighbor buys her groceries weekly, and helps to take care of her. Her neighbor used to pick up her rations, but now with Aadhaar, she is unable to. This means she is excluded from the PDS services. The very attributes that make Aadhaar secure and regulated, in this case biometrics, exclude those who are unable to travel themselves
to collect the rations. This prompts the question of how Aadhaar includes those that cannot personally go to the ration store. This is less relevant for individuals with families, in that their direct family members can be registered on the same account as them and can therefore collect the rations on their behalf. However, individuals that live alone do not have this option.

The fourth individual faced enrollment processing challenges, in which she submitted paperwork to register herself, her husband, and her children. Her children were officially registered in Aadhaar, however she and her husband were not. She resubmitted the paperwork multiple times, however they never heard back from the UIDAI. She was unable to discover the status of her application and that of her husband, and she could not get a clear answer as to what went wrong. Because she and her husband could not register for an Aadhaar, they did not have the ability to pick up their rations. Therefore, her children had to collect the rations on their behalf. She expressed significant frustration in the process. She felt that she carefully followed the instructions of the UIDAI in order to obtain an Aadhaar card, and she was still excluded.

This study did not record demographic factors such as economic status, ethnicity, or age, and therefore, it cannot speak to systematic discrimination of specific groups. However, from these anecdotes, age, disability, living alone and illiteracy presented barriers to entry for three individuals. Despite efforts from the UIDAI to enroll all individuals, including “hard-to-reach” groups, some individuals are still excluded from the system due to situational factors. Therefore, while Aadhaar has high enrollment rates, it does not perfectly achieve the criteria provided by the World Bank for universal coverage.
Accessibility

Direct and indirect costs

The second principle focuses on ensuring accessibility to the system. It separates accessibility considerations into two categories (1) removing direct and indirect costs and (2) mitigating information and technology disparities.

Due to Aadhaar’s goal to include all populations, including poor and hard-to-reach populations, the UIDAI took measures to reduce entry barriers to Aadhaar in an effort to make enrollment and use of Aadhaar accessible and convenient to individuals. These measures include:

1. All Indian residents are entitled to an Aadhaar card free of cost.
2. Aadhaar employs a decentralised enrollment system that makes use of multiple Enrollment Centres and outreach efforts.
3. They accept eighteen proofs-of-identity and thirty-six proofs-of-address, in order to make the process as flexible as possible. For individuals lacking documentation, there are alternate means of enrollment.
4. Individuals who have incomplete biometrics, including undetectable fingerprints or iris scans (due to disability or age) are still eligible to enroll. No individual can be denied because they do not possess usable biometrics.

(State of Aadhaar, 2017).
The State of Aadhaar report found that despite the official statement that all residents are entitled to an Aadhaar card free of cost, 23.7 percent of people in Rajasthan indicated that they paid to enroll in Aadhaar, 9 percent in Andhra Pradesh, and 5.7 percent in West Bengal (State of Aadhaar, 2018). Despite cases of charging unnecessary fees and failed enrollment, the majority still found the enrollment process to be “easy” (State of Aadhaar, 2018). The variation in the number of cases by state that deviated from the national policy of enrollment free of cost emphasizes the decentralization of the system. While the UIDAI organized the process, individual states and government agencies are responsible for implementing the system. Depending on the level of engagement and oversight of the process, different states have had different experiences in enrollment. At times these variations are miniscule, and at times they are drastic. For example, in Assam, the enrollment rate is merely 10.1 percent (State of Aadhaar, 2019). This is drastically different from Andhra Pradesh’s 99.8 percent enrollment. It is unclear why these rates are so different, however management of enrollment and specific state-based barriers to entry are likely responsible.

This study interviewed individuals in different localities within Mumbai, and it therefore did not address geographical differences in implementation. However, the vast majority of individuals enrolled through enrollment camps that came to their neighborhoods. With the exception of the four individuals who were unable to enroll, the participants generally felt that it was easy to enroll, although one mentioned long lines and wait times to register. However, the stories of the three individuals who were unable to enroll, two due to age, and the third due to illiteracy and maternal responsibilities, emphasize the important indirect costs of enrolling. For the two elderly
women, the cost of physically going to the enrollment agency was too high and outweighed the benefits of obtaining an Aadhaar card. For the new mother who was illiterate, the indirect cost of enrolling for Aadhaar was the time and effort that it would take to go to the Enrollment Centre. The demands of childcare presents a significant barrier for some mothers, as it is unrealistic for them to leave their children. If Aadhaar truly eliminated the direct and indirect costs, then there would not be individuals who responded this way. Therefore, while Aadhaar has made significant efforts to reduce the costs associated with enrolling for Aadhaar, it still struggles to reach everyone.

Information and technology disparities

The second component of achieving accessibility is filling information and technology disparities, specifically regarding information asymmetries with digital systems, connectivity, and technical knowledge. While this study did not encounter individuals who were unable to accustom themselves to the Aadhaar system, participants did indicate connectivity and power challenges. In order to authenticate individuals, the Aadhaar machine requires both internet connection and power. This is challenging for localities that have difficulty receiving internet connection or experience frequent power outages.

In this study, two participants indicated challenges in authenticating themselves due to internet connectivity and power outages. One individual claimed that Aadhaar works for him most of the time. However, if there is poor internet connection when he goes to the ration shop, he is unable to authenticate himself with the scanner, and therefore, he cannot pick up his rations. He clarified that it does not happen often, but when it does, it is inconvenient. Another participant echoe
similar sentiment. She said that sometimes the system does not function well if the power is out or the connection is poor. She has no choice but to leave and come back at a later time. In speaking with a ration shop owner, similar challenges were stated. He said that when the connection is poor or there is no power, he is unable to enact transactions because the machine does not function. Whereas previously, he could continue his business by authenticating individuals manually with their documents, and then taking a written record, now his business is completely halted depending on the connectivity. This directly contradicts the description of the second principle, which states “Stakeholders should work together to ensure both online and offline infrastructure can be extended to provide ‘last-mile’ access and connectivity, particularly for those in rural areas” (Principles on Identification, 2017). Because Aadhaar is entirely dependent upon internet connectivity, it excludes those without consistent internet connection, therefore reinforcing information and technology disparities.

