Journal of Cultural Economy

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rjce20

The curious case of tweeting an Aadhaar number: trust/mistrust in security practices of public data infrastructures

Ranjit Singh

To cite this article: Ranjit Singh (2023): The curious case of tweeting an Aadhaar number: trust/mistrust in security practices of public data infrastructures, Journal of Cultural Economy, DOI: 10.1080/17530350.2023.2229360

To link to this article: https://doi.org/10.1080/17530350.2023.2229360

Published online: 25 Aug 2023.

JOURNAL OF CULTURAL ECONOMY
https://doi.org/10.1080/17530350.2023.2229360

Routledge
Taylor & Francis Group

The curious case of tweeting an Aadhaar number: trust/mistrust in security practices of public data infrastructures

Ranjit Singh

AI on the Ground, Data & Society Research Institute, New York, USA

ABSTRACT

This paper explores data security practices of Aadhaar, India's biometrics-based national identification number, and the co-constitution of trust and mistrust that underlies its operation as a public data infrastructure. Based on 18-months of multi-sited ethnographic research, I document tensions around whether Aadhaar numbers were designed to be disclosed publicly or kept confidential. I further map identification practices around how residents share their Aadhaar numbers with other government and private organizations to access services. These practices to promote sharing of Aadhaar numbers broke down with growing anxieties over their public disclosure on government websites, lack of audits, and emerging forms of Aadhaar-based frauds. In response to this rising mistrust, an ex-member of Aadhaar's design team publicly disclosed his number in a tweet that went viral. The paper uses this tweet as a point of departure to: (1) provide an account of infrastructural concerns (grounded in design choices and events) that transformed Aadhaar from a public to a confidential number; and (2) illustrate that this transformation reflects how trust and mistrust co-constitute Aadhaar's data security practices. I conclude by illustrating how these infrastructural concerns imbricate to produce a spectrum of possibilities where identity numbers are simultaneously public and confidential, trusted and mistrusted.

ARTICLE HISTORY
Received 21 September 2022
Accepted 14 June 2023

KEYWORDS
Trust; mistrust; public data infrastructures; identification; digital ID

Introduction: tweeting an identity number

On 28 July 2018, Ram Sewak Sharma, Chairperson of the Telecom Regulatory Authority of India (TRAI) at the time, and an ex-member of Aadhaar's design team, tweeted: 'My Aadhaar number is: […]. Now I give you this challenge to you: Show me one concrete example where you can do any harm to me' (Scroll Staff 2018)! Aadhaar is a unique 12-digit number assigned to every enrolled Indian resident based on their biometric (ten fingerprints, two irises, and facial photograph) and demographic (name, age, gender, and residential address) data (UIDAI 2010). The Unique Identification Authority of India (UIDAI) began Aadhaar enrollment in 2010 with the ambitious goal of registering the entire Indian population. With more than 1.36 billion enrollments, Aadhaar is the largest biometric database in the world.[1] Aadhaar numbers are standardized legal identities for every resident – purportedly including those who previously lacked identity documents – and can be used in transacting with any government or private organization in India. A resident becomes a citizen when they use Aadhaar to secure other government services, and a customer when they use it to interact with private agencies. An Aadhaar enrollee, thus, is simultaneously a resident, a citizen and a customer depending on where they use Aadhaar and for what purpose.

CONTACT Ranjit Singh ranjit@datasociety.net AI on the Ground, Data & Society Research Institute, New York, USA

The standardization of identity through Aadhaar involves three key processes: (1) *Enrollment*: producing a unique Aadhaar number after collecting and deduplicating a resident's biometric and demographic data. (2) *Seeding*: adding Aadhaar numbers to a resident's data records in other government and private databases. (3) *Authentication*: verifying that an Aadhaar number belongs to a resident when they access and claim a service. These processes together operationalize Aadhaar as a public data infrastructure increasingly central to the distribution of uniquely identified know-your-resident (KYR) information (name, age, gender, and address) of Indian residents to an ecosystem of public and private organizations.

The organization of these key processes raised several questions throughout the eighteen months of my ethnographic fieldwork: Can Aadhaar numbers be disclosed publicly, or should these numbers be kept confidential? Which organizations may be trusted to access it, and which may not? I conducted fieldwork in three rounds between June 2015 and March 2018 and it spanned across multiple sites (Marcus 1995) including locations such as startup workspaces in Bengaluru; and offices of the UIDAI, frontline Aadhaar-related service outlets, the Supreme Court of India, and activist organizations in Delhi. These questions were not only matters of *framing* identification as a matter of establishing uniqueness, but also *taming* the multiple meanings of uniqueness in my broader investigation of the co-constitutive relationship between the public/confidential nature of identity numbers and trust/mistrust in data security practices of public data infrastructures such as Aadhaar (Silvast and Virtanen 2019). Sharma's tweet, a few months after I finished the last round of my fieldwork, crystallized my investigation into a viral tweet. The paper uses this tweet as a point of departure to: (1) provide an account of infrastructural concerns (grounded in design choices and events) that transformed Aadhaar from a public to confidential number; and (2) illustrate that this transformation reflects how trust and mistrust co-constitute Aadhaar's data security practices.

Sharma's tweet was a provocation on whether public disclosure of Aadhaar numbers makes Indian residents more vulnerable in a data-driven world. More than two years later, he reflected on his tweet:

> Nobody could demonstrate any harm, either then or in the months that have followed since [the tweet. …] Of course, when the hackers tried to show that they could cause me some harm, I did take a few precautionary steps. For example, I changed my passwords and hardened them on my bank accounts, social media accounts and email accounts. Yet, when hackers are out 24×7 to cause harm, *one feels vulnerable*. One does not know the source of the attack. (Sharma 2020, 121–23, emphasis added)

Sharma, a design team member, who fully understood and trusted Aadhaar's data security practices, felt justifiably anxious and vulnerable after tweeting his number. His anxiety was borne out of a consequential lack of agency in controlling what others can do with his number after its public disclosure. Such anxiety cannot solely be addressed by investing in data infrastructure literacy (Gray, Gerlitz, and Bounegru 2018); it shows how security practices of public data infrastructure can be trusted and mistrusted at the same time.

Aadhaar is simultaneously a data infrastructure for identification and an identity number. Thus, critically engaging with its nature requires interweaving the notion of 'public' with three intertwined, yet distinct conceptual threads. In the first thread, I use public to imply ownership by the state; I analyze Aadhaar as a public infrastructure owned and operated by the government of India. The second thread centers on public(s) as manifestations of 'amorphous and unarticulated' collectives of people who organize themselves in the face of problems and/or issues that affect them to express their concerns (Dewey 1927, 131). In an analytic sense, this notion of public(s) works as a formal device to engage with the cultural discourse of problems around which people get organized (Warner 2005). Perceiving these problems, Dewey (1927) argues, often requires specialized expertise (such as understanding the flow of citizen data in organization of Aadhaar-based services), and by acting upon them the public manifests its capacity to hold the government accountable (for example, in the organization of identification as a service). Finally, for the third thread, I use public to explore the principle of openness in disclosure of Aadhaar as an identity number and contrast it

with practices of keeping it confidential. Since engagement with the first and second threads are common and well-understood in sociotechnical analysis of data infrastructures, I only provide more context for the third thread.

Identity numbers can be publicly disclosed and thus, can be public like a person's name when the number itself is not sufficient to authorize access to any service. For example, a credit card number alone is not enough, additional pieces of information, such as the Card Verification Value (CVV) code, expiry date, and billing address, are required to authorize a financial transaction. Yet, credit card numbers are not publicly shared like a person's name. They are considered confidential, a secret shared only in specific situations with expectations and shared agreements over protecting data. The push and pull between openness and confidentiality of identity numbers raises *a fundamental paradox* in trusting data security practices of public data infrastructures for identification. On one hand, from an organizational design perspective, publicly disclosing citizens' identity numbers promotes trust and recognition in a state's formal economy. Consider, for example, the disclosure of bank account number printed on any check. The bank uses this number to recognize the account holder and verify their signature before debiting their account. Without this disclosure, a check cannot be trusted as a financial instrument. On the other hand, from a citizen's perspective, keeping an identity number private or confidential engenders mistrust in contending with the persistent possibility of its unwelcome revelation. Yet, the agency in choosing when to reveal this number fosters a sense of control and trust in data security practices. In either case, whether identity numbers are confidential or public, the anxieties over unwelcome revelation and future ramifications of public disclosure are responses to the risk of identity theft and/or surveillance.

