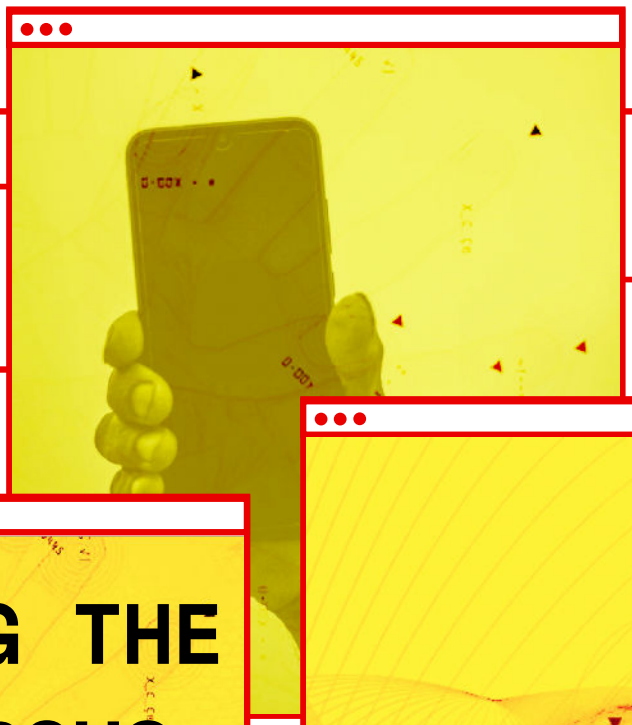
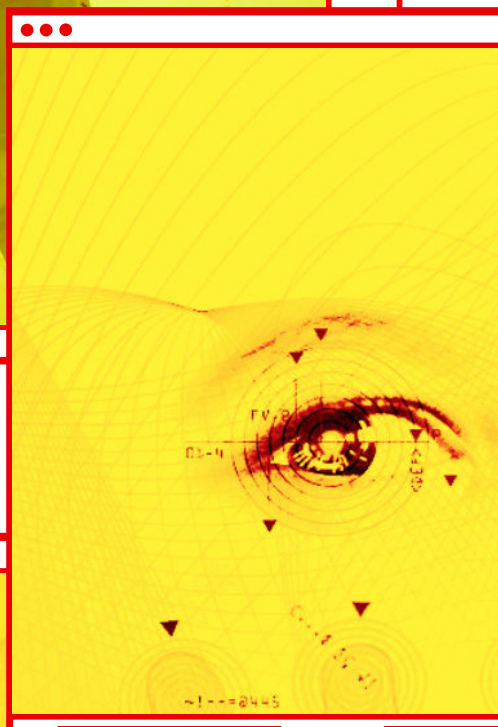
accessnow





BUSTING THE DANGEROUS MYTHS OF BIG ID PROGRAMS:

CAUTIONARY LESSONS FROM INDIA

Access Now defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions, and convenings such as RightsCon, we fight for human rights in the digital age.

accessnow.org

BUSTING THE DANGEROUS MYTHS OF BIG ID PROGRAMS: CAUTIONARY LESSONS FROM INDIA

This paper is an Access Now publication. It was written by Ria Singh Sawhney, Raman Jit Singh Chima, and Naman M. Aggarwal. We would like to thank the Access Now team members who provided support, including Verónica Arroyo, Javier Pallero, Juliana Castro, Carolyn Tackett, and Donna Wentworth. We would also like to thank the #WhyID community for participating in discussions and providing key insights for this publication.

TABLE OF CONTENTS

October 2021

I. INTRODUCTION

Around the world, the quickly expanding "Big ID" industry has driven the adoption of centralized digital identity programs that severely undermine human rights. Governments, companies, and international agencies sell and buy the idea of implementing a Big ID project as the silver bullet for solving a host of problems: more efficient delivery of public services, closing gaps in identification, fraud prevention, crime detection, and more. But far too often, these systems overpromise and underdeliver, without ever presenting evidence that these tools will actually be effective at meeting people's needs, and put millions of people's rights at risk in the process.

Aadhaar, India's flagship Big ID project, is a clear example of this approach. Despite all the positive propaganda in its favor, Aadhaar has had a disastrous impact, has been heavily criticized, and has been challenged in several courts across India, including the Supreme Court of India, for its serious violation of human rights.

In this paper, we examine 12 myths the Big ID industry uses to promote these programs and to establish a narrative that conceals the true interests and motivations behind Big ID. We refute each myth with examples from India's experience with Aadhaar, highlighting how the interests of companies, financial institutions, and other powerful players have been prioritized at the expense of people whose rights are most at risk.

The focus on Aadhaar tells a bigger story, which is important for the rapid spread of Big IDs across the world, and calls for caution. This builds on Access Now's engagement with digital IDs, including questioning **why** a digital ID is required[1] and **what** is wrong with these centralized, ubiquitous, data-heavy forms of digital identification.[2]

II. SETTING THE SCENE: WHAT IS "BIG ID"?

Big ID projects are being used across the world to supplant civil registration systems with digital identification systems. These programs often look very similar: large programs, promoted by or linked to the public sector, which seek to assign citizens and residents a

[1] #WhyID. An open letter to the leaders of international development banks, the United Nations, international aid organizations, funding agencies, and national governments. https://www.accessnow.org/whyid/

[2] Access Now et al. Recognizing Human Rights Norms in the "Principles on Identification for Sustainable Development": Civil Society Consultation Report. December, 2020. https://www.accessnow.org/cms/assets/uploads/2020/12/CSO-Consultation-on-Principles-and-DigitalID_Report.pdf

unique and ubiquitous digital identifier, store demographic and biometric data in a centralized database, and authenticate identities via a centralized system, which is often linked to biometric authentication.

Big ID projects are justified on the basis of foundational, and often dangerous, myths about why they are necessary, safe, and reliable. Most of these myths are accepted without scrutiny.

While similar programs[3] have been scrapped[4] in some developed countries,[5] they continue to spread across the developing world, often pushed by international agencies. However, these systems often have serious detrimental impacts on human rights, including the rights to privacy, equality, and nondiscrimination, and limit access to the space for participation, democracy, and accountability.[6] As nearly 100 organizations across the world have noted in the #WhyID letter, many of the justifications for these programs are often theoretical, and these projects are deployed without sufficient supportive evidence of the promised benefits.[7] On the other hand, the harms that are suffered by individuals through badly designed and implemented digital identity programs are real and, in many cases, irreparable. Unfortunately, marginalized populations suffer the greatest harm.

III. INDIA'S AADHAAR UNIQUE ID PROGRAM IS THE MODERN CAUTIONARY TALE ON BIG ID PROGRAMS

India's experience with Aadhaar starkly illustrates the dangers of Big ID programs. This paper draws on learnings from India's experience with Aadhaar to identify — and debunk — the central and dangerous myths Big ID proponents have used to advocate for its adoption.

The Aadhaar project was introduced by the Indian government's economic planning division and private software developers. It was created under an executive order and operated in a legal vacuum until 2016, when the Aadhaar Act was passed.[8] There was little precedent or reliable evidence to show that such a dangerous and large-scale centralized biometric

[3] ACLU. 5 problems with national ID cards. https://www.aclu.org/other/5-problems-national-id-cards
[4] Elets News Network. Biometric ID Database in France Found Unconstitutional. March 31, 2012. https://egov.eletsonline.com/2012/03/biometric-id-database-in-france-found-unconstitutional/
[5] Matthew Doran. Biometrics project scrapped after massive delays and budget blowouts. June 15, 2018. https://www.abc.net.au/news/2018-06-15/biometrics-project-scrapped-after-delays-and-budget-blowouts/9876068
[6] Report of the UN Special Rapporteur on extreme poverty and human rights, Philip Alston, October 11, 2019. (A/74/48037)
[7] #WhyID. An open letter to the leaders of international development banks, the United Nations, international aid organisations, funding agencies, and national governments. https://www.accessnow.org/whyid/
[8] "The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act," 2016. March 26, 2016. https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf

database would work, or that it was even necessary in the first place. India was to be an experiment.

Aadhaar's architects and other Big ID advocates have held up Aadhaar as the poster child for similar large-scale public-sector digital identity programs across the Global South.[9] It was supposed to solve two main issues: remove corruption from welfare and enable efficient, transparent, and secure digital transactions. However, since its inception, Aadhaar has had disastrous impacts on welfare systems, many of which have been extensively documented by activists, scholars, lawyers, and academics in India.[10] This myth-busting exercise is a summary of these refutations and is intended to serve as a cautionary tale of what happens when corporations, international agencies, and governments pushing for Big ID are not questioned.

Scholars, lawyers, and activists in India cautioned against Aadhaar's potential surveillance and exclusionary impacts, arguing that a digital, centralized, biometric-based national ID system posed an insurmountable threat to people's privacy and security. They challenged the project in the Supreme Court of India. In 2018, four of the five judges struck down some of the most alarming expansions of the Aadhaar project, but upheld a truncated version.[11] The dissent, which has since been subsequently relied on by other constitutional courts in Africa, the Americas, and the Caribbean, struck the project down completely, ruling that the project posed a disproportionate risk to the fundamental right to privacy and had insufficient safeguards against potential violations.

Despite its shaky foundations and poisonous roots, the Aadhaar project continues to be pushed as the gold standard for Big ID, backed by powerful international players. Many of the architects of the Aadhaar project are now part of the decision-making mechanisms that are pushing for digital ID across the world.

1.2 billion people from a low-middle income country were frog-marched into a "voluntary but mandatory" digital ID system, which paved the way for the rest of the world to follow. In doing so, Aadhaar's foundational assumptions are being exported beyond its borders and taken as incontrovertible proof. We bust these myths here.

---

[9]Anthony Kimery. Aadhaar's architect discusses what went into the world's biggest biometric repository. March 5, 2020. BiometricUpdate.com. https://www.biometricupdate.com/202003/aadhaars-architect-discusses-what-went-into-worlds-biggest-biometric-repository . See also The Evolution of India's UID Program. Center for Global Development. 2012. https://www.cgdev.org/sites/default/files/1426371_file_Zelazny_India_Case_Study_FINAL.pdf.

[10] Usha Ramanathan. A Unique Identity Bill. July 24, 2010. http://ielrc.org/content/a1003.pdf

[11] Supreme Court of India. Justice K.S.Puttaswamy (Retd) v. Union Of India. September 26, 2018. https://indiankanoon.org/doc/127517806/

The common dangerous myths used to lobby for Big ID programs

Myth #1: Big ID is needed to give people a legal identity

A common perception among Big ID evangelists is that a Big ID is required to capture vast swathes of people who have been left out of the system and to capture almost one billion people who do not have an official means of identification. Both the Universal Declaration of Human Rights and the Convention on the Rights of the Child[12] promise people the right to an identity, to recognition as a person before the law, and to a name and nationality. The Sustainable Development Goals — a set of targets that countries have committed to achieving by 2030 — also elevate the right to identity to a goal. Target 16.9 of the Sustainable Development Goals is "a legal identity for all."[13] As the World Bank notes, the "lack of identity is an impediment for poor people to exercise their basic democratic and human rights," arguing that "[d]igital identification can help overcome barriers to participation."[14]

There are, of course, many people across the world who are not counted by the state, including refugees, stateless persons, persons experiencing homelessness, and transgender people. The question is whether enrolling people into a digital Big ID system will fix the larger problem of why they are not seen by the state.

Legal is not digital

Big ID systems often promise a technological solution for a political problem. There is a conceptual sleight of hand at play here, as it conflates "legal" with "digital." Who is left out of a system and who is left unnamed are not merely a logistical issue, which can be solved with a better computing system. It is a political choice. Take the case of the Rohingya in Myanmar. The systematic exclusion they face cannot be solved with a digital ID system. In fact, it can place them at greater risk and subject them to greater exclusion and societal harm. The ID they were given in 2018, the National Verification Card,[15] is used in practice to differentiate and marginalize them on the basis of their identity. This is a use of surveillance as social

[12] Child Rights International Network. Article 7: Name and nationality. https://archive.crin.org/en/home/rights/convention/articles/article-7-name-and-nationality.html
[13] United Nations. 2030 Agenda. https://sdgs.un.org/2030agenda
[14] World Bank Group.World Development Report: Digital Dividends. 2016. https://documents1.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf
[15] Fortify Rights. Myanmar: End Campaign to Deny Rohingya Citizenship and Erase Identity. 2019. https://www.fortifyrights.org/mya-inv-2019-09-03/

"sorting" that the legal philosopher David Lyon warned about in the early 1990s.[16] In India, similar concerns have been raised about how India's National Population Register,[17] which seeks to identify non-citizens, can be linked to the Aadhaar database.

In fact, **digital decisions can trump legal decisions**. Activists in India also warned that the system would enable civil death.[18] If your identity is reduced to a number and a fingerprint, what happens if the system records you as dead? This happened to thousands of pensioners across the country.[19] There is also a clause that lets the Unique Identification Authority of India (UIDAI) make regulations to "omit" or "deactivate" the number, another form of "civil death."[20]

Visibility is a political choice

There is unquestionable value to being identified the way you want to be seen. However, this is also a political problem and not a logistical one to be solved through technology. For instance, Rohingya groups in Myanmar want to be recognized as "Rohingya," an ethnic identity which is not officially recognized in Myanmar. In Bangladesh, they want to be recognized as refugees and have demanded that the United Nations Refugee Agency (UNHCR) accords them official refugee status. In 2019, civil society groups staged a large-scale protest against smart cards issued to them by the UNHCR,[21] which labeled each person as "forcibly displaced Myanmar nationals," rather than as Rohingya. Rohingya refugees in Bangladesh are already enrolled in several digital ID systems, and the lack of a response to their ongoing demand to be recognized as Rohingya in Myanmar, and as refugees in Bangladesh, make clear that the question of how states choose to see you is a political decision that often determines whether you can exercise your fundamental rights.