While universal coverage and total accessibility is an area in which Aadhaar can improve in terms of inclusion, the report’s assumption that (1) universality and total accessibility are possible and (2) are ideal characteristics should be questioned. While universality, or the identification to all residents, is a goal, it is unclear if this standard is realistic or likely. With a country of 1.3 billion people, it is challenging to ensure that every single individual is accounted for. Aadhaar has made incredible strides towards this goal, but studies continue to show the existence of exclusion. This ties into the second question of whether universality should be the end goal of biometric identification systems. The more accurate a system becomes, the more people rely exclusively on the system. As the government and people assume that a system
works well, they provide less attention to the cases that do not work (Mordini, 2007). This argues that the level of exclusion becomes significantly more comprehensive, the more effective and accepted the system. This therefore emphasizes not the universality of the system, but instead the existence of an effective exception handling system (Biometrics at the Frontiers, 2005). The European Commission Joint Research Centre advocates for the need of exception handling in biometric identification systems in its statement “We shall have to consider exception handling processes for individuals who have difficulty with automated processes … The impact [of disenfranchisement from people excluded] will depend upon how well such factors have been considered in advance, together with the nature and practical delivery of associated exception handling processes (Biometrics at the Frontiers, 2005). Following this thinking, it is not sufficient for an identification system to simply be universal and non-discriminatory. This does not account for inevitable problems which could occur within the system, technical challenges, unenrolled individuals, etc., and instead it further excludes these individuals, consequently discriminating against certain individuals. Therefore, states can try to achieve universality, but high enrollment rates should not lead states to assume that universality is the reality. They must also establish official policies and procedures, that are effective, to account for scenarios when the identification system fails. This is essential in preventing discrimination of individuals.
Design

The third section of the *Principles on Identification* document provides standards for system design, in which it posits that systems should be robust, secure, responsive, and sustainable. It lists five principles: (3) establishing a robust - unique, secure, and accurate - identity, (4) creating a platform that is interoperable and responsive to the needs of various users, (5) using open standards and ensuring vendor and technology neutrality (6) protecting user privacy and control through system design, (7) planning for financial and operational sustainability without compromising accessibility (Principles on Identification, 2017). Due to this study’s focus on the user’s response to Aadhaar, it does not have the scope to provide an analysis of high level systematic design principles. Therefore, this chapter will focus on Principles 3 and 4.

Establishing a robust - unique, secure, and accurate - identity

The third principle in the *Principles on Identification* document is the establishment of a robust identity (Principles on Identification, 2017). It defines robust, in terms of identity, as a system that is unique, secure, and accurate. It considers identification systems *unique*, when they are able to provide a statistically unique and verifiable identity for the course of an individual’s life, from birth to death. It considers a system *secure* when it has safeguards against tampering (alteration or other unauthorized changes to data or credentials), identity theft and other errors occurring throughout the identity lifecycle. Finally, it considers systems as *accurate* when they provide up-to-date information essential for the trustworthiness of any identification database and credentials used for authentication (Principles on Identification, 2017). This section will use
the World Bank’s criteria of unique, secure, and accurate, to analyze the ways in which Aadhaar has established a robust system, and the ways in which the system design needs to improve.

Unique

The Aadhaar card is a national identification card, that includes both demographic and biometric data. The demographic information involves personal details such as name, father/mother’s name, date of birth, sex, and address (Raju, 2017). The biometric information includes a photograph, fingerprints, and iris details. There is also a Quick Response (QR) code which corresponds to each individual’s twelve-digit unique identity number (Raju, 2017). The UIDAI selected fingerprints as the common form of biometrics to be used for everyday authentication based on their ability to produce unique and consistent results.

Automatic fingerprint identification systems (AFIS) scan the friction ridges that cover the fingertips and classify patterns of minutiae such as branches and end points of the ridges (Anderson, 2008). There are three major fingerprint features: the arch, loop and whorl (Biometrics at the Frontiers, 2005). Each finger has at least one major feature (Biometrics at the Frontiers, 2005). Because fingerprints are unique to each individual, when read correctly, they are an effective method for identification. The seven pillars of biometrics offer a criteria which biometrics should meet in order to be effective in large scale implementation. Fingerprints fulfill many of the requirements. Nearly all humans possess fingerprints, with the exception of hand related disabilities, therefore making fingerprints almost universal. Fingerprints are distinctive, in that they are unique to each individual, and the details are generally permanent, however sometimes fingerprints can change due to intense friction on the fingerprints. Additionally,
fingerprints have strong collectability through fingerprint scanners. The AFIS generally offer good performance. Fingerprints have been associated with criminal recognition in the past, however people’s perceptions are beginning to change, therefore increasing its societal acceptability. As the technology improves, with more effective cryptography, fingerprint systems are increasingly more difficult to circumvent (Biometrics at the Frontiers, 2005).

While fingerprints perform better than most other forms of biometrics when considering the seven pillars, there are still significant challenges when implementing fingerprints on a large scale. Primarily, disabilities or work conditions can cause deformations in fingerprints, making them undetectable by the scanners (Biometrics at the Frontiers, 2005). One study estimated that five percent of individuals would not be able to register and produce a detectable fingerprint (Biometrics at the Frontiers, 2005). This is especially important to consider when evaluating state-wide identification systems which include millions, and sometimes billions, of people.

This study found that biometric authentication worked for 95 of the 99 participants. 56 of the 95 individuals stated that they liked the Aadhaar system. These statistics present a promising evaluation of the “uniqueness” of Aadhaar, in that it is able to correctly verify the vast majority of individual’s identities. However, for those that it did not work for, there is no alternative system.

I spoke with three individuals who expressed challenges with fingerprint authentication through Aadhaar. One individual indicated that their fingerprints were undetectable by the machine. She
was able to register for Aadhaar, however when she goes to the ration shop to authenticate themselves, her fingerprints do not scan properly. This excludes her from collecting her ration, and her husband and children must collect the ration for her. However, she expressed that this was inefficient because her husband works during business hours and her children go to school. They make it work, but it is less convenient than if she was able to access the rations. This emphasizes that Aadhaar does not provide a unique/verifiable identity for an individual.