In the following sections, I begin with reviewing two ongoing debates around datafication and technology that this paper draws on and contributes to: first is the polarization around identification technologies as tools for recognition and/or surveillance, and second is the debates over multiple dualities in articulating the role of trust in organizing sociotechnical practices. These debates form the canvas on which I go on to trace the technical choices made by Aadhaar's design team and the UIDAI, and subsequent events that shaped perceptions of different public(s) around the appropriation of Aadhaar as a public data infrastructure and a public identity number. I show how each choice and event added additional layers of meaning to how ongoing ways of trusting and mistrusting Aadhaar's data security came to mutually shape its role in identification practices of digital India. I conclude by exploring these layers together and illustrating how infrastructural factors imbricate to produce a spectrum of possibilities where identity numbers can be public and confidential, trusted and mistrusted at the same time.

Debates over trusting identity numbers

In a datafied state, citizen data mediates state-citizen relations. *Citizens become data subjects* – people 'who are not separate from but submit to and are active in the various ways that data is made' (Ruppert, Isin, and Bigo 2017, 5). On the state's side, identifying citizens becomes a problem of locating their data record (Gelb, Mukherjee, and Navis 2020). Knowing them turns into a matter of managing and interpreting their data (Cheney-Lippold 2017; Nair 2021). Identity numbers are positioned to resolve this problem of locating, managing, and interpreting citizen data, or to put it simply, the problem of identification (USAID 2020). On the citizen's side, access to the state becomes grounded in managing representation through data in public data infrastructures (Singh and Jackson 2021). Bureaucracies turn into centralized data dashboards (Singh 2019). Identity numbers are positioned as a condition for claiming citizenship (Breckenridge and Szreter. 2012). In this section, I review the ongoing debates over identification and identity numbers under two themes: first, the purpose of identification and second, the locus of trust in identity numbers as a technical solution that makes identification possible. In short, while the first set of debates are over the *why* of identification, the second is about *how*.

Starting with *why*, the debate over purpose of identification has become increasingly polarized between discursive logics of recognition and surveillance (Weitzberg et al. 2021). On the one hand, the proponents of identification argue that recognition is a precondition for claiming citizenship and engaging with state services (Breckenridge and Szreter. 2012). Such arguments have been crucial in: (1) the inclusion of providing 'legal identity to all' by 2030 in the United Nations Sustainable Development Goals (UNSDG) (Sperfeldt 2022); (2) organization of the World Bank's Identification for Development (ID4D) Initiative (World Bank Group 2016); and (3) the turn to humanitarian cash transfer in international aid programs (High Level Panel on Humanitarian Cash Transfers 2015). On the other hand, arguments against identification center on its inextricable relationship with the pursuit of legibility and surveillance (Lyon 2009; Monahan, Phillips, and Wood 2010; Scott 1998). Identification is positioned as a precondition for datafication, which in turn, is critiqued as a form of: (1) technosolutionism (Greene 2021); (2) technochauvinism (Broussard 2018); and (3) technocolonialism (Madianou 2019). Such critiques have been essential in calling attention to the need for a broader framework of human rights and dignity, encompassing privacy and non-discrimination, in the design, implementation, and appropriation of identification systems (Latonero 2018). Thus, 'rather than two sides of a binary debate, surveillance and recognition are mutually compatible developments that are increasingly collapsed' (Weitzberg et al. 2021, 2). The occasions of their collapse provide a generative space for thinking through how trust in identity numbers is secured, maintained, broken, and challenged.

Moving onto *how*, when identification is approached as a simultaneous condition of possibility for recognition and surveillance, trust in identity numbers becomes a matter of trusting data systems that make identification possible. In a computational sense, identity numbers are proxies that help locate a person's data records in data systems; they serve the purpose of a primary key. Focusing on data systems brought up the first duality in my exploration: within computational sciences, *trust is broadly placed either in technologies* (artifacts or systems) *or people* (individuals or institutions) (Shahar et al. 2021; Thiebes, Lins, and Sunyaev 2021). When placed in technology, trust is considered an outcome of its seamless operation; it is the result of technologies performing reliably (Mcknight et al. 2011), predictably (Thatcher et al. 2011), and achieving intended function and purpose (Lee and See 2004). When placed in people, it is treated as an attribute of competence/virtue/morality (Mayer, Davis, and David Schoorman 1995; McKnight, Choudhury, and Kacmar 2002). Within this duality, trust in identity numbers becomes either a matter of technical design or moral persuasion. Either the underlying data system is designed to protect personal data, or the misuse of identity numbers is prevented through individual volition and/or institutional checks and balances.

Since identity numbers play an integral role in interfacing with the state, their technical design cannot be separated from institutional checks and balances. In an administrative sense, designing public data infrastructures is policymaking by other means (Herd and Moynihan 2019). Combining technical design with institution building steered my attention towards the relationship between individuals and institutions. This sociological turn in my exploration of trust brought up the second duality between personal trust and system trust (Luhmann 2017): *Trust is either a marker of an individual's agency* in relationships such as strategy, resource, risk-taking, and game *or an emergent feature of social structures* such as family, community, organizations, industry, and political system (Möllering 2001; Sztompka 2000; Watson 2009). Engaging with this duality, trust emerges either in use or through legitimacy. Either individuals trust identity numbers when they have a sense of control over their use or existing legitimacy of institutions involved in infrastructuring identity numbers acts as a mirror for their trustworthiness.

In either case, trusting identity numbers as proxies for people during transactions inevitably implies a degree of dependency over what others can/might do with such disclosure. This dependency produces diverse risks such as identity theft and surveillance. Trust serves as an orienting principle for responses to such risks through 'a *redistribution of control*. In trusting, we both relinquish control over our environment and attempt to extend control over others' (Carey 2017, 7

emphasis in original). While trust is a way to manage and control the freedom of others, mistrust – 'a general sense of the unreliability of a person or a thing' (Carey 2017, 8) – is an equally powerful way to engage with the freedom and autonomy of others. Within this duality, *mistrust does not undo the work of trust* (for example, trust builds relationships, mistrust breaks them apart), *rather they co-constitute each other*: 'Each implies its shadow: where people assume that others can be known and so trusted, they are also aware that sometimes this does not hold; and where they assume that others are largely unknowable, they are also aware that some are less unknowable than others' (Carey 2017, 10). Seen through the lens of this duality, mistrust in identity numbers produces its own set of complementary security practices that, in turn, can enhance their reliability and trustworthiness as proxies for citizens.

Furthermore, mistrust is crucial in organizing bureaucratic processes of identification, which must contend with the limits of inductive reasoning in establishing citizen identity through evidence. As Partha Chatterjee puts it in his poignant account of the adjudicating a case of impersonation in early twentieth century Bengal: 'whereas identity may be disproved by evidence, it can never be proved beyond doubt' (Chatterjee 2002, 362). Every governmental effort to certify and authenticate citizen identity must set up a trail of evidence to achieve correspondence between citizens and their government records. Fixing identity requires work on two fronts: *First*, providing citizens with a means to claim their identity, for example, issuing an identity number/document (such as Aadhaar) and insisting that citizens produce it whenever required. *Second*, keeping government records of issuing such an identity number/document against which citizens' claims to identity could be adjudicated. Data on an identity document is compared against data on government records. A match results in authentication of identity, while a mismatch is bureaucratically considered false representation of identity. However, a match does not necessarily indicate correspondence between a citizen's identity and their government record; 'people will often try to fool them by claiming to be someone they are not, and the authorities have to be vigilant' (Chatterjee 2002, 364). Managing citizen data is replete with challenges of dealing with forgery and other forms of corruption in the way the government manages citizen records and how citizens manage their corresponding identity documents. 'Modern governmental regimes must presume every individual to be an imposter until he or she is able to prove the contrary' (Chatterjee 2002, 363). *Since proving citizen identity beyond doubt remains administratively unachievable for any government, the foundational assumption for designing any public data infrastructure for identification is mistrust of citizens*. Yet, the appropriation of such infrastructures requires that citizens trust their identity numbers and feel that they are adequately secured by the state against the risk of identity theft and/or surveillance. Identity numbers, thus, are markers of the level of trust between the state and citizens and the ongoing work of sustaining them emerges through an ever-unfolding recursion of trust and mistrust in state-citizen relations.