Visibility is not uniformly desired

---

[16] David Lyon. Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination. 2003. https://www.felfel.is/sites/default/files/2016/Lyon%2C_D._%282003%29._Surveillance_and_social_sorting%26_computer_codes_and_mobile_bodies%20%281%29.pdf

[17] Internet Freedom Foundation. Data Protection and the National Population Register. 2019. https://internetfreedom.in/data-protection-and-the-national-population-register/

[18] V. Sridhar. Threat to citizen rights. Frontline. April 15, 2016. https://frontline.thehindu.com/cover-story/threat-to-citizen-rights/article8408824.ece

[19] Anumeha Yadav, Rajasthan's living dead: Thousands of pensioners without Aadhaar or bank accounts struck off lists. August 6, 2016. https://scroll.in/article/813132/rajasthans-living-dead-thousands-of-pensioners-without-aadhaar-or-bank-accounts-struck-off-lists

[20] Statement made in the Indian Parliament. 2017. https://uidai.gov.in/images/rajyasabha/RS2964.pdf

[21] The Engine Room. Digital ID in Bangladeshi refugee camps: A case study. 2019. https://digitalid.theengineroom.org/assets/pdfs/[English]%20Bangladesh%20Case%20Study%20-%20DigitalID%20-%20The%20Engine%20Room.pdf

Marginalized groups may have good reason to conceal or control aspects of their identity. As Privacy International notes, “visibility can lead to marketing that pesters users, fleeing populations can be targeted by militaries that pursue them, or visible populations may be favoured at the expense of less visible ones.”[22] In India, religious and caste identities are contested. Dalit rights activist and co-petitioner in the Aadhaar case Bezwada Wilson has said, on the impact of Aadhaar for people from oppressed castes who worked as manual scavengers, “What they want is to bury their identity, and what they are threatened with is tagging them with this identity in perpetuity.”[23]

Aadhaar didn’t count the uncounted

In any case, evidence has shown that Aadhaar did not reach the supposed vast numbers of uncounted persons. The authority’s enrollment figures showed that most Aadhaar cards were issued to those who already had IDs.[24] Only 0.03% were enrolled through the “introducer” system, which was supposed to enable those without any other forms of identity to be enrolled when someone with an Aadhaar vouched for or introduced them. Aadhaar didn’t give a more accurate figure of the number of taxpayers either. According to recent research on Indian taxpayers, the actual number of permanent account number (PAN) cards, required to pay income tax, did not significantly increase after they were (mandatorily) linked to Aadhaar.[25] And today, the people excluded from Aadhaar coverage continue to be the same: those experiencing homelessness (30% of homeless people don’t have Aadhaar), refugees (India doesn’t have an official refugee policy), and people who live in remote areas.[26] With the imposition of mandatory Aadhaar to access many government services, these excluded groups of people have to cross additional hurdles to access public goods and services.

Myth #2: Big ID is needed to empower people

Who benefits from a Big ID system? The World Bank notes in one of its earlier documents that a good, inclusive, trusted ID is needed for “empowering individuals and enhancing their access to rights, services, and the formal economy.”[27] Was a Big ID needed for people, or was it merely useful for *some* people?

---

[22] Privacy International. Fintech: Privacy and Identity in the New Data-Intensive Financial Sector. 2017. https://privacyinternational.org/sites/default/files/2017-12/Fintech%20report.pdf

[23] Usha Ramanathan. A shaky Aadhaar. March 30, 2017. https://indianexpress.com/article/opinion/columns/aadhar-card-uid-supreme-court-a-shaky-aadhaar-4591671/

[24] The Wire. 'Most Aadhar Cards Issued to Those Who Already Have IDs'. June 03, 2015. https://thewire.in/law/most-aadhar-cards-issued-to-those-who-already-have-ids

[25] Anupam Saraph. The Curious Case of PAN–Aadhaar Linkage. Economic and Political Weekly. August 29, 2020. https://www.epw.in/journal/2020/35/special-articles/curious-case-pan%E2%80%93aadhaar-linkage.html

[26] State of Aadhaar. 2019. https://stateofaadhaar.in/download-reports.php

[27] World Bank. Good ID supports multiple development goals. Identification for Development https://id4d.worldbank.org/guide/good-id-supports-multiple-development-goals

One of the major selling points for a Big ID is its potential to fix exclusion. This rests on a misunderstanding, or a deliberate simplification,[28] of what causes exclusion. People are excluded from welfare programs because either they don't meet the targeting requirements or budgetary caps restrict the scope of a program. Merely being enrolled for an Aadhaar number does not enable people to apply for a social scheme. People have to meet additional requirements, show additional scheme-specific ID (say for old age or disability pensions), and hope that there is state funding to include them in the program. Rethink Aadhaar, a campaign tracking and contesting the spread of Aadhaar, points out: "The cure [to social exclusion] is to expand these schemes. What the government is doing instead is to additionally make it mandatory for them to enroll into a biometrics-based identity program to get the welfare benefits *they are already eligible for*."[29]

Aadhaar has caused more exclusions

India's experience with Aadhaar shows how a Big ID, particularly when made mandatory to access public services, operates as a tool of exclusion. Inflexible or onerous ID requirements have long been used to block people from accessing a service or exercising their rights. For instance, stringent voter ID requirements in states across the United States established under the pretense of preventing voter fraud are actually used to block people who experience systemic discrimination — including Black, Indigenous, and other people of color — from voting.[30]

Introducing Aadhaar into the welfare delivery system depended on several fragile technologies:[31] people have to enroll for an Aadhaar number, then hope that their biometrics are machine-readable and the server connection works. Then, they have to submit their Aadhaar numbers to be "seeded" with the ration list. They have to hope that there are no mysterious faults that cause their names to be struck off the list. Finally, at the point of sale/ distribution, they have to ensure that there is an active internet connection and server connectivity, and that their fingerprints are readable. This does not even take into account the added layer introduced by the Aadhaar Enabled Payment System, which routed all payments through an Aadhaar-linked system, a maze that has been described as Kafkaesque, as exclusions can result from a fault at any point in the system.

---

[28] Rethink Aadhaar. FAQs on Aadhaar and Welfare. https://rethinkaadhaar.in/faqs/welfare/
[29] Rethink Aadhaar. FAQs on Aadhaar and Welfare. https://rethinkaadhaar.in/faqs/welfare/
[30] PBS. Why Voter ID Laws Aren't Really about Fraud. October 20, 2014. http://www.pbs.org/wgbh/pages/frontline/government-elections-politics/why-voter-id-laws-arent-really-about-fraud/
[31] Gaurav Vivek Bhatnagar. Aadhaar-Based PDS Means Denial of Rations For Many, Jharkhand Study Shows. The Wire. September 08, 2016 https://thewire.in/rights/jharkhand-aadhaar-pds-nfsa

Since its introduction to welfare schemes across India, millions of people have been impacted.[32] Thousands of ration cards have been canceled without notice or clear modes of redress. Over one million children were denied admission in school.[33] Women found it harder to access their maternity benefits and workers of state-run programs were denied their wages.[34] A recent study showed that 1.5 to 2 million people lost access to their benefits at some point due to Aadhaar.

The result was multiple starvation deaths, as people were in effect cleansed off welfare lists.[35] Some of these deaths were even brought to the Supreme Court of India's attention during the hearing. In 2017, an 11-year-old child, Santoshi Kumari, died of starvation after her family's food ration card was deactivated because of Aadhaar-related failures.[36] In 2019, her mother petitioned the Supreme Court to challenge the basis on which her ration card (and 3 million others) was deleted.[37] A 2020 sample survey from the state of Jharkhand found that almost 88% of deleted ration cards were not fake.[38] Even industry reports on how Aadhaar is working, like the annual "State of Aadhaar" report,[39] estimated that, in 2017, around two million individuals were excluded every month from the food distribution system because of Aadhaar-related reasons, like failures in biometric authentication (for example, fingerprints not being recognized) and connectivity issues, which are particularly acute in rural areas.[40] In the state of Telangana, efforts linking voter identification and Aadhaar disenfranchised almost

---

[32] For a summary of the impacts of Aadhaar since its inception, see: Jury Report from the Peoples' Tribunal on Aadhaar-related issues. October 2, 2020. https://rethinkaadhaar.in/blog/2020/10/2/report-of-the-peoples-tribunal-on-aadhaar-related-issues-1 and the Evidence Book from the Peoples' Tribunal. March 3, 2020. https://drive.google.com/drive/u/2/folders/1ZJZI4GbGRLM3Eg_3xQNO4cW341o2qyfn

[33] IndiaSpend Team. Because of Aadhaar, over one million children in India were denied admission to schools December 10, 2019. Scroll.in. https://scroll.in/article/946285/because-of-aadhaar-over-one-million-children-in-india-were-denied-admission-to-schools

[34] Reetika Khera. How Aadhaar is making it harder for Indian women to access their maternity benefits. Scroll.in. December 7, 2019. https://scroll.in/pulse/945587/how-aadhaar-is-making-it-harder-for-indian-women-to-access-their-maternity-benefits. Aareja Johar. In Jharkhand, Aadhaar woes are depriving NREGA workers of their wages. Scroll.in. February 5, 2019. https://scroll.in/article/911575/in-jharkhand-aadhaar-woes-are-depriving-nrega-workers-of-their-wages

[35] Shiv Sahay Singh. Death by digital exclusion? On faulty public distribution system in Jharkhand. The Hindu. July 13, 2019. https://www.thehindu.com/news/national/other-states/death-by-digital-exclusion/article28414768.ece

[36] The Wire. Jharkhand Girl Dies After Family's Ration Denied for No Aadhaar Link, BJP Blames Malaria. October 17, 2017. https://thewire.in/politics/jharkhand-death-aadhaar-ration-card

[37] Shristi Ojha. 'Matter Is Too Serious' SC Seeks Centre's Response On Plea Alleging Cancellation Of 3 Crore Ration Cards For Not Linking With Aadhaar & Subsequent Starvation Deaths. LiveLaw. March 17, 2021. https://www.livelaw.in/top-stories/supreme-court-cancellation-of-3-crore-ration-cards-aadhaar-central-government-171292

[38] Jahnavi Sen. New Study Backs Reports That Aadhaar-PDS Link in Jharkhand Led to Exclusions. The Wire. February 21, 2020. https://thewire.in/rights/aadhaar-pds-ration-cards-jharkhand-jpal

[39] Karthik Muralidharan, Paul Niehaus, and Sandip Sukhtankar. Identity Verification Standards in Welfare Programs: Experimental Evidence from India. NBER Working Paper No. 26744. February 2020, revised September 2021. https://www.nber.org/system/files/working_papers/w26744/w26744.pdf

[40] Vishnu Padmanabhan. Has Aadhaar improved welfare delivery? LiveMint. April 21, 2019. https://www.livemint.com/news/india/has-aadhaar-improved-welfare-delivery-1555861461316.html

two million people.[41] In February 2021, the BBC reported that malnutrition was on the rise across India. A major cause for this was how onerous documentation requirements blocked people's access to life-saving welfare entitlements.[42]

Big ID was used to exploit individuals' data and identity for enrichment of certain interests

The biggest benefactors of the Aadhaar project were a host of private parties who were instrumental in introducing infrastructure that enabled data-extractive practices.

The chief architects of the Aadhaar project were a host of Indian software companies, many of which were associated, as "volunteers," with a lobby group called iSPIRT, the Indian Software Product Industry Round Table.[43] This group created IndiaStack, a set of Aadhaar-specific software application programming interfaces (APIs), which governs communication between different programs.[44] This framework was built on top of Aadhaar data and was central to the adoption of the National Payments Corporation of India (NPCI), which created the Aadhaar-based payments system. Close collaboration between businesses and India's government was baked into the design of UIDAI, as was seen in early documentation around Aadhaar, like the 2011 Report of the Technology Advisory Group for Unique Projects (or TAG-UP).[45] This had several implications. For one, Aadhaar was a "startling example of corporate invasion of public policy, with business consultants packing government committees, drafting laws, harvesting lucrative contracts and orchestrating Aadhaar's public relations."[46] As prominent activist and legal researcher Usha Ramanathan notes, "Aadhaar was used as a tool to get the new gold: data; and the same people who worked within the government to set the framework for Aadhaar went on to create products in the private sector to harness its commercial potential — a clear case of conflict of

[41] Bappa Sinha. Aadhaar-Voter ID Linking May Have Disenfranchised Millions. NewsClick. November 16, 2019. https://www.newsclick.in/aadhaar-voter-id-linking-may-have-disenfranchised-millions

[42] BBC. Malnutrition is rising across India - why? February 18, 2021. https://www.bbc.com/news/world-asia-india-56080313

[43] Rohin Dharmakumar. Aadhaar and the gradual collapse of India Stack. The Ken. October 3, 2018. https://the-ken.com/story/aadhaar-and-the-gradual-collapse-of-india-stack/

[44] Rohan Venkataramakrishnan. Co-founder of UIDAI-associated outfit admits to anonymously trolling Aadhaar critics on Twitter. Scroll.in. May 23, 2017. https://scroll.in/article/838468/co-founder-of-uidai-associated-outfit-admits-to-anonymously-trolling-aadhaar-critics-on-twitter

[45] Ministry of Finance. Report of the Technology Advisory Group for Unique Projects. 2011. https://www.finmin.nic.in/sites/default/files/TAGUP_Report.pdf

[46] Jean Dreze. Ill fares Aadhaar. Indian Express. October 2, 2018. https://indianexpress.com/article/opinion/columns/privacy-surveillance-pan-card-ill-fares-aadhaar-link-5381698/

interest."[47] Second, this created space for the logic of start-ups to be brought into governance, allowing room for "iterations" which people bore the brunt of.[48]

There were two ways in which Aadhaar was useful to private companies: the unique number provided a way to identify all digital transactions made by Indians, and the data trails created a "critical mass of data on each user by virtue of both the government and hundreds of private companies."[49]

Before India's Supreme Court struck down a statutory provision within the Aadhaar Act of 2016 that permitted private companies to use Aadhaar, there was a boom in companies developing apps and programs to leverage the Aadhaar number.[50] Private interests benefited from the system that enabled the collection of vast amounts of data,[51] and the government gained when private companies used Aadhaar authentication services.[52] The court struck this down, but the government pushed through an ordinance that allowed for private parties to "voluntarily" use Aadhaar authentication. This was replaced by an amendment act that is currently pending challenge in the Supreme Court.

Big ID gives states more power

As Senior Advocate Shyam Divan, one of the key lawyers, argued in the Supreme Court, by centralizing so much power, "Aadhaar alters the relationship between the citizen and the state and tilts the balance so steeply in favor of the government."[53] Aadhaar could be used to consolidate state power, as explained in the next myth on surveillance. For example, data stolen from Aadhaar enrollments were used to profile voters.[54]

---

[47] Usha Ramanathan. Data is the new gold and Aadhaar is the tool to get it. Scroll.in. December 30, 2016. https://scroll.in/article/825049/data-is-the-new-gold-and-aadhaar-is-the-tool-to-get-it

[48] Ministry of Finance. Report of the Technology Advisory Group for Unique Projects. 2011. https://www.finmin.nic.in/sites/default/files/TAGUP_Report.pdf. Page 28.