The other two of the three previously mentioned participants expressed sporadic challenges with the fingerprint scanner. One individual said that the machine often rejects his fingerprints. One time, it did not work after many attempts. Generally, he is able to get it to work, but he has to try it a few times. He found this frustrating because previously he could present physical documents, which were considered sufficient. Another participant told a similar story, in which the machine accepted his fingerprints, but sometimes only after multiple tries. For these three individuals, Aadhaar is unable to verify their identity, therefore failing the “unique” category for a small minority.

Even as technology improves, there will likely always be some that will be undetectable by fingerprint scanners. Many of those who are more likely to have difficulty - infants, the elderly, and manual laborers - are often already marginalized (Gelb, 2013). In this capacity, biometrics can lead to further exclusion. Similar to the statements from chapter one, the stronger the system and the fewer the errors, the greater the assumption that the computer is correct and the individual is wrong (Gelb, 2013). Greater reliability on a system leads to more intense exclusion.
Therefore, studies emphasize the necessity of defining clear processes and standards for resolving errors and identity disputes (Gelb, 2013). This is poorly and inefficiently implemented in Aadhaar.

In the case of Aadhaar, each state is responsible for designing its own alternative to fingerprint authentication (Aadhaar Act, 2016). In Maharashtra, the setting of this study, if individuals are unable to be authenticated with the fingerprint scanner, they must call a designated official who is assigned to that specific locality. The official travels to the ration shop, evaluates the documents of the individual, and then overrides the system by permitting dispersal of the rations. One individual whose fingerprints did not work with the Aadhaar machine expressed frustration with the system. She claimed that this process was inefficient and unrealistic. She called this official a few times, and one time he arrived hours after the call, and the other times he never arrived. She found it more effective to send her kids to pick up the ration than to call the official. A similar sentiment was expressed by a ration shop owner in the Dharavi locality. He said that if the scanner cannot detect one’s fingerprints, they have no alternative. He did not consider the appointed official a viable alternative due to its ineffectiveness. This could be a result of the location of the study. Mumbai is a highly populated and crowded city with significant traffic delays. Therefore, this system could be even more inefficient given the context. Maybe the process is more effective in smaller cities or rural areas, where the official has fewer ration shops to attend to. Regardless, whether this is an issue unique to cities or not, it needs to be addressed in order to assure unique identification to all. If an individual’s fingerprints do not work, this is
currently the only legal alternative. This necessitates the establishment of an effective alternative that people can realistically use.

Secure

The second criterion for a robust identification system is that the system must be secure and resistant to identity theft and other errors. India’s Public Distribution System (PDS) previously struggled immensely with corruption and leakages, due to misidentification and lack of regulation of users. This section will address the ways in which Aadhaar has increased accountability and security of rations through more effective identification.

Food security presents a major problem in India, where 190 million people were reported undernourished in 2016, the highest of any single country (George, 2019). India established the PDS system in 1992, in an effort to combat the severe burden of malnutrition within its population. In 1997, PDS evolved into TPDS (Targeted Public Distribution System), which specifically targeted individuals below the poverty line (Khera, 2011). PDS of India plays a crucial role in reducing food insecurity by distributing essentials, such as wheat, rice, sugar, and kerosene, to those with demonstrated need at a subsidised rate (George, 2019). PDS theoretically provides food and fuel to two thirds of households in India (Varadharajan, 2013), however there are many concerns of mis-targeting, under-coverage, and corruption, which lead to major leakages in the food supply (Varadharajan, 2013). In 2009/2010, 41 percent of the food grain obtained by states did not reach the beneficiaries (Varadharajan, 2013). While this had lowered from 54 percent in 2004/2005, it exposes devastating inefficiencies in the PDS system. A study in Tamil Nadu estimated that for every 5.43 kilograms of PDS rice distributed by the
government, only 1 kilogram reached those in need (George, 2019). Another study conducted in Rajasthan found that people rarely received their full entitlement of rations, and they were often cheated by the PDS dealer (Khera, 2011). Because individuals were unable to access their full entitlement of the goods, they were forced to buy grains from the free market without any government assisted subsidy. Two predominant challenges contribute to the failures of PDS: (1) misclassification of the poor and (2) leakage of food grains during transportation to the ration shop (Balani, 2013).

Identification is an essential component of the PDS, in that in order to work effectively, the system must correctly identify the individuals who are eligible for the benefits and exclude those who are ineligible. However, studies show that targeting mechanisms such as TPDS are prone to significant inclusion and exclusion errors, meaning those that need it are denied, and those that are not eligible obtain the benefits (Balani, 2013). When establishing which families were considered “below poverty line” (BPL) and “above poverty line” (APL), an advising group of the ministry of Rural Development estimated that 61 percent of the eligible population was incorrectly excluded from the BPL census, and 25 percent of APL individuals were included in the BPL list (Balani, 2013). This means a significant portion of the TPDS benefits are directed at the incorrect population. Other identification challenges come with authentication of established beneficiaries. Ghost cards, duplicated members, or false cards also contribute to the diversion of benefits from the eligible individuals (Dhanaraj, 2012). This impact of fake cards is evident in one study’s findings, in which the ration card database shows 83.7 million users, while the population of the state according to the Census of 2011 is 72.1 million (Dhanaraj, 2012). It is
presumed that the additional 11.6 million accounts are fraudulent accounts, each of which receives Rs. 2400. This is only one state - if the numbers nationally follow this, the financial losses are exorbitant (Dhanaraj, 2012).

Additionally, the TPDS procurement and distribution process involves multiple steps, with change of oversight, and therefore, presents multiple opportunities for leakages or corruption. The provision of TPDS food grains falls under the joint responsibility of state and central governments (Balani, 2013). The Food Corporation of India (FCI), acts as the central agency responsible for facilitating the distribution (George, 2019). It collects food grains from farmers, at a higher price than market price, called the “minimum support price” (Balani, 2013). Then, the individual state governments procure the food grains at a subsidised price known as the “central issue price” from the FCI. The FCI distributes the goods to the states, and then the states are responsible for distributing the goods to the individuals fair price shops or ration shops (George, 2019).