My efforts in this section to theoretically map trust in identity numbers foreshadows the analytic themes that I found useful in understanding controversies and negotiations over whether Aadhaar numbers are public or confidential. My field stories in the next two sections broadly focus on the interplay between trust and mistrust in data security practices and explore elements of this vocabulary of debates and dualities to unpack design choices and events that shaped the use of Aadhaar as a public data infrastructure.

Trust in data security practices of Aadhaar

Trust in biometrics

In August 2015, a couple of months into the first round of my fieldwork, I read a news story that reported a mundane, yet new projected use of Aadhaar numbers. 'Students may soon end up using Aadhaar numbers instead of their roll numbers for examinations' (Kulkarni 2015). The story indicated the ongoing function creep of Aadhaar. At the time, I was in Bengaluru conducting interviews

with the initial members of Aadhaar's design team. I met them in startups they had launched after leaving UIDAI. They talked about working on Aadhaar as one of the most exciting times of their lives and were quick to compare Aadhaar with historically antecedent practices of identifying Indian residents and identification practices in other countries. For example, they often talked about a lack of robust civil registration system issuing Birth Certificates in India (Gopinath 2012; Sadiq 2009) and compared Aadhaar numbers with Social Security Numbers (SSNs).

While this comparison between Aadhaar and SSN is contestable (Hickok 2015), it raised a different concern for me after reading the news story: Should Aadhaar numbers be considered public or confidential? SSN is considered confidential in the United States because it serves a dual purpose as identifier and authenticator for US residents. Most organizations treat it 'as a secret piece of information, available only to the consumer and themselves, and give access to information or benefits only when the consumer is able to supply and confirm his or her SSN' (FTC 2008). Taking the comparison with SSN as a crucial thread for our conversation, I asked Kairav, a member of the team, about whether residents would be similarly asked to confirm the digits of their Aadhaar number as a security measure during authentication.

> SSN is a 70-year-old technology. The reason for using the last four digits of the SSN is that there is a logic embedded in the number. So, if I have access to your SSN, I can actually figure out a certain set of things about you, for example, the place where you were born and so on [(see, for example, Acquisti and Gross 2009)]. But Aadhaar is a random 12-digit number […]. Since there is no hidden logic to the number, I cannot actually do anything with it, even if I know your Aadhaar number. The four-digit security feature is unnecessary. You can share your number with anyone, […] because your identity is connected to you, not the number. (Fieldnotes, 4 October 2015)

Kairav's response that Aadhaar numbers are random numbers with 'no built-in intelligence or profiling information' (UIDAI 2014, 33) aligns with Sharma's tweet to publicly disclose his Aadhaar number. Without any hidden information, publicly sharing Aadhaar made no difference because it is only one part of a two-factor authentication process involving biometrics or a One-Time-Password (OTP) sent to a registered mobile number.

Crucially, Kairav also argued that there is no difference between a person and their identity. The design team uses this argument to justify not only their reliance on biometrics for unique identification, but also their claim that the Aadhaar number is simply a digital record that allows residents to claim who they are, rather than what they have or know (UIDAI 2014). This approach further justified the decision of not investing in a smart card:

> *You are your identity.* A card cannot be your identity. [If] you lose your card, do you lose your identity? [… A card] is only a manifestation of my identity. I could have manifested it in a mobile. […] We said this is a time to leapfrog and say, 'Don't bother. […] Just make it a completely digital identity. […] You can verify your identity and if you want to remember [it], I will give you something that you can print'. (Kairav, Personal Communication, 24 September 2015, emphasis added)

Biometrics was articulated as a resource to provide identity to people and an assurance of data security; no one can take away who they are (or their biometric data) from a person. While a card can be forged, successful Aadhaar authentication through biometrics requires the resident to necessarily be a part of its process. This requirement made forgery difficult, if not impossible. Despite stories of cloning fingerprints (Sethi 2017) and arguments on unreliability of biometrics in uniquely identifying a person (Jonnalagadda 2017), UIDAI has consistently promoted the relative strength of data security in biometrics-based transactions by framing the biometric details of people as indicators of 'who they are' (UIDAI 2011).

Evocative of the first duality between trust in technology or people, Kairav framed Aadhaar as a public number by placing trust in biometrics as an authentication technology without concern for what others might be able to do with the number's disclosure. The number by itself neither provides any information about its holder nor can it be used to conduct any transaction without two-factor authentication. Aadhaar differed significantly from the SSN. It works more like a public key that can

be broadcast and disclosed at no purported risk. However, as I show in the next subsection, there were caveats to the public nature of Aadhaar as an identity number.

Trust in the authentication ecosystem

As I dug deeper into the public nature of Aadhaar numbers with other design team members, Dakshin brought in considerations of context in Aadhaar's use:

> Well, it can be public or confidential depending upon how you are using it. So, for example, if you are making use of the Aadhaar letter as proof of identity, then the number is public. While when the authentication is routed through your fingerprints, OTP, or your demographic details, then the number is private. Of course, you are working on the number in the background, but you are not explicitly sharing it.
>
> So, in the case you mentioned, there are so many instances around India where somebody else is giving the exam on the behalf of the student. So, a supervisor can simply authenticate a student's identity by using a biometric reader and comparing it with their Aadhaar number. If it matches, then you know that the student is the person who is supposed to be taking the exam. (Fieldnotes, 29 September 2015)

Dakshin's invocation of fraud and context of use are both equally important in understanding the function creep of Aadhaar and the tensions over its public or confidential nature. Every government service relies on some form of identification to ascertain eligibility of a citizen to access that service. This process of identification and determining eligibility is inundated by mistrust in state-citizen relations (Turkkan 2023). This mistrust engenders challenges for both citizens in securing identity documents and the state in detecting fraud and forgery in identifying them through documents (Sriraman 2018; UIDAI 2010). Aadhaar was promoted as a solution to this problem.

Aadhaar's design team imagined identification as a government service in and of itself, rather than a mechanism to facilitate last mile delivery of other government services (Nilekani and Shah 2015). As Dakshin further elaborated: '*An Aadhaar number did not have a particular bureaucratic purpose per se, it was simply intended to uniquely identify a person.* […] The rest of the uses of Aadhaar is an extension of the ecosystem that it supports by uniquely identifying Indian residents' (Fieldnotes, 29 September 2015, emphasis added). This design requires Aadhaar numbers to be public such that they can be seeded and shared across diverse government and private databases, but it also raises the potential of surveillance and convergence of resident data. The ability to identify a person across contexts traverses the spectrum of surveillance and recognition.

The design team conceived of the Aadhaar database as a minimalist archive for citizen data to retain privacy (Cohen 2019). It implemented 'one way' connections between the Aadhaar database and other public and private databases to walk this fine line (UIDAI 2014, 31). Aadhaar was imagined as a root identity, which is *permanent* and *unique* to an individual resident. Other domain specific identities such as driving license, income tax number, and IDs for claiming welfare were imagined as identities derived from Aadhaar and connected with it. This ensured that they not only served their specific bureaucratic purposes, but they also remained uniquely associated with an Aadhaar number. One-way linkage implies that these derived identities are connected with Aadhaar, but Aadhaar is not connected to them. 'Aadhaar system has no knowledge of any applications, transactions, or domain specific identities within its database. This is designed so that information about the resident (transaction history of a resident) is not centralized into one system and is kept in distributed fashion' (UIDAI 2014, 31–32). This design choice of not storing complete transaction histories was articulated as creating a zero-knowledge system. As Pramod Varma, the chief data architect of Aadhaar, further elaborated, 'We are a zero-knowledge system. Whenever you use [your Aadhaar identity], withdraw money, deposit, travel, buy pizza, whatever you want to do, [our] system has no understanding of what transaction you did. All it knows is that you claimed your identity, not where, and not for what purposes' (TEDxBangalore 2016).

A zero-knowledge system is imagined as an intervention to restrict the possibility of its use for data convergence and surveillance and afford the conditions of using it for recognition. In the case

of Aadhaar, this is evident in its organizational ecosystem for authentication (see Figure 1). There are five types of user authentications possible through Aadhaar (UIDAI 2011), leveraging combinations of demographic and biometric information and OTPs sent to mobile numbers. On the backend, authentication involves 1:1 comparison between other data provided by the resident and their Aadhaar record (UIDAI 2014). The UIDAI issues two kinds of responses: First is a Yes/No response to confirm whether the data provided matches with the data on record for any authentication request. Second is an electronic know-your-resident (e-KYR) response, which not only authenticates a resident's identity, but also includes demographic details on the resident as stored in the Aadhaar database.