[49] M. Rajshekhar. What happens to privacy when companies have your Aadhaar number? Scroll.in. December 23, 2016. https://scroll.in/article/824874/what-happens-to-privacy-when-companies-have-your-aadhaar-number

[50] Section 57 was struck down by the 2019 Aadhaar judgement. *See* M. Rajshekhar. What happens to privacy when companies have your Aadhaar number? Scroll.in. December 23, 2016. https://scroll.in/article/824874/what-happens-to-privacy-when-companies-have-your-aadhaar-number

[51] M. Rajshekhar. What happens to privacy when companies have your Aadhaar number? Scroll.in. December 23, 2016. https://scroll.in/article/824874/what-happens-to-privacy-when-companies-have-your-aadhaar-number

[52] M. Rajshekhar and Anumeha Yadav. How the government gains when private companies use Aadhaar. Scroll.in March 24, 2016. https://scroll.in/article/805467/how-the-government-gains-when-private-companies-use-aadhaar

[53] Pranav Dixit. India's National ID Program May Be Turning The Country Into A Surveillance State. Buzzfeed. April 4, 2017. https://www.buzzfeednews.com/article/pranavdixit/one-id-to-rule-them-all-controversy-plagues-indias-aadhaar

[54] Asheeta Regdi. IT Grids Aadhaar data leak: UIDAI's implicit acknowledgement of a large-scale data breach will be very welcome to anti-Aadhaar activists-India News. FirstPost. April 15, 2019. https://www.firstpost.com/india/it-grids-aadhaar-data-leak-uidais-implicit-acknowledgement-of-a-large-scale-data-breach-will-be-very-welcome-to-anti-aadhaar-activists-6452011.html

Myth #3: A Big ID program does not create a surveillance state

The UIDAI also claimed that the project and the database did not violate the right to privacy. They claimed that the Aadhaar Act only permitted them to collect minimal amounts of data, and the system did not retain any information about the nature of the transaction. It could only be used for "yes/ no" authentication, which gave no information about the type of transaction, or for Know Your Customer purposes, which had an additional layer of security in the form of biometric verification, or One Time Passwords. In an affidavit submitted to the Supreme Court in 2017, the UIDAI said, "By design, the technology architecture of UIDAI precludes even the possibility of profiling individuals for tracking their activities," stating that, "...on the basis of a single identifier, Aadhaar will enable the government agencies to track and profile and do surveillance is completely unfounded and denied."[55]

Aadhaar's law and design enabled surveillance

Section 8 of the Aadhaar Act permits sharing of any of the data (except core biometric data) that was saved in the Central Identities Data Repository (CIDR), upon an authentication request.[56] The Aadhaar (Sharing of Information) Regulations 2016 placed no restrictions on the sharing or use of demographic or biometric data (except core biometric data). Section 29 (4) gives the UIDAI wide latitude to "publish, display or post publicly" Aadhaar numbers, demographic data, or photographs for purposes specified in regulations.[57] Section 33(1) of the Aadhaar law permits the UIDAI to share ID information and all authentication records in the interest of "national security" (even as the phrase "national security" is undefined in the present bill, as well as the General Clauses Act).

The UIDAI's metadata trails also give a lot of information. When the CIDR receives a request for authentication, it has information about where the request is coming from — banks, employers, hospitals, airline companies, the Indian Railways, shops, or even the Election Commission of India. This was pointed out to the Supreme Court by expert evidence, as well as brought up by activists and researchers.[58]

Seeding a surveillance state

[55] Kumar Sambhav Shrivastava. Documents Show Modi Govt Building 360 Degree Database To Track Every Indian. HuffPost. March 16, 2020. https://www.huffpost.com/archive/in/entry/aadhaar-national-social-registry-database-modi_in_5e6f4d3cc5b6dda30fcd3462?ncid=yhpf

[56] Prashant Reddy. No longer a black box: Why does the revised Aadhaar Bill allow sharing of identity information? Scroll.In. April 06, 2016. https://scroll.in/article/806297/no-longer-a-black-box-why-does-the-revised-aadhar-bill-allow-sharing-of-identity-information

[57] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016. https://gtm.uidai.gov.in/images/Aadhaar_Act_2016_as_amended.pdf

[58] *See* description of the expert evidence in *Shanta Sinha v. Union of India*, Review Petition, filed in the Indian Supreme Court. Copy of brief available at https://scobserver-production.s3.amazonaws.com/uploads/case_document/document_upload/1262/ShanthaSinhaVUOI-AadhaarReview.pdf. [internal pages 1460, 1470].

One way in which Aadhaar helped create a surveillance state was through the push to "seed" the Aadhaar number into different databases.[59] Seeding is a term of art unique to the Indian context. The UIDAI defines "seeding" as "linking Aadhaar holder's Unique 12 digit Aadhaar number with their Personal Identification Documents or Benefit Cards."[60]

How this works in practice is that the Aadhaar number is linked to a person's name and pasted into different databases containing their details. This enables the Aadhaar number to be used as a unique identifier across different databases.

As security researcher Anand Venkatanarayanan notes, Aadhaar's system design enabled both the "organic" and "inorganic seeding" of the state's beneficiary databases.[61] [62] While "organic" seeding was done manually, by the person providing their Aadhaar number, inorganic seeding *didn't require user consent.* This meant that once a person had an Aadhaar number, this number was used to link their profiles in different databases, which allowed them to be tracked across those databases.

For example, several Indian state governments began using Aadhaar enrollment data to create State Resident Data Hubs, which linked related data.[63] This promised a "360 degree view" of people, which is a privacy threat. The Aadhaar-linked data was then put to use for other purposes—in the state of Telangana, for instance, the state tried to use Aadhaar data to "clean up" voter ID lists,[64] and data was also used to target and profile voters.[65]

Ignored by the Court

The Supreme Court's majority judgement focused on the UIDAI's limited ability to access data, ignoring the government's access to data that has been enabled by seeding. The majority judgement held that the safeguards in the law were sufficient to obviate the threat of surveillance. Cognizant of the vast amounts of data trails that were being generated, the court

---

[59] Unique Identification Authority of India. Aadhaar Workshop on Seeding. https://archive.org/details/Aadhaar_Workshop_Seeding

[60] Unique Identification Authority of India. Glossary. https://uidai.gov.in/contact-support/have-any-question/glossary.html

[61] Anand Venkatanarayan. The 360 Degree Database. December 6, 2017. Kaarana. https://medium.com/karana/the-360-degree-database-17a0f91e6a33

[62] Unique Identification Authority of India. Aadhaar Workshop on Seeding. https://archive.org/details/Aadhaar_Workshop_Seeding

[63] Anand Venkatanarayan. The 360 Degree Database. December 6, 2017. Kaarana. https://medium.com/karana/the-360-degree-database-17a0f91e6a33

[64] Srinivas Kodali. Disenfranchised by Aadhaar: Voter Deletions in Telangana. The Leaflet. March 17, 2019. https://www.theleaflet.in/disenfranchised-by-aadhaar-voter-deletions-in-telangana/

[65] Aadhaar data leak: Details of 7.82 cr Indians from AP and Telangana found on IT Grids' database-India News. Firstpost. April 15, 2019 https://www.firstpost.com/india/aadhaar-data-leak-details-of-7-82-cr-indians-from-ap-and-telangana-found-on-it-grids-database-6448961.html

directed the government to delete metadata logs retained by the UIDAI that were older than 6 months. It also read down some provisions in the Act which it thought enabled surveillance, striking down Section 57 of the Act, and directing states to delete data saved in State Resident Data Hubs.[66]

After the judgement, the government found newer ways to gather people's data in centralized, searchable databases. Many states started to develop their own databases[67] of individuals in the form of social registries.[68] This consolidation of data has now resurfaced as India Enterprise Architecture (IndEA).[69]

Lack of surveillance reform

The consolidation of data is especially troubling against the backdrop of India's pressing need for surveillance reform.[70] Many central government agencies have practically unfettered power to "intercept, monitor and decrypt all data contained in any computer."[71] The Central Monitoring System (CMS)[72] grants security agencies direct access to communication data, while the National Intelligence Grid (NATGRID)[73] is a surveillance agency set up almost simultaneously with the UIDAI. NATGRID links 10 intelligence agencies with 21 data sources, including air and train travel, telecommunications, tax, banking, and immigration data pools. Officials say that the NATGRID database had also included a pool of mobile numbers, vehicle numbers, passport numbers, Aadhaar numbers, arms licenses, bank accounts, travel details, and social media accounts.[74]

Lack of data protection

[66] Supreme Court of India. Justice K.S.Puttaswamy(Retd) vs Union Of India on 26 September, 2018. https://indiankanoon.org/doc/127517806/

[67] Kumar Sambhav Shrivastava. Telangana Offered Its Own 360 Degree Citizen Tracking System To Modi Govt. HuffPo. March 18, 2020. https://www.huffpost.com/archive/in/entry/telangana-samagram-system-social-registry_in_5e721e19c5b63c3b64881b30

[68] Kumar Sambhav Shrivastava. Documents Show Modi Govt Building 360 Degree Database To Track Every Indian. March 16, 2020. HuffPo. https://www.huffpost.com/archive/in/entry/aadhaar-national-social-registry-database-modi_in_5e6f4d3cc5b6dda30fcd3462

[69] National eGovernance Division. India Enterprise Architecture. https://negd.gov.in/india-enterprise-architecture

[70] Vrinda Bhandari. The Pegasus Case Must be Used to Press for Change in Surveillance Laws. August 20, 2021. India Forum. https://www.theindiaforum.in/article/pegasus-case-must-be-used-press-change-surveillance-laws?utm_source=website&utm_medium=organic&utm_campaign=category&utm_content=Law; Apar Gupta. Home Ministry Order: Is India Becoming A Surveillance State? Bloomberg Quint. December 23, 2018. https://www.bloombergquint.com/opinion/is-india-becoming-a-surveillance-state

[71] Section 69 of the Information Technology Act, 2000.

[72] Maria Xynou. India's Central Monitoring System (CMS): Something to Worry About? — The Centre for Internet and Society. Center for Internet and Society. January 30, 2014. https://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about

[73] Maria Xynou. Big democracy, big surveillance: India's surveillance state. Open Democracy. February 14, 2014. https://www.opendemocracy.net/en/opensecurity/big-democracy-big-surveillance-indias-surveillance-state/

[74] These systems are being challenged in the High Court of Delhi and the Supreme Court of India. *See* Software Freedom law Center. Legal Challenge by CPIL and SFLC.IN to Surveillance Projects CMS, NATGRID and NETRA. December 2020. https://www.sflc.in/legal-challenge-cpil-and-sflcin-surveillance-projects-cms-natgrid-and-netra

India still lacks data protection legislation, despite a draft having been in the works for close to four years. A bill from 2019 is currently pending consideration before a Joint Parliamentary Committee.[75] While the bill accords data subjects key rights over their data, it gives the state a concerning level of lassitude,[76] including the powers to sidestep the requirement of consent for a wide range of reasons and a broad provision under which the government can exempt its own departments from the very application of the law itself. The power to surveill, track, and digitally sort a data-based citizenry is easily abused and can quickly take on sinister overtones in the hands of an authoritarian government. For instance, IBM's punch card technology was instrumental in facilitating the genocide of Jews in Europe by permitting the easy sorting of census records.[77] This fear is central to why many Western countries have been cautious about central databases. In India, similar concerns have been raised with the links between the National Population Register and Aadhaar. [78]

Myth #4: A Big ID is needed to reform the welfare state

Another purportedly strong reason for Big IDs is their supposed ability to eliminate fraud from the welfare system. Big ID proponents have effectively co-opted this method as the best and most effective way to achieve the Sustainable Development Goals (SDG), pointing in particular to Big ID's ability to meet Goal 16 of the SDGs—"strengthening the transparency, efficiency, and effectiveness of governance and service delivery"—and Target 16.5—"substantially reduce corruption and bribery in all their forms."[79] Proponents claimed that while Aadhaar linkage was likely to cause "disruptions," the main losers would be those who got away with double dipping and other corrupt practices.[80]

This is based on a simplification of corruption to "errors of inclusion," i.e. errors which result in people who should not be on the welfare rolls being included in them. This justification was central to the myth of the need for Aadhaar: that is, that the state's failure to establish the identity of welfare beneficiaries was leading to (and the root cause of) leakage and corruption

[75] Access Now. India's proposed data protection bill: further work is needed to ensure true privacy for the next billion users. February 25, 2020. https://www.accessnow.org/indias-proposed-data-protection-bill-further-work-is-needed-to-ensure-true-privacy-for-the-next-billion-users/

[76] Access Now. India's proposed data protection bill: further work is needed to ensure true privacy for the next billion users. February 25, 2020. https://www.accessnow.org/indias-proposed-data-protection-bill-further-work-is-needed-to-ensure-true-privacy-for-the-next-billion-users/

[77] Edwin Black. IBM and the Holocaust. 2001. https://archive.org/stream/IbmAndTheHolocaust/ibm-and-the-holocaust-edwin-black-2001-history_djvu.txt

[78] Internet Freedom Foundation. Impact of the Personal Data Protection Bill, 2019 on National Population Register https://drive.google.com/file/d/104V9yn1ygjHjIdK92ZWz7P-oNvbjSrzY/view

[79] The World Bank ID4D. Good ID Support Multiple Development Goals. https://id4d.worldbank.org/guide/good-id-supports-multiple-development-goals

[80] Frances Zelazny. The Evolution of India's UID Program. Center for Global Development. 2012. https://www.cgdev.org/sites/default/files/1426371_file_Zelazny_India_Case_Study_FINAL.pdf

and was causing a hindrance to its implementation. As Reetika Khera, an Indian development economist, noted around the time Aadhaar was being challenged in the courts, "there were many stories of 'fake' school enrolments, 'ghost' teachers, 'bogus' ration cards, etc. discovered due to Aadhaar. One report claimed that nearly [10 million] fake job cards had been deleted, whereas follow-up investigations reveal that there was little substance in these stories."[81]

Can a Big ID fix welfare fraud?

This myth is based on a misconception that the most widespread form of corruption within welfare systems is caused by "ghosts" and "double dipping," that is, people who don't exist, and people who have enrolled twice or taken twice their entitlements. Experts deeply familiar with India's welfare system, like development economists Reetika Khera and Jean Dreze, point out that the focus on ghosts and duplicates is based on misconceptions about how corruption actually works within the welfare system.[82] None of the proponents of Big ID have adequately studied the other ways in which corruption works in welfare systems and what type of reform has been helpful.[83] A digital ID system can only, if at all, counter identity fraud, which is one of three common types of fraud that welfare systems usually have, such as eligibility fraud and quantity fraud.