The Government of India recognized the major flaws in the PDS system and saw Aadhaar as a way to reform the system. The UIDAI identified the following critical elements in the implementation of TPDS that need reform:

1. Beneficiary identification, addressing inclusion/exclusion errors
2. Addressing diversions and leakages
3. Managing foodgrain storage and ensuring timely distribution
4. Effective accountability and monitoring, and enabling community monitoring
5. Mechanisms for grievance redressal

6. Ensuring food security (UIDAI 2010 c:4)

Primarily, Aadhaar prevents the creation of ghost accounts due to the fact that it is a unique number including biometrics, which prevents residents from having duplicate accounts (Das, 2013). Therefore, using Aadhaar to identify beneficiaries would eliminate duplicates and fake beneficiaries in order to deliver the benefits to the eligible users (Das, 2013). Also, Aadhaar allows electronic benefit transfers (EBTs), which enable governments to send financial benefits electronically to residents, therefore, directly delivering the money to those who need it.

In order to combat leakages and diversion, Aadhaar offers a way to track foodgrain movement exchanged by the TPDS intermediaries (Das, 2013). Implementation of Aadhaar authentication at every exchange point, across the supply chain, would allow the government to regulate and track the movement of the foodgrain, therefore reducing leakages in the various stages of transportation. Additionally, Aadhaar increases the fair price shops accountability by requiring Aadhaar authentication every time the beneficiary collects the entitlement (Das, 2013). This ensures that the shop owner must clearly account for the offtake claimed by the beneficiary. In theory, Aadhaar increases accountability and regulation on a systematic level, in an effort to reduce the leakages previously prevalent in the system.

However, there is a less clear conclusion as to whether increased accountability and regulation through Aadhaar has made the desired changes in practice. One study reported that Aadhaar had significantly cut the fake accounts by deleting 940,000 ‘fake’ accounts (Khera, 2017). However,
when investigated, only 12.6 percent of those accounts were actually classified as ‘fake’ or ‘duplicate’. The remainders were deleted for other reasons, such as changes of address, surrender of a job card, etc. (Khera, 2017). Therefore, it is challenging to estimate accurately the impact of Aadhaar on reduction of leakages.

In this study, 12 individuals indicated that they feel that their rations are more secure with Aadhaar than without it. Eight of the twelve individuals which indicated that their rations were more secure with Aadhaar answered this because they felt that Aadhaar was a more secure method of authentication than the previous system. One woman explained that she felt Aadhaar was a more reliable system. Instead of depending on the ration owner to authenticate her identity, the technology does it. Therefore, Aadhaar removes the responsibility of authenticating individuals from the ration shop owners, and puts it on the technology. The hope is that the technology is a less biased and purely objective mechanism to authenticate individuals. Another woman expressed that Aadhaar was more secure because the implementation of biometrics ensure that she is the only person who can correctly match her account. She felt that no one could pretend to be her and unfairly take her ration. The other participants echoed these sentiments, claiming that with Aadhaar, no one could steal their identity or services.

Four of the twelve not only felt that Aadhaar was a more secure method of authentication, but have seen the effects in more accurate ration amounts. One man felt that he received more consistent rations after Aadhaar. Previously, he did not receive the correct weight of grain for which he was eligible. However, with Aadhaar, he now receives the exact amount he is promised
by the state. Another woman expressed similar sentiments, in that she feels her rations are more predictable with Aadhaar. She gets the same amount every time, and she believes that Aadhaar provides accountability to the ration shop owners to give the correct amount. Consequently, these twelve individuals felt that Aadhaar was a positive contribution to the TPDS system.

Because Aadhaar increased accountability in nearly every stage of the PDS distribution process, it is challenging to pinpoint the source of the claims of more accurate ration amounts. It could be that there is less leakage present in the distribution process due to greater regulation and tracking, and therefore the ration shop owners receive sufficient food and grains to provide the correct amounts to their beneficiaries. Significant reduction in ghost and fraudulent accounts could also reduce the leakage of goods, and guarantee that the rations are available for the intended beneficiaries. Or, with Aadhaar, the government can more efficiently track inventory of the ration shops, therefore ensuring that the ration shop owners do not cheat their customers by only giving a portion of their government issued ration. Other studies, in addition to the insights from this study, suggest that it is some combination of all of them. However, while it is unclear exactly which part of the process improved on a systematic level, this study found that some of the beneficiaries themselves directly felt the positive effects. Therefore, this seems to satisfy the secure criteria.

Accurate

The third criteria necessary for a robust identification system is accurate, up-to-date information. This section will discuss the extent to which Aadhaar is able to provide a database of valid users and credentials for authentication. One of UIDAI’s original goals with Aadhaar was to reduce
the identification database to existing individuals without duplicates (Das, 2015). The nature of Aadhaar prevents duplicates or fraud accounts in theory due to the integration of biometrics in the system. For example, an individual cannot register twice, as their biometrics are already in the system. Or an individual cannot register under the name of another, because their biometrics will not match. The State of Aadhaar report discusses Aadhaar seeding as a method for removing duplicate and fake entries from databases (State of Aadhaar, 2018). It found that after Aadhaar there has been a 72 to 82 percent increase in percentage of seeded PDS beneficiary households across all states in India (State of Aadhaar, 2018). While this is still not perfect, Aadhaar has increased the accuracy of the system.

This study did not specifically study the accuracy of Aadhaar. The survey did not encounter cases of individuals whose accounts had been duplicated. But even if an individual’s account was duplicated, they may not be aware. As discussed above, the participants’ belief that their rations were more secure because others were unable to take their rations seems to reflect a reduction in ghost accounts, and therefore a more accurate system. However, because this study did not receive conclusive information regarding accuracy, this study cannot make assertions regarding the accuracy of Aadhaar.