As Figure 1 illustrates, Authentication Service Agencies (ASAs) and Authentication User Agencies (AUAs) are key stakeholders in the authentication ecosystem. While ASAs interact with the Aadhaar database, AUAs interact with residents. Together they are the intermediaries between the Aadhaar database and residents. Simultaneously, these organizations also connect the UIDAI to other public and private organizations seeding Aadhaar numbers into their respective databases for delivering their own services. Thus, specifying how Aadhaar data is transmitted by and stored at ASAs and AUAs is crucial to maintaining Aadhaar as a zero-knowledge system. The Aadhaar Act of 2016 performs this crucial function by regulating data management practices of each stakeholder in the authentication ecosystem.

This design ensures that no participating organization, including UIDAI, has a panoptic view of a resident's use of their Aadhaar number. Since ASAs and AUAs serve authentication requests coming from diverse organizations, the authentication trail of a resident remains distributed across these agencies. A quick look at the Aadhaar dashboard (UIDAI n.d.) reveals that as of May 2023, there are 31 ASAs, 251 AUAs, and 224 KUAs in the authentication ecosystem. This distributed storage ensures that every participating organization only has access to data necessary for processing and transmitting authentication requests and responses at their end. Citizen data remains in distributed silos. A complete view and cross-domain analysis of a resident's Aadhaar-based transactions is difficult, if not impossible, to achieve, especially without their consent, additional large-scale investment in infrastructure for data collation, and supplemental procedures established by law (UIDAI 2014). These design features, however, have not prevented individual states, for example, Andhra Pradesh, from investing in their own infrastructure to collate data about residents

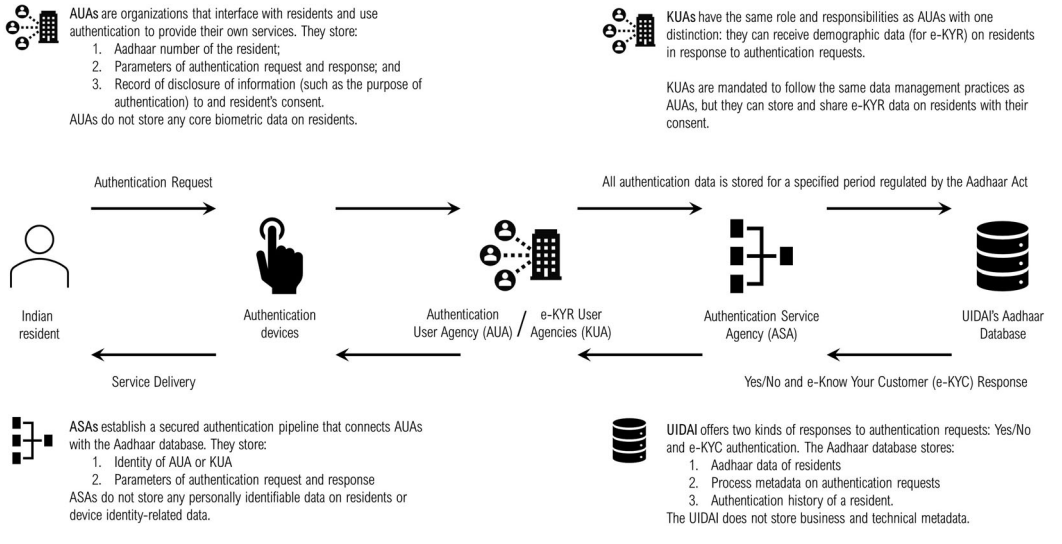

Figure 1. Organizations in the Aadhaar Authentication Ecosystem and their data management practices regulated by the Aadhaar Act.

of particular districts raising broader surveillance concerns around creation of 'public, searchable, digital profiles of minorities' (Sethi 2018). Trust in Aadhaar becomes increasingly intertwined with trust in state administrations.

While the UIDAI cannot control how state administrations collate databases of their respective services, it controls and maintains the Aadhaar authentication ecosystem, which is designed to prevent collation of personally identifiable data of Indian residents and promote data security in authentication practices. This ecosystem is an example of designing for trust through structural interventions. Irrespective of whether a resident understands the circulation of their data, it gets distributed across diverse datasets maintained by different public and private organizations. If privacy is a person's agency in controlling the social situations that emerge from circulation of their data (Marwick and boyd 2014), then *this ecosystem does little to support the agency of an Aadhaar number holder*. While it may prevent the possibility of turning Aadhaar itself into a digital panopticon, the lack of agency in controlling the distribution of one's own Aadhaar data and the potential of its collation by state administrations has created conditions for everyday conversations and public(s) around the issues of changes in 'the architecture of surveillance, moving it from centralized to distributed' in India (Masiero and Shakthi 2020; see also, Shakthi 2020).

Furthermore, this design can fail without compliance in practice. An audit of the authentication ecosystem performed by the Comptroller and Auditor General of India (CAG) in 2021 noted that the 'UIDAI was neither able to derive required assurance that the entities involved in the authentication ecosystem had maintained their information systems which were compliant with the prescribed standards nor did it ensure compliance of Information Systems Audit by the appointed entities' (CAG 2021, 49). Maintenance for trust requires continuous vigilance and accountability. This work is never ending; in practice, it is much harder than designing for trust.

To conclude this section, the concern around publicly sharing Aadhaar numbers was centered on the possibility of impersonation in the first subsection. Thus, the focus was on mediating an individual's relationship with their identity number through authentication technologies such as biometrics. In the second subsection, the possibility of data convergence and surveillance became a matter a concern, and the attention turned to structural arrangements that prevent any organization from knowing more than it needs to about a population that it provides authentication services to. Designing for trust at scale moves beyond technologies to institutional arrangements to maintain the public nature of Aadhaar numbers. However, these interventions do not account for how residents made sense of Aadhaar numbers in their everyday life and how they were used in different public or private contexts. They serve more as the preconditions for the push and pull over the public/confidential nature of and trust/mistrust in Aadhaar numbers. For example, although the design team imagined Aadhaar numbers to be public, their sharing, circulation or publication was regulated with the passage of the Aadhaar Act in 2016: 'no entity […] shall make public any database or record containing the Aadhaar numbers of individuals, unless the Aadhaar numbers have been redacted or blacked out through appropriate means, both in print and electronic form' (UIDAI 2016, 76). This provision is being amended to allow for public disclosure of records of a person containing their Aadhaar number for a specified purpose after securing their consent (UIDAI 2023). This effort towards providing more agency and control to citizens over their data is in response to an ongoing series of events and issues of mistrust narrated in the next section that contributed to the turn of Aadhaar into confidential numbers.

Mistrust in data security practices of Aadhaar

Mistrust in 'Data Leaks'

As a public data infrastructure, trust in Aadhaar is deeply intertwined with its ownership by the Indian government. On one hand, trust in government has implied trust in Aadhaar. Shankar Maruwada, the former head of demand generation at the UIDAI, noted the role of trust in the high

demand for Aadhaar enrollment: 'We found that India's biggest brand is the '*sher chhaap*'[2] – the symbol of the government' (Nilekani and Shah 2015, xxvi). In a conversation with Pranay, another member of Aadhaar's design team, he further elaborated on '*sher chhaap*':

> The government is one of the most trusted brands in India. We realized that the initial problem of demand generation was not a problem at all, because in rural areas, people tend to believe that if the government is trying to do something, it is for a new service, and you could get some benefit out of it. The mistrust of the government is a middle-class phenomenon. They were the last adopters. So, for example, in my area, no one took any interest in my work on Aadhaar for the first two years. It was only later that they came to me for 'help' with Aadhaar enrollment. (Fieldnotes, 25 August 2015)

On the other hand, mistrust of the government has also been crucial in widespread appropriation of Aadhaar for its imagined potential in manifesting accountability in governance. For example, Christopher Pinney, an anthropologist of visual culture in South Asia, describes the 2011 anti-corruption movement as a catalyst for initial enthusiasm for Aadhaar among public(s) gathered around issues of 'imbalance in the distribution of the visible' within the Indian population (Pinney 2015, 33). The movement 'repeatedly conjured an image of a state blind to the injustices suffered by citizens. Manmohan Singh [the then Prime Minister] was depicted as Dhritrashtra, the blind king from the Mahabharata, and as head of an 'andhi sarkar' (blind government)' (Pinney 2015, 33). Aadhaar addressed these concerns of becoming visible to the state by producing a standardized data record on every resident. Trust in Aadhaar remains crucial for infrastructural processes through which it mediates the relationship between citizens and the Indian state.