The extent of identity fraud is also contested. A 2017 survey conducted by the Right to Food movement found that of a sample of 135 canceled ration cards, only two were declared "fake" and three found to be duplicates — the rest were eligible beneficiaries.[84] A 2020 survey by J-PAL, a poverty action lab founded by Nobel Prize-winning economists Abhijit Banerjee and Esther Duflo, found that 88% of canceled ration cards belonged to genuine households.[85] [86]

For Aadhaar, the supposed savings were heavily overplayed. A 2016 World Bank report claimed that the government could save "over US$11 billion per year in government

---

[81] Reetika Khera (ed.) Dissent on Aadhaar: Big Data Meets Big Brother. Orient BlackSwan. 2019. https://orientblackswan.com/details?id=9789352875429

[82] Reetika Khera (ed.) Dissent on Aadhaar: Big Data Meets Big Brother. Orient BlackSwan. 2019. https://orientblackswan.com/details?id=9789352875429

[83] Reetika Khera. Aadhaar Failures: A Tragedy of Errors. Economic and Political Weekly. August 5, 2019. https://www.epw.in/engage/article/aadhaar-failures-food-services-welfare

[84] Anumeha Yadav. Aadhaar disruption: In Jharkhand's poorest regions, hundreds of people are being denied foodgrain. December 7, 2019. https://scroll.in/article/860857/aadhaar-disruption-in-jharkhands-poorest-regions-hundreds-of-people-are-being-denied-foodgrains

[85] Karthik Muralidharan, Paul Niehaus & Sandip Sukhtankar. Identity Verification Standards in Welfare Programs: Experimental Evidence from India. National Bureau of Economic Research. February 2020. https://www.nber.org/papers/w26744

[86] Jahnavi Sen. New Study Backs Reports That Aadhaar-PDS Link in Jharkhand Led to Exclusions. The Wire. February 21, 2020. https://thewire.in/rights/aadhaar-pds-ration-cards-jharkhand-jpal

expenditures through reduced leakage and efficiency gains."[87] This figure was relied on by the government in the proceedings before the Supreme Court. These "savings" were found to be an almost entirely fabricated number, referring to the entire welfare budget.[88] This was pointed out by prominent economists, but the court chose not to respond and the World Bank quietly rescinded the figures.[89]

Even more troubling, the linkage of the welfare systems to Aadhaar was imposed by applying an "ultimatum" to the linkage.[90] Those who were unable to link their Aadhaar numbers in time were simply removed from the welfare lists. These people were then labeled as fake names, and the reduction in the welfare budget was called "savings."

What reform does the welfare system need?

The single-minded focus on digital ID also takes attention and resources away from the reforms[91] that are actually needed and have worked to reduce leakage within the welfare systems. Some examples are supply chain reforms (door-to-door delivery of food rations), food coupons, the digitization of records (records of how the food deliveries were made), measures for doorstep delivery (to eliminate the middleman), SMS alerts, social audits, and toll-free helplines.

Is Big ID a cure worse than the disease?

Rather than reducing corruption, Aadhaar has enabled new forms of corruption[92] because of the centralization of decision-making and the opacity that the system has introduced. At the local level, the unequal power structure that enables corruption continues — for example, people who are unlettered can be made to input their biometrics for authentication, while they are given less than their entitlements. A beneficiary from Jharkhand told a researcher, "a

[87] The World Bank. World Development Report 2016. Digital Dividends. https://documents1.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf at page 195.
[88] Reetika Khera. On Aadhaar Success, It's All Hype - That Includes The World Bank. July 25, 2016. https://www.ndtv.com/opinion/yes-aadhaar-is-a-game-changer-in-wrecking-welfare-schemes-1434424
[89] Anand Venkatanarayanan. The Curious Case of the World Bank and Aadhaar Savings. The Wire. October 3, 2017. https://thewire.in/economy/the-curious-case-of-the-world-bank-and-aadhaar-savings
[90] Jean Dreze. Ill fares Aadhaar. Indian Express. October 2, 2018. https://indianexpress.com/article/opinion/columns/privacy-surveillance-pan-card-ill-fares-aadhaar-link-5381698/
[91] Jean Dreze. Aadhaar-based biometric authentication—Dark clouds over the PDS. September 10, 2016. https://www.thehindu.com/opinion/lead/Dark-clouds-over-the-PDS/article14631030.ece
[92] Rebecca Ratcliffe. How a glitch in India's biometric welfare system can be lethal. The Guardian. October 16, 2019. https://www.theguardian.com/technology/2019/oct/16/glitch-india-biometric-welfare-system-starvation

dealer entered something in his machine and the slip said I had taken two months of grain but he gave me only one month."[93]

In 2017, a door-to-door survey conducted in the state of Jharkhand by the Right to Food campaign, a grassroots pan-India group, found that, of a small sample of 135 canceled ration cards, six households had their cards canceled when the head of the household died, and 26 were canceled for "failure to link."[94] The rest — and the vast majority — were not told why their cards were canceled. In 2020, a scholarship scam was reported from the state of Jharkhand where the Aadhaar details of minority students were used to apply for scholarships in their name without their receiving the scholarships.[95]

Is targeting the goal of all welfare programs?

The digitalization and "cleaning up" of welfare rolls is also based on an assumption that it will help target welfare programs better. Targeting welfare schemes is a form of fiscal austerity that many international development agencies push countries toward, regardless of whether it is appropriate in the context or whether it works at all. Research suggests that countries that minutely target their welfare resources exclusively at the poor achieve less redistribution and are less effective at reducing inequality — a phenomenon described as the "paradox of redistribution."[96]

Minute targeting also adds a high administrative burden that diverts resources and impacts the quality of the public good or service. As Nobel Prize-winning economist Amartya Sen has said, "benefits meant exclusively for the poor often end up being poor benefits."[97] Determining the scope and extent of a welfare program is a political choice that should be done with due public deliberations and not smuggled in under the cloak of digitalization. In 2019, the U.N. Special Rapporteur on extreme poverty and human rights Philip Alston warned that the digitalization of the welfare state being seen across the world was being used as a

[93] Anumeha Yadav. Aadhaar disruption: In Jharkhand's poorest regions, hundreds of people are being denied foodgrain. Scroll.in. December 9, 2017. https://scroll.in/article/860857/aadhaar-disruption-in-jharkhands-poorest-regions-hundreds-of-people-are-being-denied-foodgrains

[94] Anumeha Yadav. Aadhaar disruption: In Jharkhand's poorest regions, hundreds of people are being denied foodgrain. Scroll.in. December 9, 2017. https://scroll.in/article/860857/aadhaar-disruption-in-jharkhands-poorest-regions-hundreds-of-people-are-being-denied-foodgrains

[95] Abhishek Angad. Direct Benefit Transfer is direct siphoning of school scholarship. Indian Express. November 2, 2020. https://indianexpress.com/article/express-exclusive/scholarship-scam-direct-benefit-transfer-6911896/

[96] Walter Korpi and Joakim Palme. The Paradox of Redistribution and Strategies of Equality: Welfare State Institutions, Inequality, and Poverty in the Western Countries. American Sociological Review. 1998. https://www.jstor.org/stable/2657333?seq=1

[97] Amartya Sen. The Political Economy of Targeting. Annual Bank Conference on Development Economics, World Bank. 1992.https://scholar.harvard.edu/sen/publications/political-economy-targeting

Trojan horse to push a neoliberal agenda.[98] There are often private interests looking to step into the role played by the state. As a Privacy International report from 2019 notes, "austerity [is] a juicy business for companies benefitting from the outsourcing of the welfare state."[99]

Who is to blame?

This myth also reframes the problem with the welfare systems as one of individual culpability (from those benefiting from the system) rather than institutional accountability. As Usha Ramanathan warned in 2016, one of the tragedies of Aadhaar was how it "made a villain of the recipients of state support, institutionalising the notion of the 'undeserving' poor,"[100] a move that threatens to expand, instead of curtail, the extent of deprivation in the country. **This notion criminalizes people by default, and puts the burden on people to prove their identity and inverts the idea that people are "innocent until proven guilty."** This is contrary to human rights standards, which holds that social protection is a core human right.[101]

The extent of "double dipping," that is, the idea that welfare recipients are defrauding the system by taking more than they are entitled to, has not been proved. As the Supreme Court of India held while striking down mandatory linkage of Aadhaar to bank accounts: the "mere ritualistic incantation of black money" was not sufficient to justify linking every bank account to an Aadhaar number.[102]

Does welfare need Aadhaar or did Aadhaar need welfare?

Whether the welfare systems needed Aadhaar, it was clear that the Aadhaar project needed welfare as a way to scale up quickly, regardless of its disastrous impact on beneficiaries.[103] Lobbyists pushed the government to make Aadhaar mandatory for welfare schemes to ensure that the project could reach critical mass, even as it was pending scrutiny in court.

---

[98] UN Office of the High Commissioner for Human Rights. World stumbling zombie-like into a digital welfare dystopia, warns UN human rights expert. October 17, 2019. https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25156

[99] Privacy International. Benefitting whom? An overview of companies profiting from "digital welfare". November 25, 2020. https://privacyinternational.org/long-read/4144/benefitting-whom-overview-companies-profiting-digital-welfare

[100] V. Sridhar. Threat to citizen rights. Frontline. April 14, 2016. https://frontline.thehindu.com/cover-story/threat-to-citizen-rights/article8408824.ece

[101] Magdalena Sepulveda,

[102] Supreme Court of India. Justice K.S.Puttaswamy(Retd) vs Union Of India on 26 September, 2018. https://indiankanoon.org/doc/127517806/

[103] Rethink Aadhaar. FAQs: Aadhaar and Welfare. https://rethinkaadhaar.in/faqs/welfare

Myth #5: Big ID brings efficiency

When making the case for the use of biometric authentication for social welfare delivery, software entrepreneur Nandan Nilekani said it would enable the government to go "paperless, presenceless and cashless,"[104] arguing that Aadhaar "could enable more than [300 million] daily seekers of government services to save at least two hours every day."[105]

System failures mean fewer people can access services

The introduction of Aadhaar has been best described as "Kafkaesque," a disorientingly and illogically complex system. This is best explained through an example. A recent randomized controlled trial studying the impact of Aadhaar linkage to the food distribution system in 16,000 households found that the introduction of Aadhaar modalities had *increased* the transaction costs for the average beneficiary by 17% and *reduced* the value of benefits received by 10% — in part because Aadhaar's inefficiencies necessitated multiple trips to receive benefits.[106] Similarly, a 2019 report by the research and advocacy group LibTech on how workers in India's national rural employment guarantee program experienced the payment system found that the Aadhaar-enabled system had introduced delays.[107] The survey found that 40% of workers who used "customer service points" or "business correspondents," a mechanism that relied on biometric authentication, experienced "biometric failure."

Myth #6: Big ID enables transparency

Aadhaar was also supposed to bring transparency into the welfare systems. An early report pushing for Aadhaar to play a role in the welfare delivery system promised that it would introduce authenticity to transactions, make data available "for community monitoring," strengthen the use of right to information in the public distribution system, and that an Aadhaar-enabled information technology grievance system "would ensure that complaints are visible publicly and across different levels of government."[108] Aadhaar's architect and chief evangelist went so far as to claim that Aadhaar was being demonized precisely because "it was so transparent."[109]

---

[104] Nandan Nilekani. Basis of a revolution. Indian Express. March 9, 2016. https://indianexpress.com/article/opinion/columns/aadhaar-bill-lpg-subsidy-mgnrega-paperless-govt-basis-of-a-revolution/

[105] Nandan Nilekani. Basis of a revolution. Indian Express. March 9, 2016. https://indianexpress.com/article/opinion/columns/aadhaar-bill-lpg-subsidy-mgnrega-paperless-govt-basis-of-a-revolution/

[106] Karthik Muralidharan, Paul Niehaus, and Sandip Sukhtankar. Evaluating the Aadhaar-PDS link. Hindustan Times. February 16, 2020. https://www.hindustantimes.com/columns/evaluating-the-aadhaar-pds-link/story-jZAAhL5u586zNqzqFIYhmM.html

[107] LibTech India. Length of the Last Mile. Delays and Hurdles in NREGA Wage Payments. November 2020. https://ruralindiaonline.org/en/library/resource/length-of-the-last-mile-delays-and-hurdles-in-nrega-wage-payments/

[108] Envisioning a role for Aadhaar in the Public Distribution System. India Environmental Portal. http://www.indiaenvironmentportal.org.in/files/cash-transfer-Circulated_Aadhaar_PDS_Note.pdf

[109] Nandan Nilekani: Aadhaar is being demonised because it's so transparent. Quartz India. April 13, 2017. https://qz.com/india/957607/nandan-nilekani-aadhaar-is-being-demonised-because-its-so-transparent/

Darkening the sunshine laws

In the 2000s, India's welfare system adopted several rights-based welfare laws,[110] including the Right to Information Act of 2005 and the National Food Security Act of 2006, which gave legal backing to the public system to distribute food. These laws gave citizens power to hold the government accountable by making its decisions accessible and transparent.

The Aadhaar Act and project inverted this mandate, rendering the mechanisms of the state opaque to citizens. The gains from these sunshine laws were undermined by Aadhaar's centralized, digitized system, under which "(...) decisions about you are made by a centralized server, and you don't even know what has gone wrong."[111] As a result, when people's welfare entitlements stopped, no one had clarity on how to fix it.

This tendency was repeated in the Aadhaar Payment Bridge System that replaced the existing National Electronic Funds Transfer system used by the central government to disburse welfare payments for Direct Benefits Transfers (DBT).[112] This new system led to frequently misdirected payments. The architecture was described as a "bridge to nowhere" and led to scores of payments disappearing or being credited to the wrong bank account number.[113]

Research conducted by the Indian School of Business found that "68% of total payments made under the right to work scheme in Jharkhand, which were processed through Aadhaar, were misdirected."[114] There was no mechanism for redress, or accountability, as a result of which people were not paid for their work.

Moreover, Aadhaar's architecture also created chaos in other parts of the system. Different government departments which attempted to authenticate beneficiary identities were faced with error codes that they could not decipher. [115]

---

[110] Yamini Aiyyar and Michael Walton. Rights, Accountability and Citizenship: Examining India's Emerging Welfare State. Accountability India. October 2014. https://accountabilityindia.in/sites/default/files/rights_based_welfare_state_aiyar_walton.pdf

[111] Rebecca Ratcliffe. How a glitch in India's biometric welfare system can be lethal. The Guardian. October 16, 2019. https://www.theguardian.com/technology/2019/oct/16/glitch-india-biometric-welfare-system-starvation

[112] Sakina Dhorajiwala and Niklas Wagner. Consent to nothing: Aadhaar-based payment systems in welfare. . Ideas for India. August 29, 2019. https://www.ideasforindia.in/topics/governance/consent-to-nothing-aadhaar-based-payment-systems-in-welfare.html

[113] Sakina Dhorajiwala, Jean Dreze and Niklas Wagner. A Bridge to Nowhere. The Hindu. March 27, 2019. https://www.thehindu.com/opinion/lead/a-bridge-to-nowhere/article26646131.ece

[114] Rebecca Ratcliffe. How a glitch in India's biometric welfare system can be lethal. The Guardian. October 16, 2019. https://www.theguardian.com/technology/2019/oct/16/glitch-india-biometric-welfare-system-starvation

[115] Srinivas Kodali. COVID-19, Aadhaar-DBT and a Reminder of the Issues With Transaction Failure Data. The Wire. April 15, 2020. https://thewire.in/government/covid-19-aadhaar-dbt-and-a-reminder-of-the-issues-with-transaction-failure-data

Digitalization does not mean more transparency

Tamil Nadu, a state in the south of India, is one of the few states with a universal public distribution system. A study on the impact of automating the ration delivery system found that "digitised smartcards and mobile text messages had transformed transparency for beneficiaries, and introduced new opacities and information gaps."[116] Beneficiaries who were used to recording their entitlements in a paper book had to now depend on receiving a text message. However, they found that a text message didn't have the same reliability as the written record because they depended on access to the technology to get the text messages, and the messages were in English, which few beneficiaries could read. Keeping track in a paper book was much easier for them. Thus, "digitisation changed the proof of purchase for recipients, shifted the language of communication, and enhanced reliance on mobile phone technology."[117] This reduced transparency and the space for negotiation and (re)produced earlier forms of exclusion.