Interoperable and responsive platform

The fourth principle in the Principles on Identification, advocates for the need to create a platform that is (1) responsive to the needs of various users and (2) interoperable. It defines responsiveness as a system in which the services are flexible, scalable, and meet the needs and
concerns of end-users or individuals (Principles on Identification, 2017). It should also meet the
needs of public agencies and private companies that use - or could use - this identity as a
foundation for other services or operations (Principles on Identification, 2017). It defines
interoperability as the ability to increase efficiency and allow multiple stakeholders to leverage
the benefits of the identification system, both within a country and across borders. It specifies
that domestically, this includes the ability of different databases or registries to communicate
with each other and/or exchange information in a timely and low-cost manner, subject to
appropriate privacy and security safeguards (Principles on Identification, 2017).
This section will analyze the ways in which Aadhaar is interoperable and responsive to the needs
of the users.

Responsiveness

The World Bank report identifies responsive systems as those which are flexible, scalable, and
meet the needs and concerns of end-users. This study does not have sufficient data to discuss
flexibility and scalability, and therefore it will focus on meeting the needs and concerns of
end-users. The UIDAI designed Aadhaar to document those who were previously undocumented
and to reduce corruption and leakages in the PDS system (Das, 2015). Documenting its citizens
and reducing expenditures on the PDS fulfill national goals. However, the literature of Aadhaar
continuously refers to identity as a human right (Das, 2015). Nilekani’s vision emphasizes the
ways in which Aadhaar will help the poor - namely in improving access to government services
and providing opportunities for inclusion in essential private sector activities (Das, 2015; Gelb,
2013). This demonstrates the effort by the UIDAI to meet the needs of the individual. This
section will analyze whether Aadhaar actually does meet the needs of the individual, or if some
users feel that they have been ignored. This study will specifically address whether Aadhaar is more convenient for users, and whether Aadhaar has helped users achieve financial inclusion - two needs of the user.

Before Aadhaar, the government had multiple different forms of identification for specific populations and various purposes (Srijoni, 2019). These included the electoral identity card, the income-tax PAN card, the ration book, the birth certificate, and the drivers licence. No single card was universally accepted for all public and private services. This presented multiple challenges for the government. At a high level, the system was not centralized, and therefore it was harder for agencies and services to confirm a beneficiary’s identity (Das, 2015). Aadhaar offers a universal number, and agencies and services can contact the central UID database from anywhere in the county, to confirm any individual’s identity (Das, 2015). This is significantly more convenient for both the state and the implementers. A universal ID also helps to standardize systems throughout the country. This is important given the scale and diversity of India - a country with over one billion people, 29 states, and 22 major languages. Aadhaar helps to create a singular and central portal that the government can control uniformly throughout the country.

The advantages in convenience for the state are clear and often cited. Aadhaar also presents a more convenient option for individuals. Due to the existence of multiple different types of documents for identification, individuals needed to present the correct card depending on the service (Srijoni, 2019). The abundance of documents created inconveniences for individuals to
receive their government services, as they often had to present and keep track of multiple
documents at a time. Additionally, with an already high number of individuals without
government identity documents throughout the country, this created more barriers to entry for
individuals who did not have IDs. Therefore, Aadhaar offers a solution to this, by creating a
platform in which residents can easily establish their identity, wherever they are in the country
(Das, 2015). This means that residents can use the same card for multiple services, from opening
a bank account to picking up weekly rations. It also theoretically allows users to access PDS
benefits from anywhere in the country because every shop will use the same system.

In this study, participants were asked: “Does Aadhaar work for you?” and “Does Aadhaar make
a difference in the way you receive your government services?” Fifteen participants,
representing approximately fifteen percent of the total individuals, indicated that they found
retrieval of PDS services to be more convenient with Aadhaar.

The majority of individuals which indicated that Aadhaar made the PDS collection process more
convenient, said so because they now have to bring fewer documents to the ration shops.
Previously, in order for individuals to authenticate themselves at the ration shop, they had to
bring multiple documents each visit. However, now with Aadhaar, individuals only need to bring
their Aadhaar card and their ration book. Fourteen people found this to be more convenient than
the previous system. Three individuals found the system so convenient that they wished more
services, even voting, could be connected to Aadhaar.
One individual used Aadhaar for PDS services, and she had linked it to additional government services as well, including health care. Once she became ill, and she was admitted to the hospital. Because her Aadhaar was linked to her health insurance, she only had to provide her fingerprint and Aadhaar card in order for the hospital to register her. With access to her Aadhaar card, the hospital was automatically able to apply the government benefits to her visit and know how much she would pay out of pocket. She was especially impressed by this result. According to her, it would have been more complicated, or at the very least slower, prior to Aadhaar. She mentioned that Aadhaar remediated external stresses from an already stressful situation.

Despite the positive reports, thirteen individuals found Aadhaar to be inconvenient. They cited varying reasons which have made collection of government welfare benefits less convenient. Three individuals discussed inconveniences with the fingerprint detection technology. They claimed that at times, the reader cannot detect their fingerprints, and it takes multiple tries. While it is usually able to work eventually, one individual claimed that previously he could present his PAN card as a method of identification, but now if his fingerprints do not work, there is not an alternative. Three individuals expressed challenges with internet connection and the functionality of the Aadhaar scanner without proper service. One explained that when the power is out or the connection is poor, the machine does not work. If this happens when he arrives at the ration store, he has to return to his house and come back at a later time. While it does not happen consistently, when it does occur, he finds it to be very inconvenient. Four others cited inconveniences with accessibility. Two women were elderly and were unable to travel to the enrolment center, therefore, they could not receive their benefits. Another woman was illiterate,
and consequently, she could not enrol without her husband. Because her husband worked all day, she was never able to enrol. These examples showcase the inconveniences that prevent individuals from participating in Aadhaar, and therefore receive their benefits. Three other individuals cited inconveniences due to migration. They had moved to Mumbai from different villages throughout Maharashtra, and they were unable to access their benefits in Mumbai. The topic of migration is specifically interesting. One of the most significant promised conveniences of Aadhaar was that individuals would be able to access Aadhaar throughout the entire country. However, the experiences of these three individuals directly contradicts this. This underscores the importance of understanding the user experience, as not all promises and intentions function as intended.