However, beyond critiques of its relationship with the government, civil society organizations have also expressed rich public dissent on and mistrust of Aadhaar with questions around its use of biometrics and its data security practices right since its inception (Khera 2018). The critics of the project have consistently pointed to the fallibility of biometrics in uniquely identifying segments of Indian population (such as manual laborers and the elderly) and possibilities of data convergence and surveillance through circulation of Aadhaar-enabled data. Such critical civil society responses to Aadhaar gained momentum in early 2017 with growing list of social media complaints and press reports on 'data leaks' where Aadhaar numbers were made publicly accessible at a large scale on government websites (Pahwa 2017; SFLC 2017). This controversy took shape on Twitter under the hashtag #AadhaarLeaks[3] (Sharma's tweet was a response to it) and offline in debates over Aadhaar in multiple arenas including the Supreme Court of India. These 'data leaks' often followed a similar pattern: A government department released a list of beneficiaries of its scheme, which included their personally identifiable information including redacted or complete Aadhaar numbers. The report published in May 2017 by the Center for Internet and Society (CIS) based in Bengaluru concretely exemplified this pattern by highlighting four government projects run by different state and central government departments that disclosed personally identifiable information of beneficiaries (Sinha and Kodali 2017). The report estimated public disclosure of around 130–135 million Aadhaar numbers and around 100 million bank account numbers.

Such civil society anxieties over information disclosure at scale raises several interrelated issues: *First*, both these numbers can be and are often shared publicly to promote recognition in the formal economy. Knowing these numbers by themselves is not a sufficient condition for successful authorization of any service. Yet, their disclosure produces anxiety in experiences of a loss of control over who may have access to them. It calls attention back to the fundamental paradox of publicly sharing identity numbers. *Second*, these departments are mandated to disclose information on beneficiaries to ensure transparency in delivery of government services under the Right to Information (RTI) Act. Such transparency mandates raise the question: *When does public data disclosure constitute a data leak?* I used quotes around data leaks earlier in this subsection to forebode this tension between an established bureaucratic practice for good governance and its potential unintended consequences such as privacy harms and increased risk of identity theft or financial fraud. Finally, *third*, although redacting Aadhaar numbers was mandated in such public disclosures, there was 'no

consistent standard' for such redaction; either the first few digits or the middle digits arbitrarily redacted (Sinha and Kodali 2017, 14). In the circulation of Aadhaar numbers, managing consistency in data security practices becomes increasingly harder. The possibility of reconstructing Aadhaar numbers through aggregation was plausible and eventually inevitable.

More than a year after publishing its report, CIS issued a clarification in November 2018:

> To our knowledge, no harm, financial or otherwise has been caused to anyone due to the public availability. […] We published the report only after ascertaining that the websites in questions had masked or removed the data. Therefore our report only points to the possibility that there could be harm caused by malicious actors before the data was taken down. However, we are not aware of any such cases of exploitation, nor do we suggest so anywhere in our report. (Sinha and Kodali 2018)

On the one hand, this conclusion resonates with issues faced by victims of data breaches in claiming that they have been concretely harmed. In the United States, for example, most data breach lawsuits where victims have claimed risk of and anxiety over future identity theft and fraud have been dismissed by the courts as 'insufficient to warrant recognition of harm' (Solove and Citron 2018, 739). On the other hand, sharing Aadhaar numbers on government websites created conditions of mistrust in two ways: first, there was a general sense of mistrust around future risks of such disclosure, and second, there was mistrust in the ability of the government departments to competently maintain and secure citizen data.

This emergent feeling of mistrust within civil society pushed the UIDAI to begin a media campaign to assure the Indian public(s) that Aadhaar data has not been breached or leaked from its own database and thus, their biometric data is secure (UIDAI 2017). Furthermore, it began the work of getting publicly shared Aadhaar numbers removed from other government websites. In response to a RTI inquiry in November 2017, the UIDAI revealed that about 201 government websites were publicly displaying Aadhaar details of the beneficiaries of their schemes, which were subsequently removed (PTI 2017a). In the 'data leaks' controversy, the public disclosure of Aadhaar numbers did not challenge the assumptions of the design team and the harm seemed unclear. In the next subsection, I focus on fraud as a form of harm emergent in unauthorized uses of Aadhaar numbers that only exacerbate with their public disclosure.

Mistrust in authorization

Aadhaar numbers were considered publicly shareable under the assumption that by themselves they are not a sufficient condition for authorizing access to any service. The number needs to be combined with additional data such as biometrics, an OTP, or other demographic data. These combinations produce a range of outcomes for secure authorization: combining Aadhaar numbers with biometrics is considered the most secure, while combining it with demographic information is considered the least secure (UIDAI 2011). This assumption, however, was put to test in systematic efforts to compile reports of Aadhaar-based fraud (Somanchi 2018; 2020). Most of these reports center on fake or forged Aadhaar numbers (Saldanha 2018). In these cases, the Indian state is the victim of fraud where fake beneficiaries are added to welfare schemes. A good example here is Sharma being registered as an eligible farmer in a welfare program after he tweeted his Aadhaar number. He received three installments of welfare payments before his account was deactivated (Ahmed 2020). However, a significant number of these stories also focused on Aadhaar-related banking fraud (Saldanha 2018). Here, Indian residents are victims of fraud. These reports typify a pattern of phishing scams where residents are made to reveal their OTPs, for example, 'con-men tricked persons on the pretext of linking their Aadhaar to their PAN (issued by the income-tax department for taxation) into revealing an OTP which was then used to change the linked-mobile number in the Aadhaar database' (Somanchi 2018). Once the mobile number linked to Aadhaar number is changed, fraudulent digital transactions in the name of the victim through authentication via OTPs can continue until the victim can secure due process to rectify the situation.

The design team would argue that this authentication is based on what residents have (i.e. an OTP or paper-based identity document) rather than who they are (i.e. their biometrics). Biometrics are more secure. An OTP or paper-based documents are unfortunate trade-offs to account for diversity in infrastructural conditions of a country where biometric authentication is not always possible. On the state's side, the 2018 Supreme Court ruling on limiting access of private agencies to Aadhaar numbers has made it difficult for banks to digitally verify Aadhaar data, which has increased the possibility of opening bank accounts based on fake cards. Banks are accountable for checking the veracity of such cards and confirming KYR details before opening accounts. Similarly, government departments are responsible for rigorously enforcing eligibility conditions to welfare programs. When these checks lack rigor, publicly disclosed Aadhaar numbers and fake Aadhaar cards, combined with bank accounts connected with them become readily available tools to perpetrate fraud (Sircar and Sachdev 2020). On the resident's side, the responsibility of making the mistake of revealing confidential information such as OTPs is also placed solely on the victims. It is, what Sharma would describe as, 'privacy or security vulnerabilities already present in the digital world' (Sharma 2020, 123). In both cases, the victim is blamed for their vulnerability to fraud, which in turn fosters secrecy in disclosing and mistrust as a norm in using Aadhaar numbers. Such vulnerability is again not just a matter of lacking data infrastructure literacy (Gray, Gerlitz, and Bounegru 2018); it is also an uneven structural consequence of societal inequities along well-recognized intersections of gender, class, caste, and ability.

I have discussed cases of fraud perpetrated by external actors up until now, there have also been cases of fraud by actors internal to Aadhaar's authentication ecosystem. A typical example of this kind would be when organizations within Aadhaar's authentication ecosystem authorized to access residents know-your-resident (KYR) information – e-KYC User Agencies (KUAs) – use it to create new service accounts (such as digital wallets) for residents without their informed consent (PTI 2017b). Government subsidies can then be digitally rerouted from the beneficiaries' existing bank account to these new mobile wallet accounts, which the beneficiaries have no knowledge of creating (Venkatanarayanan and Lakshmanan 2017). An argument could be made here that since the subsidy was still transferred into digital wallets of beneficiaries themselves, there was no harm done. However, *when a beneficiary does not have any knowledge of creating such an account, then should it not be considered a form of fraud?* This form of fraud emerges in conditions of circulation of resident data without their informed consent or knowledge within and across organizations internal to the structural arrangement designed to secure trust in a public data infrastructure.