Lack of accountability

Aadhaar continues to have no meaningful grievance redress mechanisms.[118] The early grievance redress processes were call centers, which were later changed into a handful of Aadhaar service centers. However, there are only 200 of these centers, which is pitiful for a country of one billion. There is also no clarity within the UIDAI on how to fix basic issues with Aadhaar. For instance, in July 2021, a report from Jharkhand noted that people who lost their Aadhaar numbers were not able to retrieve them, given the lack of a reliable and well-defined way to access a remedy for failures or glitches in the Aadhaar system with disastrous results.[119]

The type of redress for failures, glitches, and other errors that are made available affects peoples' access to their welfare benefits. As LibTech's 2019 report on the impact of Aadhaar payments in the employment guarantee scheme found, people were most comfortable making complaints orally (in person), but for those who managed to lodge a complaint, only 59% reported that their grievance had been resolved.[120]

---

[116] Grace Carswell and Grete de Neeve. Transparency, exclusion and mediation: how digital and biometric technologies are transforming social protection in Tamil Nadu, India. Oxford Development Studies. March 31, 2021. https://www.tandfonline.com/doi/full/10.1080/13600818.2021.1904866?src=recsys&

[117] Grace Carswell and Grete de Neeve. Transparency, exclusion and mediation: how digital and biometric technologies are transforming social protection in Tamil Nadu, India. Oxford Development Studies. March 31, 2021. https://www.tandfonline.com/doi/full/10.1080/13600818.2021.1904866?src=recsys&

[118] Unique Identification Authority of India. Grievance Redress. https://uidai.gov.in/contact-support/grievance-redressal.html

[119] Anil Vyom and Jean Dreze. Without Aadhaar, without identity. Indian Express. July 05, 2021. https://indianexpress.com/article/opinion/columns/flaw-in-aadhaar-architecture-uidai-card-enrolment-7389133/

[120] LibTech India. Length of the Last Mile. Delays and Hurdles in NREGA Wage Payments. November 2020. https://ruralindiaonline.org/en/library/resource/length-of-the-last-mile-delays-and-hurdles-in-nrega-wage-payments/

The UIDAI side-stepped transparency

The UIDAI refused to answer Right to Information requests on the number of Aadhaar authentication requests that had failed.[121] In its own operations, rather than enabling transparency, the UIDAI hid behind exceptions in the Right to Information Act, claiming that "national security and confidentiality" exceptions prevented disclosures about data breaches.[122]

Myth #7: Big ID is neither coercive nor mandatory

The proponents of Aadhaar kept insisting that it was wholly voluntary and not mandatory at all. Even the Supreme Court of India stated that it is an "entitlement" that, by design, was never meant to be mandatory. When Aadhaar was made mandatory, it led to disastrous consequences, with scores of people excluded from their welfare benefits.

Until the Aadhaar Act was brought into force, there was no mandatory obligation on enrolling agencies to obtain informed consent from residents who were enrolling for Aadhaar. While the 2016 Aadhaar Act mentions "informed consent," the regulations rolled out by UIDAI under the Act do not provide any guidance on how this consent is to be ensured, or give options in case persons do not want to submit their information for authentication.[123]

Schrödinger's Aadhaar: voluntary and mandatory

In practice, Aadhaar was a study in shifting standards of voluntariness because of state coercion. It was introduced as voluntary, slowly crept through the system, and became mandatory to access public and private services. It was referred to as "Schrodinger's Aadhaar."[124]

Rethink Aadhaar, a volunteer-run campaign that has been advocating against the harms caused by Aadhaar since 2016, sums up how coercive this was: the UIDAI enlists 31 acceptable ways to prove your identity and 44 ways to prove your address. However, once a person gets

[121] Anumeha Yadav. How efficient is Aadhaar? There's no way to know since the government won't tell. Scroll.in. April 5, 2017. https://scroll.in/article/833060/how-efficient-is-aadhaar-theres-no-way-to-know-as-the-government-wont-tell

[122] Anumeha Yadav. Under the right to information law, Aadhaar data breaches will remain a state secret. Scroll.in. March 5, 2017.https://scroll.in/article/830589/under-the-right-to-information-law-aadhaar-data-breaches-will-remain-a-state-secret

[123] Justice Chandrachud noted this in his dissent. See Supreme Court of India. Justice K.S.Puttaswamy(Retd) vs Union Of India on September 26, 2018. https://uidai.gov.in/images/news/Judgement_26-Sep-2018.pdf at pages 467 and 468.

[124] Zakhar Naved and Isha Kaushal. Aadhaar: Its Implementation and Implications. Christ University Journal. 2019. https://core.ac.uk/download/pdf/236436908.pdf

an Aadhaar number, they are pressured to only validate themselves through their Aadhaar numbers.[125]

Coercive consent cannot be valid

The Supreme Court found that, while Aadhaar was not mandatory, people who wanted to take advantage of welfare benefits had to enroll. Is consent valid and free when given in exchange for access to a welfare entitlement? As the International Committee of the Red Cross (ICRC) notes, consent cannot be considered valid, or provide a valid basis for data processing, in the context of an unequal power relationship.[126] Consent is not valid and free if the person has no real choice. While the Supreme Court mandated that people should be given options to authenticate themselves (or rather, that they should not be excluded "for authentication failures"), the government got around the requirement to give options by making the proof of applying for enrollment in Aadhaar itself as the alternate ID it will recognize.

Inorganic seeding

Apart from this, the whole concept of "inorganic seeding"[127] of Aadhaar numbers, as discussed above, was non-consensual by design: a person's Aadhaar number was automatically "seeded" or fed into different databases without any regard for individual consent.[128]

Myth #8: Establishing the uniqueness of individuals is a crucial need that only Big ID can fulfill

One of Big ID's major selling points is its capacity to establish individual "uniqueness," and with it the assumption that the state's ability to "see" people uniquely as they move through the system is of paramount importance. The majority bench of the Supreme Court in the

[125] Rethink Aadhaar. Myths. https://rethinkaadhaar.in/myths
[126] Ben Hayes and Masimmo Marelli. Facilitating innovation, ensuring protection: the ICRC Biometrics Policy. ICRC. October 18, 2019. https://blogs.icrc.org/law-and-policy/2019/10/18/innovation-protection-icrc-biometrics-policy/
[127] Unique Identification Authority of India. Aadhaar Workshop on Seeding. https://archive.org/details/Aadhaar_Workshop_Seeding
[128] Anand Venkatanarayan. The 360 Degree Database. December 6, 2017. Kaarana. https://medium.com/karana/the-360-degree-database-17a0f91e6a33

Aadhaar judgement also began with a quote which extolled the virtues of a unique identity,[129] and the World Bank supports this position. A 2016 report held:

> Robust unique IDs offer a number of benefits... by ensuring that each person is unique, they **reduce errors in the identification system and increase the efficiency of identity records** management over time and across agencies. These improvements can have direct financial benefits by reducing operating and administrative costs for identity providers. Furthermore, unique IDs can indirectly increase savings and revenue generation opportunities by enabling other features of identification systems. For example, when used as a "key" or common reference across identity databases and systems, unique IDs enable many of the benefits associated with integration and interoperability described below. In addition, unique IDs typically precede and strengthen the robustness of digital authentication processes and services.[130]

The promise of Big ID programs is, as researcher Ursula Rao points out, that they can "provide automated surveillance at crucial checkpoints in order to protect spaces of privileged sociality against unwanted entrants — in short, they offer a means to separate 'bad' flows from 'good' flows."[131] But why does the state really need to track people "uniquely" as they interact with the government or move through life, and how can it be justified in the face of such heightened privacy risks?

Tying people to a unique identity confuses the idea of an "identity" with a mode of identification

The system pins people down to just one identity and infringes on their right to identify themselves with choice. Justice Chandrachud's dissent, in which he struck down the Aadhaar project as a whole, captured the dangers of this approach.[132] He pointed out that the notion that individuals possess only one or at least a dominant identity is not a sound constitutional principle and that people have the right to hold *different* identities and to be identified how they choose. He also said that the multiplicity of identities is a key right in a networked society, where individuals have the right to determine the forms through which their identity is expressed, including the right to not be identified. The multiplicity of identities is a

---

[129] The Wire. 'Better to Be Unique Than the Best' – Highlights From the Majority Judgment on Aadhaar. September 26, 2018. https://thewire.in/law/highlights-majority-judgment-aadhaar-act ("It is better to be unique than to be best, because being the best makes you the number one, but being unique makes you the only one.")

[130] The World Bank. Digital Dividends. 2016. https://documents1.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf

[131] Ursula Rao. Biometric IDs and the remaking of the Indian (welfare) state. November 2019. economic sociology_the european electronic newsletter. https://econsoc.mpifg.de/38379/03_Rao_Econsoc-NL_21-1_Nov2019.pdf

[132] Supreme Court of India. Justice K.S.Puttaswamy(Retd) vs Union Of India on September 26, 2018. https://uidai.gov.in/images/news/Judgement_26-Sep-2018.pdf

constitutional right, which cannot be obliterated by an "instrument which facilitates proof of an identity."[133]

Interoperability, in the absence of data privacy safeguards, poses a serious surveillance threat

A unique Big ID promises interoperability as the unique ID acts as a sort of key to integrate and link different databases. Giving the government the capacity to track a person across different databases bolsters its capacity for surveillance and is a serious threat to privacy. This could also be done without the person's consent, which is a serious problem. True interoperability places the user and their control over their information at the center of systems; it otherwise constitutes surveillance under the guise of interoperability.

This surveillance harms the right to privacy — a fundamental human right enshrined in many human rights instruments. It is foundational, as the Supreme Court of India's landmark judgement affirming the right to privacy held, to the dignity and autonomy of a person and enables a person to enjoy other rights accorded to them.[134] The right includes a person's bodily integrity, control over their information, and a person's right to choose. Although the right is not absolute, there are conditions constraining how and the extent to which it can be infringed. A measure that infringes the right to privacy is permissible only if it meets a specific and targeted test called the proportionality test. This is a three-part evaluation of whether a violation of privacy is permissible to achieve a particular aim. First, is there a legal basis for the proposed aim? Second, is the proposed measure *proportionate* to achieve that aim? Third, is the proposed measure *necessary* to achieve that aim, or in other words, are there less restrictive means available to achieve the same desired effect? Importantly, whether a proposed measure meets the proportionality test has to be tested on a **case-by-case** basis. The decision to link different databases neither meets the requirements of legality, necessity, or proportionality nor is it justified on a case-by-case basis.

Myth #9: Big ID is needed for financial inclusion

The need for financial inclusion is one of the key motivators for Big IDs. Backed by international players like the World Bank and Mastercard, a digital ID is sold as the way to capture the vast numbers of the "unbanked," or those who lack "access to formal financial

[133] Supreme Court of India. Justice K.S.Puttaswamy(Retd) vs Union Of India on September 26, 2018.https://uidai.gov.in/images/news/Judgement_26-Sep-2018.pdf at page 350.
[134] Supreme Court of India. Justice K.S.Puttaswamy(Retd) vs Union Of India (Writ Petition No. 494 of 2012) on August 24, 2017. https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf

services."[135] Financial inclusion has been identified as an enabler for seven of the 17 Sustainable Development Goals; and the World Bank Group "considers financial inclusion a key enabler to reduce extreme poverty and boost shared prosperity" and has put forward an ambitious global goal to reach Universal Financial Access by 2020.[136] A 2016 report by the World Economic Forum emphasized the importance of identity to financial services.[137]

The World Bank considers financial inclusion to be a key "enabler to reduce poverty and boost prosperity."[138] In India, Aadhaar was the cornerstone of what the central government called a "JAM trinity," which proposed to gather all citizens into the net of a "Jan dhan" ('peoples' wealth') bank account, a digital identity (Aadhaar), and a Mobile phone connection.

However, the notion of what exactly financial inclusion means, who it benefits, and why it should look so data-heavy, bears unpacking. The vision pushed by the Big ID evangelists, including the International Telecommunication Union (ITU) and IndiaStack,[139], is that of a "presenceless, paperless, cashless" service delivery model, which treats consent as a technical "layer" that "allows data to move freely and securely to democratise data".[140]

What are the ID requirements, really?

Under international norms to prevent financial fraud, and terror financing, financial institutions are required to identify customers. The responsibility to adhere to Know Your Customer (KYC) rules and the requirements of the Financial Action Task Force are often pointed to when justifying why a national biometric database is a prerequisite for financial inclusion. The question to ask is what *level* of identity authentication is required to transact safely. Experts have found that the KYC norms followed in India under the Prevention of Money Laundering Act are "excessively prescriptive," particularly when it comes to requirements for proof of address.[141] Many countries have enabled high levels of digital service delivery without a national, centralized database and biometrics, and as the failures in the welfare system show, biometric authentication doesn't offer much other than a point of failure. Other less harmful models of authenticating your identity exist.

---

[135] Mastercard. MasterCard Hosts A Cashless Conversation on Financial Inclusion: Panel Discussion. https://newsroom.mastercard.com/videos/mastercard-hosts-a-cashless-conversation-on-financial-inclusion-panel-discussion/

[136] World Bank. Financial Inclusion: Overview. https://www.worldbank.org/en/topic/financialinclusion

[137] World Economic Forum. A Blueprint for Digital Identity. August 2016. http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

[138] World Bank. Financial Inclusion: Overview. https://www.worldbank.org/en/topic/financialinclusion

[139] India Stack. https://www.indiastack.org/about/

[140] India Stack. https://www.indiastack.org/about/

[141] Rishab Bailey, Trishee Goyal, Renuka Sane and Ridhi Varma. Analysing India's KYC Framework: Can We Do Things Better? National Institute of Public Finance and Policy. January 22, 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3776008

Why are people unbanked?

Lack of ID is neither the only nor most important reason why people are not included in the formal financial market.[142] The banking system has limited reach, particularly in rural India, and the banking sector is often reluctant to take on the costs of financing new, low-worth customers. There was no basis for the myth that a lack of ID was preventing financial inclusion. A 2017 report by the World Bank noted that 31% of adults worldwide are unbanked.[143] When asked why, the "most commonly cited barrier was lack of enough money." The report also found that nearly two-thirds of adults without an account at a financial institution said that they have too little money to use one, and roughly one in five cited this as their sole reason for not having one. This was echoed in a similar report from India: the 2017 Findex survey found that, among 3,000 respondents, the most common reason given for not having a bank account was having insufficient funds, followed by "living too remotely," and services being too expensive.[144] One of the biggest reasons for the lack of banking infrastructure at the village level is the high operational costs. A brick-and-mortar bank requires staff, paperwork, and physical presence — all costs that may not be returnable.