While these 28 cases provide both positive and negative perspectives to the user experience of Aadhaar, the 71 that did not indicate any reference to convenience, good or bad, is equally as insightful. One of the most important selling points of Aadhaar is that it is more convenient, both for the user and the government. However, when asked about their experience with Aadhaar, 71 percent did not reference convenience at all. This raises the question of whether the previous system really was that inconvenient for individuals. This could mean that convenience was less important to people than the UIDAI thought. It could also reflect a lack of awareness and education regarding the Aadhaar system. When asked about their thoughts about Aadhaar, many individuals did not have opinions. To them, Aadhaar is the system that they use to receive their benefits, and nothing more. It serves its purpose because they are able to receive the benefits for which they are eligible, and that is the most important factor.
These results paint a complex picture of Aadhaar in which people experience varying levels of convenience. The majority found that Aadhaar is more convenient, however a still significant minority found the system very inconvenient and their needs are met by the system. However, the individuals for which Aadhaar is inconvenient are severely disadvantaged or excluded completely, and therefore the system does not meet their needs.

Prior to Aadhaar, India admitted various identity documents, such as the electoral identity card, the income-tax PAN card, the ration card, the birth certificate and the driving licence; however they each served a specific purpose and therefore did not provide total coverage over the entire population (Srijoni, 2019). The main justification for Aadhaar was “better inclusion”, in which the government hoped to create a centralized ID that could be used for various services (Srijoni, 2019). Prior to Aadhaar, lack of legal documentation accounted for 20 percent of exclusions in India (State of Aadhaar, 2017). By providing a proof of identity and address, the Indian government hoped that this statistic would become obsolete.

Literature demonstrates the positive relationship between access to formal financial services and economic prospects for poor individuals and communities (Cull, R., 2014). The hope was to provide documents for those who did not previously have them, which would then lead to greater financial inclusion (State of Aadhaar, 2017). While it is challenging to attribute the use of Aadhaar directly to bank account openings, the vast majority of individuals do use Aadhaar as an ID to open bank accounts (State of Aadhaar, 2018). In Andhra Pradesh, 95 percent of
participants used Aadhaar to open a bank account (State of Aadhaar, 2018). The report estimates that approximately 90 percent of the respondents that used Aadhaar to open a bank account also had another legitimate proof-of-identity document prior to obtaining Aadhaar (State of Aadhaar, 2018). Consequently, Aadhaar has served 10 percent of the respondents in opening a bank account. This is significant, especially when considering the population of India. However, given the urgency with which the UIDAI discussed Aadhaar, it does not necessarily justify the system.

This study encountered two individuals for which Aadhaar was their first identity document. Aadhaar allowed both of them to participate in essential financial activities. One man that I spoke with asserted that Aadhaar allowed him to be a citizen. Previously, he did not have an identity document, and therefore, he was excluded from many basic services. He did not have the correct documentation to register for an identity document to receive government benefits, and was consequently ineligible for rations, subsidies, and other non-governmental services such as bank accounts. With Aadhaar, he was able to purchase a phone and open a bank account, services that he was previously unable to use. He expressed gratitude to Aadhaar for connecting him to the services that are now available to him.

Another woman similarly stated that she previously did not have a document to prove her identity. Aadhaar enrolment allowed her to open a bank account, something she previously would not have been able to do. She said that this has helped her to be financially responsible and independent. This gave her a very positive experience in regards to Aadhaar, and she felt that the system is beneficial.
Therefore, Aadhaar has met the needs of the individual in that it has provided identity documents to those who previously did not have one. However its relation to convenience of access to PDS services is more complicated, in that it has improved convenience for some, while inconveniencing others.

Interoperability

The second criterion in the fourth principle is that the identity platform is interoperable, in that it allows multiple stakeholders to leverage the benefits of the identification system (Principles on Identification, 2017). Aadhaar has been both praised and criticized due to the government’s effort to link Aadhaar to both public and private services. The UIDAI includes a long list of services and can be linked with Aadhaar, including PDS food and fuel subsidies, schools, banks, SIM cards, health insurance, properties, and pensions. The diversity of services that use Aadhaar, from public to private and direct deposits to services, emphasize Aadhaar’s ability to operate with multiple stakeholders.

This study asked individuals who had Aadhaar cards, 96 individuals, which services they linked their cards to. All of the 96 participants with cards linked their Aadhaar to at least two schemes, with the most being six schemes. The most common linkages were rations, with 82 individuals; gas subsidies, with 76 individuals; SIM cards, with 68 individuals; and banks, with 65 individuals.
Three participants indicated initial challenges linking their services to Aadhaar. One man linked his Aadhaar to his gas subsidy, which through Aadhaar directly deposits into his bank account. However, his money was transferred to the incorrect bank account, so he did not receive his subsidy for five months. It took him a while to understand why he was not receiving his subsidy. He first went to the gas company, which referred him to the bank. The bank was able to resolve the issue, and he now receives government subsidies without a problem. His gas subsidy has been linked with Aadhaar for four years now. He mentioned that some of his friends have had trouble receiving subsidies even after they are correctly linked, but he does not have problems anymore. Another woman expressed a similar challenge. She had trouble linking her salary to the Aadhaar card. The direct deposits did not process the first time, but she reported the error, and it was fixed by the next month. Another woman worked as a janitor at a school, and she claimed that the school switched to salary payments through Aadhaar, however she did not yet have an Aadhaar card. Therefore, she had to link her salary to her Aadhaar. Once it was linked it worked well, however she lost that month of income. These three examples of linking challenges are all short term errors that were resolved when noticed. The linking challenges could result from the new nature of the system. Hopefully, as Aadhaar develops, such mistakes will be eliminated.

Aadhaar demonstrates a strong capability to link with multiple services, therefore serving as a central system to which other public and private entities can connect. In speaking with individuals, it is clear that there are a few challenges with the linking process, especially in establishing the first link. However, it seems that once the systems are effectively linked,
individuals generally do not face significant challenges. This affirms the interoperability of Aadhaar.
Governance

The final section focuses on effective governance to build trust by protecting privacy and user rights (Principles on Identification, 2017). It emphasizes the importance of a strong legal and operational foundation between government agencies, international organizations, and public and private actors (Principles on Identification, 2017). It also underlines privacy and data protection of users as a priority for identification systems. This governance section lists three principles: #8 Safeguarding data privacy, security, and user rights through a comprehensive legal and regulatory framework. #9 Establishing clear institutional mandates and accountability; and #10 Enforcing legal and trust frameworks through independent oversight and adjudication of grievances (Principles on Identification, 2017). This chapter will focus on Principles 8 and 10.