Responding to the potential of external and internal Aadhaar-based fraud, the UIDAI introduced a new set of technical interventions in January 2018 to provide residents with the option of not having to share their Aadhaar numbers at all for authentication. In lieu of Aadhaar numbers, authentication could also be conducted through a combination of two unique numbers, one used by the resident and the other used by the authenticating agency:

(1) For a resident seeking enhanced protection of their Aadhaar data, UIDAI issued Virtual ID (VID), a temporary and revocable 16-digit random number mapped onto their Aadhaar number. Residents can share their VID, instead of Aadhaar, to access services. VID, however, cannot be used for de-duplication, and is only valid for a period set by the UIDAI (UIDAI 2019, 86).
(2) On the authenticating agency's side, since Virtual ID cannot be used for deduplication, the UIDAI offered a unique UID token for each Aadhaar number to each agency. The token is connected with the Aadhaar number of the resident accessing authentication services through the agency. Irrespective of the VID number provided by the resident in lieu of their Aadhaar number, the token remains the same on the backend for each agency (UIDAI 2019, 87–88).

The UID token also allowed the UIDAI to respond to internal fraud by differentiating levels of trust within the authentication system. Organizations designated as 'Local AUAs' were only allowed to

have access to limited KYR data based on UID tokens and were not allowed to store Aadhaar numbers at all. The UIDAI reserved the right to categorize organizations within its authentication ecosystem as 'Global AUAs,' which could be trusted to have access to e-KYR data and store Aadhaar numbers (UIDAI 2019, 87–88).

These interventions highlight how mistrust is a generative resource for organizing identification practices. Public disclosure of VID numbers is not as anxiety-inducing as Aadhaar numbers; VID numbers are temporary by design and residents have agency in revoking them as opposed to the permanent and unique nature of Aadhaar numbers. Similarly, UID tokens operationalize mistrust as an organizing principle for the authentication ecosystem. Organizations must earn the UIDAI's trust to become a Global AUA, and this trust can be revoked with their recategorization as a Local AUA. Audits and ensuring compliance become even more critical in such conditions of mistrust. The CAG report, for example, has pointed to the need for the UIDAI to be proactive in enforcing its regulations around audits and prescribed standards for data collection (CAG 2021).

With emerging concerns over public disclosure of Aadhaar numbers, the UIDAI and the government departments became more conscientious about redacting Aadhaar numbers. By August 2018, the UIDAI began to warn residents 'against sharing the number 'openly in the public domain,'' while encouraging them to use it 'without any hesitation' to prove their identity (Scroll Staff 2018). Redaction, however, was only the beginning of employing mistrust as a strategy. In contending with proliferation of Aadhaar-based fraud cases, the UIDAI invested in revocation of trust as a strategy to ensure data security. It not only provided residents with the individual agency to revoke their own identity credentials from any service provider, but also ensured a mechanism to implement differential trust and ability to revoke data access at scale from defaulting organizations within its authentication ecosystem. Addressing concerns of Aadhaar-based frauds, it further offered reassurances that neither can anyone open a bank account 'merely by using the Aadhaar number' nor can anyone 'withdraw money from a bank account merely by knowing an Aadhaar number' (Staff 2018). It re-invoked the requirement of two-factor authentication for any transaction. Diverse forms of trust, mistrust, and vigilance in the triadic relationship between the UIDAI, public/private organizations, and citizens/residents as public(s) are increasingly becoming the norm in maintenance of data security practices of Aadhaar.

Conclusion: securing Aadhaar as a public data infrastructure

This paper began with Aadhaar numbers being imagined as publicly shareable and ends with an emerging technical and regulatory regime that is slowly turning them into confidential numbers. My field stories present the conditions of possibility for using Aadhaar to identify Indian residents. Sharma and other members of Aadhaar's design team imagined Aadhaar to be a publicly shareable number because its usage was tightly coupled with who residents are (i.e. their biometrics) rather than what they have or know (for example, a card or a password). Several features of Aadhaar's infrastructural design showcase how the process of Aadhaar-based identification is siloed and distributed across an ecosystem of public and private organizations. These mechanisms to promote trust in Aadhaar's design broke down in emerging civil society anxieties over public disclosure of Aadhaar numbers on government websites, lack of audits and assurance of compliance by the UIDAI (CAG 2021), and emerging concerns around Aadhaar-based frauds by organizations/actors internal as well as external to its authentication ecosystem. Such breakdowns in trust are not a bug in organizing security practices of any public data infrastructure, they are a feature of it.

Mistrust is a generative organizational principle in contending with such breakdowns and to repair and reorganize practices to get any interaction back on track. For example, in late May 2022, a regional office of the UIDAI issued an advisory to warn residents against sharing photocopies of their Aadhaar cards to prevent the possibility of their misuse. This advisory was rescinded two days later after it provoked widespread mistrust and critique on social media of existing circulation of Aadhaar information. The UIDAI advised residents to exercise 'normal

prudence' in sharing Aadhaar numbers (Staff 2022). This short example succinctly illustrates my broader argument in this paper that the tensions over public/confidential nature of Aadhaar numbers has mirrored the shifting norms of trust/mistrust in their use as identity numbers. This tension is the backdrop against which the UIDAI responds to any challenge to Aadhaar's legitimacy.

Over the course of this paper, I have engaged with various dualities that can emerge at the intersection of discourses around recognition and surveillance in identification practices and debates around the interplay between technology and people, structure and agency, and trust and mistrust. I have shown that these dualities are not mutually exclusive; they are implicated in making sense of each of them individually. The way mistrust manifests in using Aadhaar affords an opportunity to reflect on how investments in technical, legal, administrative, and policy interventions to ensure trust in identity numbers is much like playing a game of Whack-A-Mole. A simple example here is that identity numbers (technical intervention) may ease problems of locating people through data in delivery of services, but they create surveillance concerns that are resolved in a court of law (legal intervention), through legislation (policy intervention) and ensuring compliance to standards (administrative intervention). Each intervention must hold its legitimacy and complement other interventions in different domains of state governance to practically achieve trust in identification. However, they also engender diverse operational challenges and thus, mistrust in identification. Aadhaar is technically designed to be a digital and public number to address the core challenge of mistrust in state-citizen relations and prevent fraud. It was designed to ensure that knowing the number itself was insufficient in authorizing access to any service. However, without appropriate administrative verification of their veracity, Aadhaar numbers become implicated in fraud and mistrust as possession of even a fake card can be enough to authorize access to services. Trust in identity numbers is only achieved partially through imbrication of these serially linked interventions. Mistrust triggers another cycle of interventions that build on existing interventions and produce their own operational challenges and consequences. Although these cycles will continue, the current arrangement of these interventions is turning Aadhaar into confidential identity numbers.

Finally, in this paper, I showcase mistrust in state-citizen relations as the foundational norm of organizing identity numbers (Chatterjee 2002). This does not imply that state-citizen relations are not possible or cannot be maintained; rather it implies that they require continuous rearticulation and recalibration. This is evident in UIDAI's ongoing work of encouraging the everyday use of Aadhaar by citizens in interacting with any organization and turning it from a public to confidential identity number. UIDAI's ultimate hope is that Aadhaar will slowly become the invisible background (Star and Ruhleder 1996) of everyday lives of Indian citizens/residents (UIDAI 2010). However, what is invisible background for one kind of public is a daily object of concern for another. On one hand, public(s) for whom Aadhaar increasingly becomes invisible exhibit a form of trust in the Indian state; trust that is practically established through measured responses to emergent challenges of mistrust in Aadhaar's authority and credibility. On the other hand, digital mistrust is crucial to the process of questioning public data infrastructures; *mistrust makes infrastructures visible*. Public(s) for whom Aadhaar remains an object of concern, and hence visible (whether in the terms of struggles to achieve recognition or resist surveillance), will continue to assert their mistrust as a resource to demand interventions in its operation as an identity number and data security practices. Trust, after all, is earned, not given.

Notes

1. See, the Aadhaar Dashboard: https://www.uidai.gov.in/aadhaar_dashboard/.
2. Hindi for 'mark of a lion.' The imprint of the state emblem of India features three Asiatic lions standing back-to-back on a circular base.
3. See, posts on Twitter: https://twitter.com/hashtag/AadhaarLeaks

Acknowledgments

I would like to thank the editors of this special issue, Kristoffer Albris and James Maguire, anonymous reviewers, and members of the RAW session at Data & Society Research Institute for their invaluable feedback and suggestions. Parts of the paper were presented in a Data & Society academic workshop on Trust and Doubt in Public-Sector Data Infrastructures in 2021 and in a session on Trust in a Digital Age at the 21st Science and Democracy Network Annual Meeting in 2022.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

Fieldwork for this research was supported by National Science Foundation [Grant Number 1655753]. Support for writing this paper was provided by Siegel Family Foundation.