What is presenceless, paperless, and cashless, and who benefits from it?

The Aadhaar model of financial inclusion seeks to eliminate operational and transactional costs by gathering data to make more sophisticated financial products and enable greater access to credit. This system is designed to create digital footprints that would, in the candid words of the Aadhaar architect Nandan Nilekani, "bring millions of consumers and small businesses (who are in the informal sector) to join the formal economy to avail of affordable and reliable credit," adding, "(a)nd as data becomes the new currency, financial institutions will be willing to forego transaction fees to get rich digital information on their customers."[145] "Presenceless" means reliance on digital authentication (like Aadhaar); "paperless" indicates removing the need for records or rooms to store those records; and "cashless" means a switch to digital payments. And "consent" has been reframed as a measure to secure the "free and secure movement of data."[146]

---

[142] Sriram. Moving Beyond Aadhaar: Identity for Inclusion. Economic & Political Weekly, July 12, 2014. https://www.epw.in/journal/2014/28/special-articles/identity-inclusion.html

[143] World Bank. Chapter 2: The Unbanked. 2018.https://globalfindex.worldbank.org/sites/globalfindex/files/chapters/2017%20Findex%20full%20report_chapter2.pdf

[144] Asli Demirgüç-Kunt, Leora Klapper, Dorothe Singer, Saniya Ansar Jake Hess. 2018. The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution. World Bank. https://openknowledge.worldbank.org/bitstream/handle/10986/29510/211259ov.pdf

[145] Credit Suisse Securities Research and Analytics. India Financials Sector. June 2016. https://plus.credit-suisse.com/rpc4/ravDocView?docid=qDx15C

[146] Kathryn Henne. Surveillance in the Name of Governance: Aadhaar as a Fix for Leaking Systems in India. June 22, 2019. Information, Technology and Control in a Changing World. Pages 223-245.

Removing cash from the financial system is not necessarily pro-poor: it shifts a crucial cost (of handling cash and having a network of brick-and-mortar banks) onto the consumer, while creating digital trails which can be mined for data and insight.[147] Second, the data trail can reveal more than intended about people's spending patterns, particularly in the absence of data protection laws. Digital methods are also not "cleaner" than cash or better at reducing corruption. The global Financial Action Task Force had expressed concerns about the impact of digital financial inclusion on anti-money-laundering and anti-terrorism-financing efforts.[148] As Phil Mader, a research fellow at the Institute of Development Studies, notes, "if the mission really is poverty alleviation, it's not money's physical form, but how it is distributed, that matters."[149]

Is digital financial inclusion the only answer?

Access to people's data is a key element in this model of financial inclusion being sold. People seeking accounts, and loans, have to hand over their data in exchange. This upholds a data-extractive system, referred to as the "fintech-philanthropy-development complex."[150] This creates a structure that uses people and can harm individuals. In India, COVID-19 saw the rise of shady predatory loan applications that abused unfettered access to mobile phone data and contact lists to harass and shame borrowers, which in some cases, had tragic results.[151] Acting on research conducted by Cashless Consumer expert Srikanth Lakshmanan, Google has taken down these apps, and the Reserve Bank of India has issued guidelines.[152]

Is digital financial inclusion necessary?

The focus on data-heavy models also diverts resources and attention away from non-tech innovations for access to finance. At the same time, a mandatory shift to cashless transactions affects people living in poverty disproportionately, as the informal economy usually relies on cash.

---

https://link.springer.com/chapter/10.1007/978-3-030-14540-8_11#CR28

[147] Phil Mader. Why the Crusade Against Cash Isn't Clearly 'Pro-Poor'. December 22, 2017. https://nextbillion.net/why-the-crusade-against-cash-isnt-clearly-pro-poor/

[148] The Financial Action Task Force. FATF Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion. June 2011. http://www.fatf-gafi.org/publications/financialinclusion/documents/fatfguidanceonanti-moneylaunderingandterroristfinancingmeasuresandfinancialinclusion.html

[149] Phil Mader. Why the Crusade Against Cash Isn't Clearly 'Pro-Poor'. December 22, 2017. https://nextbillion.net/why-the-crusade-against-cash-isnt-clearly-pro-poor/

[150] Daniel Gabor and Sally Brook. The digital revolution in financial inclusion: international development in the fintech era. November 28, 2016. https://www.tandfonline.com/doi/abs/10.1080/13563467.2017.1259298

[151] Wired. Shame, suicide and the dodgy loan apps plaguing Google's Play Store. January 21, 2020. https://www.wired.co.uk/article/google-loan-apps-india-deaths

[152] Reserve Bank of India. RBI Cautions against unauthorised Digital Lending Platforms/Mobile Apps. December 23, 2020. https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=50846

Keith Breckenridge, who has worked extensively on digital identity, suggests that this focus on issuing digital identities can be "understood as the instrument of a new digital capitalism, one less concerned with including individuals and 'vulnerable groups' within civic life, and more with sorting them depending on their financial solvency."[153]

What are the safeguards?

There are also dangers in linking social protection measures with financial inclusion, as it assumes a level of knowledge of how the financial sector works which is not always present in beneficiaries.[154] Often, recipients are not taught to safely engage with the financial sector, which can result in fraud and exclusions. Predatory loans can also lead to debt traps that are difficult to get out of.[155]

Did Aadhaar linkage help welfare payments?

The manner in which the Aadhaar linkage occurred disrupted the existing financial system through which welfare payments were being made. As a 2019 study by researchers with LibTech on the impact of Aadhaar on the banking sector found, the process of "seeding" Aadhaar with bank accounts to link welfare schemes and cash transfers with the Aadhaar payment systems was done with no thought, understanding, or sensitivity and created chaos on the ground. One banker interviewed in the study said, "the government created a huge mess by introducing an untested system coercively."[156]

Myth #10: Biometric verification is necessary, safe, and reliable

Biometrics verification is being sold as a part of Big ID programs as the "safest" way to verify and deduplicate (or detect duplicate registrations of) identities. Biometric systems collect and store a representation of a person's physiological characteristics, biological properties, behavioral aspects such as, but not limited to, fingerprints, facial features, irises, and retinal veins. Biometric verification can be either one-to-one (checking a saved fingerprint against one provided on the spot) or one-to-many (checking the input against the whole database). The first is used to authenticate an identity, while the second to deduplicate. Sunil Abraham

[153] Keith Breckenridge. The failure of the "single source of truth about Kenyans": the National Digital Registry System, collateral mysteries and the Safaricom monopoly. August 23, 2017. https://wiser.wits.ac.za/sites/default/files/12_Kenya-FinalBeforeWordConv.pdf

[154] Sarina Kidd. The perils of linking social protection to financial inclusion. Development Pathways. August 21, 2020. https://www.developmentpathways.co.uk/blog/the-perils-of-linking-social-protection-to-financial-inclusion/

[155] Soutik Biswas, India's micro-finance suicide epidemic. BBC. December 16, 2010. https://www.bbc.com/news/world-south-asia-11997571

[156] Sakina Dhorajiwala and Niklas Wagner. Consent to nothing: Aadhaar-based payment systems in welfare. Ideas for India. August 23, 2019. https://www.ideasforindia.in/topics/governance/consent-to-nothing-aadhaar-based-payment-systems-in-welfare.html

succinctly lists all that can go wrong with a biometric identification system.[157] They can be used remotely, covertly, and nonconsensually. They are not reliable, as they are based on probabilistic matching. They usually need to be stored in a centralized network, which is a honey pot for cyberattacks. They are irrevocable, can always be tricked by ever more sophisticated deception techniques, and depend on technology that is opaque and often proprietary. As Justice Chandrachud notes in his dissent, "Once compromised, a biometric database is compromised forever."[158]

Biometrics are a threat to dignity

The collection and use of biometrics pose a serious threat to the right to privacy, integrity, and the right to equality and nondiscrimination, among other human rights.

Justice Chandrachud's dissent on the validity of Aadhaar notes:

> Biometric data, by its very nature, is intrinsically linked to characteristics that make us 'humans' and its broad scope brings together a variety of personal elements… Ultimately, organisations and governmental agencies must demonstrate that there is a compelling legitimate interest in using biometric technology and that an obligatory fingerprint requirement is reasonably related to the objective for which it is required. One way of avoiding unnecessary collection of biometric data is to set strict legal standards to ensure that the intrusion into privacy is commensurate with and proportional to the need for collection of biometric data.[159]

When the Aadhaar project was being discussed before the Parliament of India in 2010, an expert, Dr. R. Ramkumar, said that errors in biometric authentication had been evident in as high as 15% of the population, namely those who work with their hands.[160] This figure was considered sufficiently high for the standing committee to reject the bill, but the risk was considered sufficiently low for the project to move along, and another bill (which became the Aadhaar Act) was introduced in 2016.

Are biometrics the safest and least intrusive methods of authentication?

Biometrics are not the only way to verify identities. Other options include photo-ID checks, scanning barcodes, inputting passwords and PINs, and using one-time passwords or codes

---

[157] Sunil Abraham. It's the technology, stupid. The Center for Internet and Society. March 31, 2017. https://cis-india.org/internet-governance/blog/the-hindu-businessline-march-31-2017-sunil-abraham-its-the-technology-stupid/

[158] Supreme Court of India. Justice K.S.Puttaswamy(Retd) vs Union Of India on 26 September, 2018. https://uidai.gov.in/images/news/Judgement_26-Sep-2018.pdf. Pg. 467.

[159] Supreme Court of India. Justice K.S.Puttaswamy(Retd) vs Union Of India on 26 September, 2018. https://uidai.gov.in/images/news/Judgement_26-Sep-2018.pdf

[160] Standing Committee on Finance (2011-2012). Forty-Second Report. The National Identification Authority of India Bill, 2010.https://uidai.gov.in/images/report_of_the_departmental_standing_committee_on_finance_on_the_bill_13012017.pdf. Pages 11 and 26.

(OTPs) sent to phones. From being a feature in sci-fi movies, today biometric authentication has become relatively ubiquitous in daily life without the core questions being addressed: are they useful, necessary, and safe?

Given the high risk they pose to privacy, the state needs to show the justification for endangering its citizenry by imposing biometric authentication programs. Should biometric authentication programs be a requirement to walk into an airport, get your monthly rations from the neighborhood store, or obtain a ration card or SIM card? Should access to these spaces or services be treated on par with the safeguards to enter a sensitive government building?

The necessity and proportionality of the authentication standard must be reviewed on a case-by-case basis for each use case, and it needs to be proved that such biometric authentication is completely safe, inclusive, and not liable to error and is the only available means to authenticate identity. Take attendance in schools, for instance, where identity verification was a simple roll call. This works because the teacher knows you. If you go to another school for an exam, you have to show an ID. Aadhaar was beginning to be used as a way to verify children's identities, but was struck down by the majority decision, which held that this did not meet the proportionality standard. Similarly, the majority judgement of the Supreme Court was quick to point out how mandating Aadhaar linkage and a biometric deduplication process for all bank accounts was not, in fact, proportional. The court said the "mere ritualistic incantation of black money" was not sufficient to justify linking every bank account to Aadhaar. The purpose creep of biometrics is also a real threat. Once their use is normalized, they become an attractive resource for private commercial exploitation.

Is biometric verification reliable?

Biometric authentication is based on probabilistic matching. However the reliability of biometric authentication is overstated. Biometric information is just a type of information that "offers representations of bodily attributes captured at a particular moment in time under specific material conditions, and of no greater epistemic caliber [than demographic data]."[161]

[161] Nayantara Ranganathan. The Economy and Regulatory Practice that Biometrics Inspire: A study of the Aadhaar Project. AI Now. https://ainowinstitute.org/regulatingbiometrics-ranganathan.pdf

Researchers warned of "false positives," or new entries into the database being falsely flagged as duplicates. At scale, this is an incredibly high number — almost 69 million enrolments were rejected.[162]

In India, the envisioned lack of reliability of fingerprint authentications led to increasing the range of biometric attributes collected (engineers decided to include scans of irises in the database to reduce the margin of error for false positives during the deduplication process). Experts also drew attention to the increasing rate of "false negatives" because of the unreliable underlying technology.[163] Realizing that biometrics are susceptible to change with time, the Aadhaar Act imposes a duty on persons enrolled within Aadhaar to periodically update their biometric records, thus expanding the types of biometric attributes collected.

Myth #11: Big ID systems ensure that your personal information is safe

The UIDAI claimed that the Aadhaar database was secure, stressing the sufficiency of legal and technical measures to ensure the sanctity of the data in the central system.[164] The argument was that, because the Central Information Database (CIDR) — the centralized database maintained by the central Aadhaar authority — was secure, Aadhaar was secure.

Legal flaws

Although the Aadhaar Act[165] and the Authentication Regulations[166] prohibit persons, entities, or agencies from displaying a person's Aadhaar number, there are no obligations on the UIDAI to give notice to an individual in case of a breach of his or her information, an established principle of data privacy laws.