Data privacy, security, and user rights

The World Bank addresses the importance of data privacy and security in Principle 8. It divides this topic into two core parts (1) legal and regulatory frameworks and (2) user rights (Principles on Identification, 2017). Because this study collected data from Aadhaar users regarding their experience, this section will focus on the second criteria regarding user rights. The report defines user rights as providing individuals “the genuine choice and control over the use of their data, including the ability to selectively disclose only those attributes that are required for a particular transaction” (Principles on Identification, 2017). It also highlights the importance of efficient data correction and transparency in use of user’s data. This section will analyze participants’
responses to the study survey to understand Aadhaar’s efforts to promote data privacy, security and user rights.

Different societies and cultures view biometrics differently. In 1995, the first study investigating people’s perceptions of biometrics, conducted in the United States, found that overall, biometrics were rated significantly less acceptable than other security measures, such as passwords (Deane, F., et al 1995). A study in 2004 surveyed individuals regarding fingerprint scanning in air travel (Riley, C. et al, 2009). The majority expressed a positive attitude to the use of biometrics for air travel (Riley, C. et al, 2009). The study did find that the German participants were more supportive than the British participants, one fourth of which found the effects of biometric technology potentially concerning for their civil liberties (Riley, C. et al, 2009). The UK Passport Service biometrics enrolment trial represents one of the largest published studies of biometric technology, with over 10,000 participants (UKPS, 2005). This study indicated that most people were comfortable integrating a biometric technology with national passports (UKPS, 2005). However, one fourth of the individuals still expressed concerns about the effects of biometrics on their civil liberties (UKPS, 2005). One study conducted by a bank which implemented mandatory fingerprint scanning for new customers in the United States found that people showed less resistance than anticipated, especially if the facilitators used scanners instead of ink and paper (Anderson, 2008). While it is difficult to compare these studies, as they are distinct in their methods, the studies ultimately reach similar conclusions, that people (specifically Western individuals) recognize the value of biometrics and support the
implementation of biometrics, but a significant minority still expresses concerns regarding the implications of such a system on civil liberties.

Public reception of systematic biometric authentication with fingerprints in India tends to be more optimistic (Riley, 2009). A study which compared cultural perceptions of systematic use of biometrics in India, South Africa, and the United Kingdom, found that the majority of Indian respondents believed that biometrics were a “positive technological innovation” or that they thought biometrics would be beneficial for particular applications in their life (Riley, 2009). The positive association of biometrics with Indian citizens differentiated India from the other countries represented in the study, which both expressed more fear and uncertainty towards the technology (Riley, 2009). Another study investigated perceptions of computer privacy and security in India in comparison to the United States, and found the Indian subjects were significantly less concerned with privacy than their American counterparts. When asked a specific question regarding concerns about keeping computerized information secure, 79 percent of American participants expressed concern in contrast to 21 percent of the Indian participants (Kumaraguru, 2004). While this is not specific to biometrics, it provides insights into perceptions of privacy and security of technology in general in India.

Understanding Indian citizens’ perceptions of technology, and specifically biometrics, presents important context when analyzing the public’s reception of Aadhaar. The 2017-2018 State of Aadhaar Report found that the majority of beneficiaries approve of Aadhaar’s use to deliver PDS, but a significant minority oppose it (State of Aadhaar, 2018). In Rajasthan, the study found
that 67.4 percent of beneficiaries said that the new system improved PDS delivery, while 22.2 claimed that the new system worsened the PDS delivery system (State of Aadhaar, 2018). Those who indicated that Aadhaar made the PDS system better did so because they felt that biometrics made the system more secure (State of Aadhaar, 2018). The Center for Global Development and MicroSave conducted a survey in Rajasthan, which specifically asked whether the individual thought Aadhaar was better or worse (Gelb, 2013). 41 percent indicated that the new system was better with Aadhaar, 12 percent indicated that it is worse, and the remaining were indifferent. While there have been conflicting opinions regarding the implementation of biometrics in India, the majority believe that it is beneficial overall.

This study also found that the majority of individuals surveyed positively viewed the use of biometrics through Aadhaar in PDS delivery. Of the 95 individuals with an Aadhaar card, 56 participants answered that they liked Aadhaar. 29 participants of 95 indicated that they were indifferent, unsure, or did not have an opinion as to whether they liked Aadhaar. 9 individuals of 95, 9 percent, answered that they do not like Aadhaar. They all had varying reasons for their like or dislike of the system, however the absence of worry or concern regarding data privacy and security stood out. When directly asked if they were concerned regarding their data security, only three participants expressed concern. One individual felt that the government did not need access to the personal details and biometrics of all residents. Another questioned the government’s intent in linking so many services to Aadhaar. He found Aadhaar convenient, but it worried him that everything will be linked to one system owned by the government. The other 92 expressed no concern.
The eighth principle suggests that identification services should provide end-users with genuine choice and control over the use of their data (Principles on Identification, 2017). It also emphasizes the need for stakeholders to be transparent regarding identity management and provide them tools to manage their privacy (Principles on Identification, 2017). This study emphasizes not only the importance of transparency, but of education regarding data usage in Aadhaar. The *Principles on Identification* seem to assume that individuals are aware that data privacy in regards to Aadhaar is a concern. It discusses the necessity of documentation of data sharing arrangements, however it does not provide suggestions for disseminating this information to citizens who may not know to investigate the official data security policies.

Legal and trust frameworks

The final principle addresses the importance of (1) oversight and (2) adjudication in enforcing legal and trust frameworks (Principles on Identification, 2017). This section will analyze participant feedback to understand the ways in which Aadhaar establishes trust and mitigates user challenges.

Adjudication

This criterion emphasizes the need for independent administrative and judicial authorities to provide a grievance redressal system, in which people can submit complaints if an issue is not satisfactorily resolved by the providers responsible (Principles on Identification, 2017).
Aadhaar has an official grievance redressal system posted on their website. This survey did not produce any data regarding the effectiveness of the Aadhaar grievance redressal system.