ORCID

Ranjit Singh http://orcid.org/0000-0001-6453-8676

Notes on contributor

Ranjit Singh is a Researcher at the AI on the Ground Initiative of Data & Society Research Institute. His research interests lie at the intersection of data infrastructures, global development, and public policy. His current research projects invigorate existing efforts to reframe the global south as home to the majority of the human population and investigate the diverse ethics, politics, and experiences of living with and regulating data and AI. His dissertation research at Cornell University focused on data-driven marginality and challenges faced by citizens in claiming voice and representation through data in biometrics-based data-driven organization of welfare services in India.

References

Acquisti, Alessandro, and Ralph Gross. 2009. "Predicting Social Security Numbers from Public Data." *Proceedings of the National Academy of Sciences* 106 (27): 10975–10980. https://doi.org/10.1073/pnas.0904891106.

Ahmed, Yasmin. 2020. "Former UIDAI Chief RS Sharma Suffers Aadhaar Fraud, Rs 6000 PM Kisan Fund Deposited in His Account." *India Today*, December 14, 2020.

Breckenridge, Keith, and Simon Szreter. eds. 2012. *Registration and Recognition: Documenting the Person in World History (Proceedings of the British Academy)*. Oxford: Oxford University Press.

Broussard, Meredith. 2018. *Artificial Unintelligence: How Computers Misunderstand the World*. Cambridge, MA: MIT Press.

CAG. 2021. *Report of the Comptroller and Auditor General of India on Functioning of Unique Identification Authority of India*. New Delhi.

Carey, Matthew. 2017. *Mistrust: An Ethnographic Theory*. Chicago, IL: HAU Books.

Chatterjee, Partha. 2002. *A Princely Impostor? The Strange and Universal History of the Kumar of Bhawal*. Princeton, NJ: Princeton University Press.

Cheney-Lippold, John. 2017. *We Are Data: Algorithms and the Making of Our Digital Selves*. New York: New York University Press.

Cohen, Lawrence. 2019. "The 'Social' De-Duplicated: On the Aadhaar Platform and the Engineering of Service." *South Asia: Journal of South Asian Studies* 42 (3): 482–500. https://doi.org/10.1080/00856401.2019.1593597.

Dewey, John. 1927. *The Public and Its Problems*. New York: H. Holt and Company.

FTC. 2008. *Security in Numbers: SSNs and ID Theft*. Washington, DC: Federal Trade Commission.

Gelb, Alan, Anit Mukherjee, and Kyle Navis. 2020. *Citizens and States: How Can Digital ID and Payments Improve State Capacity and Effectiveness?* Washington, DC: Center for Global Development.

Gopinath, Ravindran. 2012. "Identity Registration in India During and After the Raj." In *In Registration and Recognition: Documenting the Person in World History*, edited by Keith Breckenridge, and Simon Szreter, 299–322. Oxford: Oxford University Press.

Gray, Jonathan, Carolin Gerlitz, and Liliana Bounegru. 2018. "Data Infrastructure Literacy." *Big Data & Society* 5 (2): 1–13. https://doi.org/10.1177/2053951718786316.

Greene, Daniel. 2021. *The Promise of Access: Technology, Inequality, and the Political Economy of Hope*. Cambridge, MA: MIT Press.
Herd, Pamela, and Donald P Moynihan. 2019. *Administrative Burden: Policymaking by Other Means*. 1st ed. New York: Russell Sage Foundation.
Hickok, Elonnai. 2015. "Aadhaar Number vs the Social Security Number." CIS India Website. 2015. https://cis-india.org/internet-governance/blog/aadhaar-vs-social-security-number.
High Level Panel on Humanitarian Cash Transfers. 2015. *Doing Cash Differently: How Cash Transfers Can Transform Humanitarian Aid*. London: ODI.
Jonnalagadda, Kiran. 2017. "Public, Private and Secret Information." Kaarana. 2017. https://medium.com/karana/public-private-and-secret-information-f857f3931f6b.
Khera, Reetika. ed. 2018. *Dissent on Aadhaar: Big Data Meets Big Brother*. Delhi: Orient BlackSwan.
Kulkarni, Tanu. 2015. "Aadhaar May Soon Replace Roll Numbers." *The Hindu*, August 21, 2015.
Latonero, Mark. 2018. *Governing Artificial Intelligence: Upholding Human Rights & Dignity*. New York: Data & Society Research Institute.
Lee, John D, and Katrina A See. 2004. "Trust in Automation: Designing for Appropriate Reliance." *Human Factors: The Journal of the Human Factors and Ergonomics Society* 46 (1): 50–80. https://doi.org/10.1518/hfes.46.1.50.30392.
Luhmann, Niklas. 2017. "Trust and Power." Translated by Christian Morgner and Michael King. 1st ed. Malden, MA: Polity.
Lyon, David. 2009. *Identifying Citizens: Id Cards as Surveillance*. Cambridge: Polity.
Madianou, Mirca. 2019. "Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises." *Social Media + Society* 5 (3). https://doi.org/10.1177/2056305119863146.
Marcus, George E. 1995. "Ethnography in/of the World System: The Emergence of Multi-Sited Ethnography." *Annual Review of Anthropology* 24 (1): 95–117. https://doi.org/10.1146/annurev.an.24.100195.000523.
Marwick, Alice E, and boyd danah. 2014. "Networked Privacy: How Teenagers Negotiate Context in Social Media." *New Media & Society* 16 (7): 1051–1067. https://doi.org/10.1177/1461444814543995.
Masiero, Silvia, and S. Shakthi. 2020. "Grappling with Aadhaar: Biometrics, Social Identity and the Indian State." *South Asia Multidisciplinary Academic Journal* 23. https://doi.org/10.4000/samaj.6279.
Mayer, Roger C, James H Davis, and F. David Schoorman. 1995. "An Integrative Model Of Organizational Trust." *The Academy of Management Review* 20 (3): 709–734. https://doi.org/10.2307/258792.
Mcknight, D Harrison, Michelle Carter, Jason Bennett Thatcher, and Paul F Clay. 2011. "Trust in a Specific Technology." *ACM Transactions on Management Information Systems* 2 (2). https://doi.org/10.1145/1985347.1985353.
McKnight, D Harrison, Vivek Choudhury, and Charles Kacmar. 2002. "Developing and Validating Trust Measures for E-Commerce: An Integrative Typology." *Information Systems Research* 13 (3): 334–359. https://doi.org/10.1287/isre.13.3.334.81.
Monahan, Torin, David J Phillips, and David Murakami Wood. 2010. "Surveillance and Empowerment." *Surveillance & Society* 8 (2): 106–112. https://doi.org/10.24908/ss.v8i2.3480.
Möllering, Guido. 2001. "The Nature of Trust: From Georg Simmel to a Theory of Expectation, Interpretation and Suspension." *Sociology* 35 (2): 403–420. https://doi.org/10.1177/S0038038501000190.
Nair, Vijayanka. 2021. "Becoming Data: Biometric IDs and the Individual in 'Digital India'." *Journal of the Royal Anthropological Institute* 27 (S1): 26–42. https://doi.org/10.1111/1467-9655.13478.
Nilekani, Nandan, and Viral Shah. 2015. *Rebooting India: Realizing a Billion Aspirations*. Gurgaon: Penguin Books India.
Pahwa, Nikhil. 2017. "#AadhaarLeaks: A List of Aadhaar Data Leaks." Medianama. 2017. https://www.medianama.com/2017/04/223-aadhaar-leaks-database/.
Pinney, Christopher. 2015. "Civil Contract of Photography in India." *Comparative Studies of South Asia, Africa and the Middle East* 35 (1): 21–34. https://doi.org/10.1215/1089201X-2876068.
PTI. 2017a. "UIDAI Reveals 210 Govt Websites Made Aadhaar Details Public, Did Not Specify When Breach Took Place." *FirstPost*, November 19, 2017.
PTI. 2017b. "UIDAI Suspends E-KYC Licence of Airtel, Airtel Payments Bank Over Alleged Aadhaar Misuse." *The Wire*, December 17, 2017.
Ruppert, Evelyn S, Engin Isin, and Didier Bigo. 2017. "Data Politics." *Big Data & Society* 4 (2): 1–7. https://doi.org/10.1177/2053951717717749.
Sadiq, Kamal. 2009. *Paper Citizens: How Illegal Immigrants Acquire Citizenship in Developing Countries*. Oxford: Oxford University Press.
Saldanha, Alison. 2018. "164 Aadhaar-Related Frauds Reported Since 2011, Most in 2018: New Database." *IndiaSpend*, May 22, 2018.
Scott, James C. 1998. *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*. New Haven: Yale University Press.