Lack of institutional accountability

The UIDAI failed to take responsibility for data breaches and for giving people guidance on how to protect their data. Instead of rewarding public interventions, the UIDAI filed criminal

[162] V. Anand. Guest Post: The Aadhaar Judgment and Reality – I: On Uniqueness. September 28, 2018. https://indconlawphil.wordpress.com/2018/09/27/guest-post-the-aadhaar-judgment-and-reality-i-on-uniqueness/

[163] Aadhaar as a hurdle: On authentication failures and welfare delivery. The Hindu. https://www.thehindu.com/opinion/editorial/aadhaar-as-a-hurdle-the-hindu-editorial-on-biometric-authentication-failures-and-welfare-delivery/article34102754.ece

[164] The Hindu. Aadhaar data safe behind five-feet thick walls, govt. affirms in Supreme Court, March 21, 2018. https://www.thehindu.com/news/national/aadhaar-data-safe-behind-five-feet-thick-walls-centre-tells-supreme-court/article23313608.ece

[165] Government of India. The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf

[166] Government of India. The Aadhaar (Authentication) Regulations, 2016. https://uidai.gov.in/images/regulation_1_to_5_15092016.pdf.

proceedings against researchers uncovering flaws in its security system.[167] For years, the UIDAI did not have a chief information security officer.[168]

Design flaws

There were design flaws in the enrollment system. Enrollers were private entities that had been given targets to incentivize enrollment.[169] This incentive structure resulted in the database being full of fake names. People were arbitrarily assigned the same birthdate: January 1, with different years.[170]

Widespread use of the number

The concept of "seeding" Aadhaar numbers, which was actively pushed by the proponents of Aadhaar, meant that people's Aadhaar numbers were put into different private and government databases,[171] where they could be copied from.[172] *What could a person do with an Aadhaar number?* In an act of bravado, the first Director General of UIDAI, Ram Sewak Sharma, published his Aadhaar number publicly in a bid to show how safe it was.[173] Security activists reacted swiftly, creating new bank accounts in his name and unearthing personal material.[174]

Single point of failure

Contrary to the UIDAI's claims, the central database where Aadhaar data was stored could be breached to input or pull out data.[175] Illegal data markets abound in India,[176] where Aadhaar

---

[167] Rohan Venkatramakrishnan. What Aadhaar authority UIDAI can learn from Zomato when it comes to hacking and data breaches. May 27, 2017. Scroll.in. https://scroll.in/article/838137/what-the-aadhaar-authority-needs-to-learn-from-zomatos-response-to-hacking

[168] Moneylife. Aadhaar Truth: UIDAI Never Appointed a Chief Information Security Officer, Reveals RTI. February 19, 2019. moneylife.in/article/aadhaar-truth-uidai-never-appointed-a-chief-information-security-officer-reveals-rti/56267.html

[169] Moneylife. Dr Goyal exposes vulnerabilities in Aadhaar architecture and ecosystem before the Supreme Court. February 21, 2018. https://www.moneylife.in/article/dr-goyal-exposes-vulnerabilities-in-aadhaar-architecture-and-ecosystem-before-the-supreme-court-part1/53161.html

[170] Scroll.in. "Aadhaar: UIDAI says January 1 birth date assigned to 1,000 UP villagers was policy, not 'goof up'." May 25, 2017. https://scroll.in/latest/838646/put-jan-1-as-birth-date-on-1000-aadhaar-cards-as-many-dont-know-when-they-were-born-says-uidai; Also *see* Scroll.in. "Everyone in this Uttarakhand village has the same birth date on their Aadhaar cards." October 28, 2017. https://scroll.in/latest/855731/everyone-in-this-uttarakhand-village-has-the-same-birth-date-on-their-aadhaar-cards

[171] Zack Whittakar. Indian state government leaks thousands of Aadhaar numbers. TechCrunch. February 1, 2018. https://techcrunch.com/2019/01/31/aadhaar-data-leak/

[172] Scroll.in. Security researcher finds serious flaw in Aadhaar system that leaves data open for download: Report. March 24, 2018. https://scroll.in/latest/873159/security-researcher-finds-serious-flaw-in-aadhaar-system-that-leaves-data-open-for-download-report

[173] The Print. What harm can you do to me if you have my Aadhaar details, asks TRAI Chairman RS Sharma. July 27, 2018. https://theprint.in/india/governance/what-harm-can-you-do-to-me-if-you-have-my-aadhaar-details-asks-trai-chairman-r-s-sharma/88798/

[174] Srinivas Kodali. The R.S. Sharma Fiasco is Proof of Aadhaar's Inescapable Nature. July 30, 2018. The Wire. https://thewire.in/tech/rs-sharma-aadhaar-challenge-twitter

[175] The Tribune. Rs 500, 10 minutes, and you have access to billion Aadhaar details. January 5, 2018. https://www.tribuneindia.com/news/archive/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details-523361

[176] Snigdha Poonam and Samarth Bansal. Inside India's Booming Dark Data Economy. December 22, 2020. Rest of the World. https://restofworld.org/2020/all-the-data-fit-to-sell/

details are available for sale. Enrollers' fingerprints could be duplicated and used to create new IDs. Aadhaar's architecture and lack of accountability resulted in vast leakages of Aadhaar numbers — in 2018,[177] an Aadhaar leak was named that year's biggest data breach.[178] For less than 10 dollars, a buyer could get information on anyone in the CIDR via an illegal "gateway" into the UIDAI portal.[179] This was just one of many data leaks.[180] Other government departments that collected Aadhaar data were also insecure. For example, in 2018, reproductive health information of almost 200,000 women were leaked.[181]

Researchers have extensively documented the range of Aadhaar-enabled frauds that have grown over the last decade.[182] This includes identity theft, fingerprints of enrollers being faked (using fingerprint molds) to generate hundreds of fake Aadhaars, markets where fingerprint molds can be bought, and bank frauds. Some of this was due to government websites with open web directories that had PDF scans of dozens of Aadhaar cards available to view and download.[183]

Myth #12: Big ID is a reliable tool for national security

Big ID programs are a security establishment's dream. Section 33 of the Aadhaar Act permits data to be shared with a requesting entity "in the interest of national security," a power that is curtailed with no checks or balances.[184] However, in many ways, the design of the Aadhaar project also introduced a lack of safety by permitting "offline verification" of a piece of paper that lacked the necessary safeguards of identity cards, like holograms.

Enrollment targets with no verification

[177] Firstpost. Aadhaar Security Breaches: Here are the Major Untoward Incidents that happened with Aadhaar and what was actually affected. September 25, 2018. https://www.firstpost.com/tech/news-analysis/aadhaar-security-breaches-here-are-the-major-untoward-incidents-that-have-happened-with-aadhaar-and-what-was-actually-affected-4300349.html

[178] Avast Blog. 10 of the Biggest Data Breaches in 2018. December 20, 2018. https://blog.avast.com/biggest-data-breaches

[179] The Tribune. Rs 500, 10 minutes, and you have access to billion Aadhaar details. January 5, 2018.https://www.tribuneindia.com/news/archive/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details-523361

[180] Asheeta Regidi. IT Grids Aadhaar data leak: UIDAI's implicit acknowledgement of a large-scale data breach will be very welcome to anti-Aadhaar activists. April 15, 2019. Firstpost. https://www.firstpost.com/india/it-grids-aadhaar-data-leak-uidais-implicit-acknowledgement-of-a-large-scale-data-breach-will-be-very-welcome-to-anti-aadhaar-activists-6452011.html

[181] Vidyut. AP govt leaks mobile, Aadhaar and pregnancy info of 20,71,913 women. Medianama. 2018. https://www.medianama.com/2018/04/223-ap-govt-leaks-mobile-aadhaar-pregnancy-info/

[182] Anmol Somanchi. Aadhaar Fraud is Not Only Real But Worth Examining. May 3, 2018. The Wire. https://thewire.in/economy/aadhaar-fraud-uidai

[183] Karan Saini. Aadhaar Remains an Unending Security Nightmare for a Billion Indians. May 11, 2018. The Wire. https://thewire.in/government/aadhaar-remains-an-unending-security-nightmare-for-a-billion-indians

[184] Government of India. The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. .https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf

Aadhaar enrollers were given enrollment targets to incentivize how many persons they were enrolling. This resulted in mass enrollments. The documents used to enroll were not verified by the enrollers, which led to the database being riddled with fake names: a dog, a spy, and a Hindu god have all been issued Aadhaar cards.[185]

Widespread use of a printout as a "card"

The Aadhaar Act only refers to the Aadhaar number. Despite this, the Aadhaar "card" (the printout of the Aadhaar number) is used as a substitute for a photo ID. This diminishes security, as this card is only a printout of the Aadhaar number and lacks traditional security features present in other photo IDs, like a microchip, hologram, or an official seal.[186]

Foreign players

The Court did not address the question of the security implications of UIDAI or the Indian government not owning the source-code for the deduplication technology, which was owned by a foreign licensee.[187]

---

[185] Kuwar Singh. India has over a billion Aadhaar IDs, including for dogs, spies and even gods. October 10, 2018. Quartz India. https://qz.com/india/1402415/indias-uidai-has-issued-aadhaars-to-dogs-spies-and-gods/

[186] Mardav Jain. The Aadhaar Card: Cybersecurity Issues with India's Biometric Experiment. May 9. 2019. Henry M. Jackson School of International Studies, University of Washington. https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/#_ftn11

[187] Asheeta Regidi. Aadhaar hearing: Lack of governmental ownership of CIDR's Source Code Can Have Serious Consequences. FirstPost. January 26, 2018. https://www.firstpost.com/india/aadhaar-hearing-lack-of-governmental-ownership-of-the-cidrs-source-code-can-affect-its-status-as-a-protected-system-4320625.html

A summary of common dangerous myths used to lobby for Big ID programs

MYTH	REFUTATION
Myth #1 **Big ID is needed to give people a legal identity**	➔ This conflates the legal right to identification with a digital identity. *Who* is identified is a political decision, *how* this is done digitally is a technical consideration. ➔ A digital identity adds a layer of digital authentication on top of the legal identity. The result is that the digital layer can create a barrier to someone being identified, in potential violation of the legal right to identification. ➔ Big ID promises "visibility," without examining whether this is always safe and desirable. Persons at risk and vulnerable communities like refugees, religious and caste minorities, journalists, dissidents, and activists are already over-surveilled, and do not necessarily desire to be more visible to the state on a universal basis. ➔ In India, most Aadhaar cards were issued to those who already had IDs.[188]
Myth #2 **Big ID is needed to empower people**	➔ A digital ID cannot fix the social and political causes of exclusion of underprivileged or otherwise marginalized individuals and communities. ➔ Aadhaar caused mass exclusion of individuals from welfare systems and schools, in effect, taking power away from people by centralizing decision-making, tying people to a single mode of authentication for all government services, and adding barriers to how they could access welfare entitlements and social services. ➔ Big IDs give states more power by centralizing information about people within their borders. ➔ Big ID was used to empower the private sector in India, who influenced the design of the Aadhaar project, and subsequently used its open-API architecture to develop products, many of which were data-extractive and undermined privacy and data protection.

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

Myth #3 **A Big ID does not create a surveillance state**	➔ The law and design of Aadhaar enabled surveillance. Government notifications that mandated one's Aadhaar identification number be used to link different databases, enabled the government to track a person. ➔ Different states used Aadhaar data to create a panopticon and a "360-degree surveillance" system. ➔ Certain Indian state governments even created a dashboard that was searchable by caste and religion.[189] The power to track, sort and surveil citizens can be easily abused, particularly by an authoritarian government. ➔ The lack of appropriate legislation or safeguards protecting against surveillance imperils this. India has a pressing need for surveillance reform, and many central agencies have practically unfettered power to "intercept, monitor, and decrypt all data contained in any computer."[190] ➔ India still lacks a data protection law — this exacerbates the possibility that data can be misused.[191]
Myth #4 **Big ID is needed to reform the welfare state**	➔ Aadhaar created another barrier to eligibility for welfare entitlements. ➔ Administrative disruptions caused by the introduction of Big ID caused massive exclusions from welfare systems,[192] which even led to starvation deaths. Just in 2017, around two million individuals were excluded, every month, from the food distribution system because of Aadhaar-related reasons. ➔ A digital ID system can only, if at all, counter identity fraud. This is just one of three common types of fraud that welfare systems usually have, in addition to eligibility fraud and quantity fraud. ➔ Digital ID systems do not always result in government expenditure savings that offset their establishment costs and other harms. The extent of identity fraud is contested. Claims of savings in government

[189] Aman Sethi. AADHAAR Seeding Fiasco: How To Geo-Locate By Caste and Religion In Andhra Pradesh With One Click. April 25, 2018. https://www.huffpost.com/archive/in/entry/aadhaar-seeding-fiasco-how-to-geo-locate-every-minority-family-in-ap-with-one-click_a_23419643

[190] Apar Gupta. Is India Becoming A Surveillance State? December 23, 2018. https://www.bloombergquint.com/opinion/is-india-becoming-a-surveillance-state

[191] Raman Jit Singh Chima, Naman Aggarwal and Estelle Massé. India's proposed data protection bill: further work is needed to ensure true privacy for the next billion users. February 25, 2020.https://www.accessnow.org/indias-proposed-data-protection-bill-further-work-is-needed-to-ensure-true-privacy-for-the-next-billion-users/

[192] Nikhil Dey and Aruna Roy. Excluded by Aadhaar. June 5, 2017. https://indianexpress.com/article/opinion/columns/excluded-by-aadhaar-4689083/

	expenditure due to Aadhaar were found to be grossly inflated by the government[193] and international organizations.[194] Big ID systems are often rolled out without any factual or evidential proof of the extent of this type of fraud. ➔ The focus on digital ID systems takes attention and resources away from other necessary reforms and interventions[195] and diverts focus from the quality of public services, their impact on the public's wellbeing, and exclusions.[196] ➔ Targeting of government services and welfare benefits using digital identity is a form of problematic fiscal austerity which has a detrimental impact on welfare systems. Whether this improves inequality is contested by economists. Minute targeting adds a high administrative burden that diverts resources, and impacts the quality of the public good or service. A focus on targeting and cleaning the rolls also reframes welfare recipients as needing to be "deserving." ➔ This is also a convenient myth. Private sector proponents of the Aadhaar project piggybacked on the claim that it was needed to reform the welfare system and used this as a way to scale up the project quickly rather than providing what individuals wanted.
Myth #5 **A Big ID brings efficiency**	➔ The digital infrastructure introduced by Aadhaar is difficult to navigate. It has been described as "Kafkaesque," for introducing a disorienting and illogically complex system.[197] ➔ In India, studies found that the introduction of Aadhaar-linked payment modalities *increased* transaction costs for the average beneficiaries, and delayed payments.[198]

[193] Nizam Pasha. Data Put Forth by the Modi Government on Aadhaar Is Anything but Authentic. May 28, 2018. https://thewire.in/government/data-put-forth-by-the-modi-government-on-aadhaar-is-anything-but-authentic

[194] Jean Drèze and Reetika Khera. Aadhaar's $11-bn question: The numbers being touted by govt have no solid basis. February 08, 2018. https://economictimes.indiatimes.com/news/economy/policy/aadhaars-11-bn-question-the-numbers-being-touted-by-govt-have-no-solid-basis/articleshow/62830705.cms?from=mdr

[195] Reetika Khera. Viable solutions to PDS portability are being ignored in the push for Aadhaar. November 28, 2019. https://indianexpress.com/article/opinion/columns/aadhaar-pds-public-distribution-system-6140150/

[196] Ursula Rao. Biometric IDs and the remaking of the Indian (welfare) state. November 2019. https://econsoc.mpifg.de/38379/03_Rao_Econsoc-NL_21-1_Nov2019.pdf

[197] Ritvik Khare. Aadhaar: Kafka's ghost has come back to haunt us. July 5, 2017. https://www.newslaundry.com/2017/07/05/aadhaar-kafkas-ghost-has-come-back-to-haunt-us

[198] LibTech India. Length of the Last Mile. November 2020. https://libtech.in/wp-content/uploads/2020/11/LoLM_ExecutiveSummary_English.pdf