However, there was an individual who spoke regarding his experience with Aaple Sarkar, a grievance redressal portal for the state of Maharashtra. When prompted if he had used Aaple Sarkar for his challenge with Aadhaar, he responded saying that he had used Aaple Sarkar in the past, and it was ineffective. He reported a property dispute through the Maharashtra grievance redressal portal. The complaint was processed and the officer addressed the problem with the accused individuals. However, afterwards, the accused individuals sought him out and pressured him to drop the complaint. He was deeply disappointed with the way in which this grievance redressal process was handled, as he felt it should have been completely anonymous. Therefore, he was unwilling to use Aaple Sarkar or the UIDAI grievance redressal portal for Aadhaar.

This participant was the only individual interviewed in this study who was familiar with government grievance redressal platforms. One participant had trouble enrolling, and then when he was told about Aaple Sarkar by the study facilitators, said he had never heard of the service. The lack of awareness regarding grievance redressal programs was significant, and it prevented individuals from reporting challenges with Aadhaar.

In order to have an effective grievance adjudication system, the system primarily must work. It must be responsive and effective. Secondly, people must be aware of the system. There must be an informational campaign regarding the service in order to ensure that individuals are aware of resources available to them. While the UIDAI grievance redressal portal is distinct from Aaple
Sarkar, this individual’s experience with Aaple Sarkar questions whether these systems, which are often created with benign intentions, achieve the desired and anticipated effects. This would require a greater analysis of the system to understand the consequences, intended and unintended.

Overall, this study found that the largest concern with governance in Aadhaar is education of the users. There seemed to be a significant gap in education and awareness of Aadhaar with the poor, and this makes the users vulnerable to being taken advantage of, and it reduces the effectiveness of the system in that individuals are unsure of how to resolve errors when they arise.
Conclusion

This study sought to understand the user experience of Aadhaar in an effort to answer the questions originally posed in the literature review. Through interviews with PDS recipients in Mumbai, this study generates insights into Aadhaar, which can also be applied to identification systems more broadly.

One theme present in the literature questioned whether identification systems, and other forms of state-sponsored standardization, allow the state to understand and therefore support its citizens. Through interviews with Aadhaar users, this study found that Aadhaar does help the state reach citizens by delivering services to users more effectively. Two participants were able to receive PDS services for the first time because Aadhaar provided them an identity document. Additionally, it allowed the PDS to reach citizens more effectively by improving the convenience of collection of services for some individuals. However, others experienced difficulties receiving their services, due to accessibility challenges or logistical challenges. These challenges, while a minority, imply that Aadhaar, an example of state-sponsored standardization, still struggles serving its citizens. Therefore, this study finds that increased data collection through standardized systems does not always allow states to serve citizens better. Instead, sometimes standardized systems complicate service distribution.

Another theme discussed the concept of universal access in identification systems. Identification systems generally strive for universal access, and this is evident in the World Bank’s Principles
on Identification, which specifies universal access as the primary priority. However, some scholars argue that as a state becomes more reliant on a system and as the system becomes more embedded in society, those who cannot access the system are even more excluded than previously. This study affirmed the dangers of universal access. It found that the majority of participants felt that Aadhaar was accessible, in that nearly all, except four individuals were enrolled in Aadhaar. These accounts present a promising image of Aadhaar’s inclusion of the urban poor. However, the four participants that were unable to enroll were entirely excluded from Aadhaar, and therefore expressed negative opinions of Aadhaar. Three of the four participants who were unable to enroll, were unable to enroll due to physical mobility and domestic responsibilities, constraints that should not prevent individuals from enrolling. These three perspectives illustrate the ways in which Aadhaar has not achieved universal inclusion and further isolates those who are unable to enroll in the system. The UIDAI has put policies and actions in place to include hard-to-reach groups, but clearly those efforts still have not reached everyone. The UIDAI could improve access by increasing education about the importance of enrolling, even if the individual does not plan to receive PDS services through Aadhaar, and by providing more accessible enrollment options for individuals with travel constraints. This emphasizes that in order for digital identification systems to work, they must be accessible to the users.

Another well-discussed topic regarding biometric identification systems is surveillance. Scholars emphasize the importance of good governance in prioritizing security of individual’s data and establishing trust. This study also sought to understand whether Aadhaar users themselves
expressed concerns about surveillance. In speaking with participants, this study found it difficult to measure users’ perception of the UIDAI’s prioritization of their privacy due to a prominent lack of awareness of data security in general. Only three individuals expressed concerns regarding data security of Aadhaar. The vast majority of participants expressed no concern regarding data security with Aadhaar. This could have been a result of their confidence in Aadhaar to protect their data. However, in speaking with individuals it seemed to emphasize a gap in education regarding privacy rights and implications. Additionally, the governance section emphasizes the importance of establishing trust and confidence through adjudication of grievances. This study found that the few who had negative experiences with Aadhaar, with the exception of linking errors, were unable to resolve these challenges through the UIDAI established process. This questions the effectiveness of the grievance redressal platforms, and manifested a sense of hopelessness for these individuals in correcting their challenges. Trust in the system is essential in developing a successful experience for individuals. The loss of trust expressed from these individuals paints a negative image of the governance systems which manage Aadhaar.

Overall, when Aadhaar worked well for individuals, they expressed very positive sentiments towards the system. However, when Aadhaar did not work for individuals, it completely excluded individuals from the system. Even though the negative experiences of Aadhaar represent a significant minority, the experiences of these participants exposes key inclusion, design, and governance flaws, as defined by the World Bank’s Principles on Identification. In order for Aadhaar to fulfill the qualifications designated in the Principles, the UIDAI needs to
consider and understand these negative experiences and enact appropriate solutions to make Aadhaar work for all Indian residents. Future scholarship should focus on how to effectively facilitate and include individuals in government services if they are unable to enroll or access the system through the biometric identification system. In order for biometric identification systems to effectively serve as an enabler of government services, they must be able to account for excluded cases. This is a topic that needs to be further investigated going forward.
References


UKPS (2005) *UK passport service biometrics enrolment trial*. Atos Origin


Yadav, Sunil (2018). Personal interview.