Sethi, Aman. 2017. "Fresh Concerns After Cops Bust Gang Cloning Fingerprints of Aadhaar Operators." *Hindustan Times*, September 12, 2017.
Sethi, Aman. 2018. "AADHAAR Seeding Fiasco: How To Geo-Locate By Caste and Religion In Andhra Pradesh With One Click." *HuffPost*. 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.
SFLC. 2017. "Aadhaar Breaches and Leaks." Software Freedom Law Center, India's Website 2017. https://sflc.in/uidai-aadhaar-breaches-and-leaks.
Staff, Scroll. 2018. "UIDAI Warns Citizens Against Sharing Aadhaar Number in Public." *Scroll.In*, 2018.
Staff, Scroll. 2022. "Centre Asks Not to Share Photocopies of Aadhaar, Then Withdraws Advisory." *Scroll.In*, May 29, 2022.
Shahar, Avin, Belfield Haydn, Brundage Miles, Krueger Gretchen, Wang Jasmine, Weller Adrian, Anderljung Markus, et al. 2021. "Filling Gaps in Trustworthy Development of AI." *Science* 374 (6573): 1327–1329. doi:10.1126/science.abi7176.
Shakthi, S. 2020. "Crafting "Integrity": The Implications of Authentication Through Unique Identification Databases." *South Asia Multidisciplinary Academic Journal* 23. https://doi.org/10.4000/samaj.6414.
Sharma, Ram Sewak. 2020. *The Making of Aadhaar: World's Largest Identity Platform*. New Delhi: Rupa.
Silvast, Antti, and Mikko J. Virtanen. 2019. "An Assemblage of Framings and Tamings: Multi-Sited Analysis of Infrastructures as a Methodology." *Journal of Cultural Economy* 12 (6): 461–477. https://doi.org/10.1080/17530350.2019.1646156.
Singh, Ranjit. 2019. "Give Me a Database and I Will Raise the Nation-State." *South Asia: Journal of South Asian Studies* 42 (3): 501–518. https://doi.org/10.1080/00856401.2019.1602810.
Singh, Ranjit, and Steven J. Jackson. 2021. "Seeing Like an Infrastructure: Low-Resolution Citizens in the Aadhaar Identification Project." *Proceedings of the ACM on Human-Computer Interaction* 5 (315):1–28. https://doi.org/10.1145/3476056.
Sinha, Amber, and Srinivas Kodali. 2017. *Information Security Practices of Aadhaar (or Lack Thereof): A Documentation of Public Availability of Aadhaar Numbers with Sensitive Personal Financial Information.* Bengaluru.
Sinha, Amber, and Srinivas Kodali. 2018. Clarification on the Information Security Practices of Aadhaar Report." CIS India Website. 2018. https://cis-india.org/internet-governance/blog/clarification-on-the-information-security-practices-of-aadhaar-report.
Sircar, Sushovan, and Vakasha Sachdev. 2020. "Revealed: How Publicly Available Aadhaar Was Used in PM KISAN Scam." *The Quint*, December 11, 2020.
Solove, Daniel J., and Danielle Keats Citron. 2018. "Risk and Anxiety: A Theory of Data-Breach Harms." *Texas Law Review* 96 (4): 737–786.
Somanchi, Anmol. 2018. "Aadhaar Fraud Is Not Only Real, But Is Worth More Closely Examining." *The Wire*, May 3, 2018.
Somanchi, Anmol. 2020. "Database of Aadhaar Fakes & Fradulent Transaction (DAFFT)." Google Document. 2020. https://docs.google.com/spreadsheets/d/1RGBHeWSxebftjIJGku4Z8MsMvqSwt934eFVNS1Tpl6Y/edit#gid = 1555027670.
Sperfeldt, Christoph. 2022. "Legal Identity in the Sustainable Development Agenda: Actors, Perspectives and Trends in an Emerging Field of Research." *The International Journal of Human Rights*, 217–238. https://doi.org/10.1080/13642987.2021.1913409.
Sriraman, Tarangini. 2018. *In Pursuit of Proof: A History of Identification Documents in India*. New Delhi: Oxford University Press.
Star, Susan Leigh, and Karen Ruhleder. 1996. "Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces." *Information Systems Research* 7 (1): 111–134. https://doi.org/10.1287/isre.7.1.111.
Sztompka, Piotr. 2000. *Trust: A Sociological Theory*. New York: Cambridge University Press.
TEDxBangalore. 2016. *Aadhar: A Number to Facilitate the Lives of the Next Billion | Dr. Pramod Varma*. India: YouTube.
Thatcher, Jason Bennett, D. Harrison McKnight, E. W. Baker, R. E. Arsal, and N. H. Roberts. 2011. "The Role of Trust in Postadoption IT Exploration: An Empirical Examination of Knowledge Management Systems." *IEEE Transactions on Engineering Management* 58 (1): 56–70. https://doi.org/10.1109/TEM.2009.2028320.
Thiebes, Scott, Sebastian Lins, and Ali Sunyaev. 2021. "Trustworthy Artificial Intelligence." *Electronic Markets* 31 (2): 447–464. https://doi.org/10.1007/s12525-020-00441-4.
Turkkan, Candan. 2023. "Screening for Eligibility: Access and Resistance in Istanbul's Food Banks." *Journal of Cultural Economy* 16 (2): 151–167. https://doi.org/10.1080/17530350.2023.2176339.
UIDAI. 2010. *UIDAI Strategy Overview: Creating a Unique Identity Number for Every Resident in India*. New Delhi: Unique Identification Authority of India.
UIDAI. 2011. *Aadhaar Authentication Framework (Version 1.0)*. New Delhi: Unique Identification Authority of India.

UIDAI. 2014. *Aadhaar Technology and Architecture: Principles, Design, Best Practices, & Key Lessons.* New Delhi: Unique Identification Authority of India.
UIDAI. 2016. *Unique Identification Authority of India (Transaction of Business at Meetings of the Authority) Regulations*. The Gazette of India.
UIDAI. 2017. *Aadhaar Data Is Never Breached or Leaked: UIDAI. UIDAI Press Releases*. November 20, 2017.
UIDAI. 2019. *Compendium of Regulations, Circulars, & Guidelines for AUA, KUA, ASA, and Biometric Device Provider.* New Delhi: Unique Identification Authority of India.
UIDAI. 2023. *The Aadhaar (Sharing of Information) (First Amendment) Regulations,* 2023. https://uidai.gov.in/images/Revised_Draft_Sharing_of_Information_Regulations_20042023_CEO_Sir_approved.pdf.
UIDAI. n.d. "Aadhaar Dashboard." Unique Identification Authority of India. Accessed May 17, 2022. https://uidai.gov.in/aadhaar_dashboard/.
USAID. 2020. *Identity in a Digital Age: Infrastructure for Inclusive Development.* Washington, DC: Center for Digital Development, USAID.
Venkatanarayanan, Anand, and Srikanth Lakshmanan. 2017. "Aadhaar Mess: How Airtel Pulled Off Its Rs 190 Crore Magic Trick." *The Wire*, December 21, 2017.
Warner, Michael. 2005. *Publics and Counterpublics*. New York: Zone Books.
Watson, Rod. 2009. "Constitutive Practices and Garfinkel's Notion of Trust: Revisited." *Journal of Classical Sociology* 9 (4): 475–499. https://doi.org/10.1177/1468795X09344453.
Weitzberg, Keren, Margie Cheesman, Aaron Martin, and Emrys Schoemaker. 2021. "Analysis and Best Parameters Selection for Person Recognition Based on Gait Model Using CNN Algorithm and Image Augmentation." *Journal of Big Data* 8 (1): 1–7. https://doi.org/10.1186/s40537-020-00387-6.
World Bank Group. 2016. *Identification for Development: Strategic Framework.* Washington, DC: World Bank.