Myth #6 **Big ID enables transparency**	➔ Big IDs introduce centralized decision-making systems for authenticating identities, where decisions are made within an opaque "black box." This opacity subverts governance and participatory gains brought in by "sunshine" laws, such as right to information laws. This made scrutiny and accountability by local communities much harder by forcing linkage to one national digital system instead of decentralized systems that are closer and more accountable to location populations. ➔ Research has found how the process of digitization can diminish transparency for beneficiaries by introducing "new opacities and information gaps." ➔ The Unique Identification Authority of India itself operated in a nontransparent manner, refusing to answer several right to information requests,[199] including on the number of Aadhaar authentication requests that had failed. ➔ A decentralized system built on transparency would permit more scrutiny and accountability.
Myth #7 **Big ID is not coercive or mandatory**	➔ Consent cannot be considered to be valid and free if people are given no viable alternatives, or if their consent is mandatory to authenticate their identity and receive welfare support. ➔ Although Aadhaar was introduced as voluntary, it gradually became *de facto* mandatory, as more and more public and private services demanded Aadhaar-based identification as a basis for access.[200] ➔ The Indian Supreme Court ordered the Unique Identification Authority of India to give people choice in how they could enrol, but the choice the Authority offered, in the Aadhaar Act, was illusory. The proof that you had enrolled for Aadhaar was used as the "alternate ID," i.e., applying for Aadhaar was made de facto mandatory.[201]
Myth #8 **Establishing the uniqueness**	➔ Tying people to a unique identity, confuses the idea of their "identity" with a mode of identification. Far from being a "single source of truth," a unique identity can create a single source of failure. It privileges one mode of authentication, which depends on a digital

[199] Anumeha Yadav. How efficient is Aadhaar? There's no way to know since the government won't tell. April 5, 2017. https://scroll.in/article/833060/how-efficient-is-aadhaar-theres-no-way-to-know-as-the-government-wont-tell
[200] Gurman Bathia. PAN, bank accounts and over 100 services, schemes you need to link your Aadhaar to. April 2, 2017. https://www.hindustantimes.com/interactives/aadhaar-mandatory-schemes-timeline/
[201] Rethink Aadhaar. Myths. https://rethinkaadhaar.in/myths

of individuals is a crucial need that only Big ID can fulfill	process, over all other ways that people choose to establish their identities. If there is a failure, the burden is on people to prove their identity. ➔ Mandating that people link their identity to a unique identifier dismisses the multiple ways that people could choose to identify themselves. As the Justice D.Y. Chandrachud, the Indian Supreme Court judge on the bench that heard the Aadhaar case noted in his dissent, the "multiplicity of identities," is a key right in a networked, democratic, and rights-respecting society, which "cannot be obliterated by an instrument intended to facilitate proof of identification." ➔ The idea that people need to always be uniquely visible to the state at all times places a burden on them to prove their identity to the state, and inverts the principle of the presumption of innocence. People have a right to anonymity, and to choose how, and when, they want to appear to the state. ➔ Using the unique ID as a "key" to integrate and link different databases also poses a serious surveillance threat. ➔ A unique identity means that people are constantly "visible" to the state, and to commercial actors. This enables the state to create dossiers of persons which can lead to the creation of a totalitarian state. This could be misused, and may put persons who are at-risk at additional danger. Many groups, like refugees, religious and caste minorities, journalists, dissidents, and activists, are already over-surveilled, and do not necessarily want to be more visible to the state. For vulnerable communities, such as persons who are HIV+,[202] the risk of records being created, and one part of their identity being linked to other parts, could have dangerous consequences.
Myth #9 Big ID is needed for	➔ Lack of ID is not the only, or most important, reason why people are not financially "included."

[202] Menaka Rao. Why Aadhaar is prompting HIV positive people to drop out of treatment programmes across India. The Wire. November 17, 2017. https://scroll.in/pulse/857656/across-india-hiv-positive-people-drop-out-of-treatment-programmes-as-centres-insist-on-aadhaar. This has caused disruptions in other contexts too - *see*
Channel News Asia. HIV-positive status of 14,200 people leaked online. January 28, 2019. https://www.channelnewsasia.com/singapore/hiv-positive-records-leaked-online-singapore-mikhy-brochez-909666

financial inclusion	➔ There are dangers in linking social protection measures to meet financial inclusion goals.[203] Many people who depend on social protection could be vulnerable, and linking them to the financial market without protection, and assuming a level of knowledge of how the financial sector works, could put them at risk. ➔ In India, Aadhaar linkage negatively disrupted the existing financial system through which welfare payments were being made. [204] ➔ The Big ID model of financial inclusion, particularly in areas where the banking system has limited reach, privileges a data-extractive model of financial inclusion. Private players are reluctant to take on the costs of financing new customers in rural areas, as they are seen as "low value" customers. Digital banking offsets this by eliminating operational and transactional costs *for financial institutions*, and enable them access to "rich digital information on their customers," data which they can use to design financial products, and enable greater access to credit. This approach "monetized information about people's personal liv[es] ahead of creating adequate digital and legal literacy and safeguards."[205] ➔ The focus on data-intensive models diverts resources and attention away from non-tech innovations to increase access to finance, like local governments, and self-help groups. ➔ A 2021 study found that financial inclusion infrastructures have proven to be a tool for revenue capture rather than distribution.[206]
Myth #10 Biometric verification is	➔ Biometrics are irreversible and intimate, and their collection and use poses a serious threat to the rights to privacy, integrity, equality, and non-discrimination.

[203] Sarina Kidd. The perils of linking social protection to financial inclusion. August 21, 2020. https://www.developmentpathways.co.uk/blog/the-perils-of-linking-social-protection-to-financial-inclusion/

[204] Digital Potholes Lead To Exclusion In MNREGA payments. Medianama. January 7, 2021. https://www.medianama.com/2021/01/223-digital-potholes-lead-to-exclusion-mnrega/; Why linking MGNREGA payments to Aadhaar is a mistake, Down to Earth. March 21, 2019. https://www.downtoearth.org.in/blog/agriculture/why-linking-mgnrega-payments-to-aadhaar-is-a-mistake-63680;

[205] Reetika Khera. The Different Ways in Which Aadhaar Infringes on Privacy. July 19, 2017. The Wire. https://thewire.in/government/privacy-aadhaar-supreme-court

[206] Isabelle Guérin, Nithya Joseph and G. Venkatasubramanian. How India's Financial Inclusion Infrastructure Failed During the Pandemic. June 23, 2021. https://thewire.in/rights/how-indias-financial-inclusion-infrastructure-failed-during-the-pandemic

necessary, safe, and useful	➔ Biometrics create a real security challenge to the digital ID system. Once they are leaked, they can no longer be used due to risk of impersonation. ➔ Systems based on biometrics are easy to fool, through more and more sophisticated measures. ➔ Some people cannot give their biometrics. e.g. people may be unable to do so as they are blind or do not have eyes or fingerprints. ➔ The usage of biometrics — even for one-to-one matching — has to be justified according to the purpose on a case-by-case basis and must be completely safe, inclusive, not liable to error, and only used if there are no other means for authentication. ➔ Biometrics are not the only way to authenticate identities. Mandating biometric verification for all identification is not necessary or proportionate.
Myth #11 **Big ID systems ensure that your personal information is safe**	➔ Aadhaar enabled new forms of fraud, which were difficult to track, understand, and remedy. These have been extensively documented.[207] For instance, an Aadhaar breach was named the world's biggest data breach of 2018.[208] ➔ Sophisticated software hacks into computers linking to the central database permitted false information to be fed into the system.[209] In some cases, the enroller's fingerprints were duplicated and used to create new IDs. ➔ Aadhaar numbers were "seeded,"[210] or linked/copied into different private and government databases from where they could be copied.[211] Access to a person's Aadhaar number enabled new kinds of identity fraud, and permitted malicious actors to access personal information, like bank accounts.

[207] Anmol Somanchi. Aadhaar Fraud is Not Only Real, But is Worth More Closely Examining. May 3, 2018. https://thewire.in/economy/aadhaar-fraud-uidai

[208] Martin Hron. Top 10 Biggest Data Breaches in 2018. December 20, 2018. https://blog.avast.com/biggest-data-breaches

[209] Rachna Khaira and Aman Sethi, and Gopal Sathe. UIDAI's Aadhaar Software Hacked, ID Database Compromised, Experts Confirm. September 11, 2018. huffpost.com/archive/in/entry/uidai-s-aadhaar-software-hacked-id-database-compromised-experts-confirm_a_23522472

[210] Unique Identification Authority of India. Glossary. https://uidai.gov.in/contact-support/have-any-question/glossary.html

[211] Tech Crunch. Indian state government leaks thousands of Aadhaar numbers. 2019. https://techcrunch.com/2019/01/31/aadhaar-data-leak/

	➔ The Aadhaar Act doesn't impose any obligations to give notice to an individual in case of a breach of his or her information, an established principle of data privacy laws. ➔ The Unique Identification Authority of India (UIDAI) failed to take responsibility for data breaches, or to give people guidance on how to protect their data. For years, it didn't even have a Chief Information Security Officer.[212] The UIDAI also went after reporters reporting on software vulnerabilities[213] including filing criminal charges against a journalist who reported on an illegal online marketplace for Aadhaar numbers.[214]
Myth #12 **Big ID is a reliable tool for national security**	➔ The Aadhaar database is riddled with fakes. At its inception, Aadhaar enrollers were private entities who were given enrollment targets, to incentivize how many persons they enrolled into the Aadhaar system.[215] This incentive structure resulted in mass enrollments, with no checks for the accuracy of the background document.[216] ➔ Aadhaar's widespread use as an identity card is insecure. Often, a printout of the proof of Aadhaar registration is used as a form of photo ID, despite it not being designed to be used in this manner. The printout of the Aadhaar registration, which contains the Aadhaar number is a document that lacks any traditional security features present in other photo-IDs such as a microchip, hologram, or an official seal.

[212] Money Life. Aadhaar Truth: UIDAI Never Appointed a Chief Information Security Officer, Reveals RTI, February 5, 2019. moneylife.in/article/aadhaar-truth-uidai-never-appointed-a-chief-information-security-officer-reveals-rti/56267.html
[213] Anumeha Yadav. Security of Aadhaar's data is under question, but pointing to the gaps could lead to a police case. Scroll.in. March 02, 2017. https://scroll.in/article/830580/security-of-aadhaars-data-is-under-question-but-pointing-to-the-gaps-could-lead-to-a-police-case
[214] NDTV. UIDAI Files Case In Aadhaar-Data-For-Rs 500 Report, Journalist Named. January 8, 2018. https://www.ndtv.com/india-news/uidai-files-case-for-aadhaar-data-for-rs-500-report-journalist-named-1796899
[215] Moneylife. Dr Goyal exposes vulnerabilities in Aadhaar architecture and ecosystem before the Supreme Court. February 21, 2018. https://www.moneylife.in/article/dr-goyal-exposes-vulnerabilities-in-aadhaar-architecture-and-ecosystem-before-the-supreme-court-part1/53161.html
[216] Scroll.in. Everyone in this Uttarakhand village has the same birth date on their Aadhaar cards. October 28, 2017. https://scroll.in/latest/855731/everyone-in-this-uttarakhand-village-has-the-same-birth-date-on-their-aadhaar-cards

IV. CONCLUSION

Over the last decade, institutional support for digital identification programs has grown significantly. The World Bank, for example, has been an enthusiastic supporter of digital identity systems like Aadhaar. While the Aadhaar project predates groups like ID4D, it played an important role in growing similar projects. This paper draws on a decade of reporting, research, and commentary on Aadhaar in India to highlight five main points:

➔ First, despite its stated purpose, Aadhaar was not intended or designed to work "for people," but instead to serve commercial interests by developing an 'infrastructure' for digital services in India. This had two consequences: it was rolled out without solid proof of *why* it was required. There was never a satisfactory answer to #WhyID was required: no studies backed up the myth that identity fraud was the biggest issue that welfare systems faced, and no studies showed that Aadhaar was in fact enabling access — it only showed that people had to jump through hoops to gain access to what they were already entitled to — or that it was good for security.

This has consequences for the discourse on digital identities. For one, the urgent and continued need to demand evidence for why a particular form of digital identity is required. Second, to ensure that the focus on "inclusion" should not focus on ensuring more people are enrolled but that people are not disadvantaged because of the digital identity, and that they continue to have a real and meaningful choice of how they access public goods and services and exercise their right to freedom of association.

➔ Second, despite ample evidence of the harms being caused by Aadhaar, little was done to remedy, halt, or prevent these harms. As we have pointed out before, the scalability of digital products means that their harms are scalable[217] — and the mechanisms to ensure these harms are addressed have to be equally scalable. There is an urgent need to address flaws, build in systems that track failures, and remedy them. Today, the millions whose lives were "disrupted" by Aadhaar have been left by the wayside, while the industry developing software products thrives.

➔ Third, there is a lot of discussion in the institutional literature on the need for "sufficient" legal, regulatory, and institutional safeguards when rolling out digital identities. The Aadhaar project did all it could, each step of the way, to challenge, circumvent, or avoid being bound by those safeguards. The "black box" was in its

[217] #WhyID. An open letter to the leaders of international development banks, the United Nations, international aid organisations, funding agencies, and national governments. https://www.accessnow.org/whyid/

design. This is evident in how it was rolled out without a law and how the eventual law was slipped in by way of a money bill.

➔ Fourth, there is no justification for the continued push to expand biometric systems across the developing world. Aadhaar is the world's largest biometric database. However, there is little evidence that biometric authentication works, is reliable, or that it meets the standards of the test of necessity and proportionality test.

➔ Fifth, despite assurances, unique centralized systems can not be rolled out without serious harms to privacy, not all of which are knowable at the time. Afghanistan is a sobering illustration of this. It bears repeating that the Indian government rolled out the Aadhaar project without a data protection law, and today continues to advocate for data governance models that seek to make data a "public good," which the state can exercise its powers of eminent domain over.[218]

The Aadhaar story is a cautionary tale for how a Big ID program can be disastrous for a country, its welfare systems, and its most vulnerable. It also offers some insight into what should be avoided. These systems can have long-term impacts on people, and before rolling them out, people, governments, and companies should ask #WhyID: why is it needed, how is it being considered and rolled out, who is being involved in each step of the process, and are there sufficient legal, regulatory and institutional safeguards to protect privacy, prevent exclusions, and safeguard human rights?[219] Technology can not be used to replace or obscure political choices, and any digital identity system must center people, not commercial interests or data-rich models. Building on the recommendations we have previously made,[220] we call on international organizations, states, and private organizations to demand #WhyID is necessary, and ensure digital ID projects fully respect human rights.

---

[218] Eminent Domain and the expropriation of data. https://hasgeek.com/PrivacyMode/non-personal-data/sub/eminent-domain-and-expropriation-of-data-indias-da-RoYFHRf57MEGAEU9Kks2hy

[219] #WhyID. An open letter to the leaders of international development banks, the United Nations, international aid organizations, funding agencies, and national governments. https://www.accessnow.org/whyid/

[220] Access Now. National Digital Identity Programmes. What's Next? May 2018. https://www.accessnow.org/cms/assets/uploads/2019/11/Digital-Identity-Paper-Nov-2019.pdf