Information, Communication & Society

ISSN: 1369-118X (Print) 1468-4462 (Online) Journal homepage: https://www.tandfonline.com/loi/rics20

Aadhaar and data privacy: biometric identification and anxieties of recognition in India

Pawan Singh

To cite this article: Pawan Singh (2019): Aadhaar and data privacy: biometric identification and anxieties of recognition in India, Information, Communication & Society, DOI: 10.1080/1369118X.2019.1668459

To link to this article: https://doi.org/10.1080/1369118X.2019.1668459

Published online: 07 Oct 2019.

INFORMATION, COMMUNICATION & SOCIETY
https://doi.org/10.1080/1369118X.2019.1668459

Routledge
Taylor & Francis Group

Aadhaar and data privacy: biometric identification and anxieties of recognition in India

Pawan Singh[a,b]

[a]Contemporary Histories, Deakin University, Melbourne, Australia; [b]Australia India Institute, University of Melbourne, Melbourne, Australia

ABSTRACT

The data privacy debate in India has evolved with respect to the government's biometric identity programme, Aadhaar that enrols welfare-dependent, poor populations to grant them access to government benefits. While legal challenges to Aadhaar by civil society groups argued that the biometric identity infrastructure creates conditions of mass surveillance and violation of individual privacy, the Indian Supreme Court in 2018 ruled that the government was justified in restricting individual privacy for the collective good of providing welfare in a transparent and corruption-free manner. Given the disproportionate burden on these populations to prove their identities to the state, this paper draws on a close reading of legal and policy texts, and activist documentation to argue that there is a need to move beyond the narrative of mass surveillance as privacy violation. Data privacy interests of the welfare-dependent emerge in the moment of biometric authentication, which creates anxieties of recognition when their authentication attempts fail or are deliberately falsified. Often, to have better social mobility, they are compelled to be physically mobile in order to enrol or update their records under conditions of physical disability and meagre socioeconomic means. These anxieties illuminate their privacy interests through a compromise of dignity or dignified living, a formulation articulated in the 2018 Aadhaar verdict. The paper makes a critical contribution to the global conversation on data privacy through a discussion of the Indian case that demonstrates the privacy-recognition nexus in local contexts.

ARTICLE HISTORY
Received 8 October 2018
Accepted 1 September 2019

KEYWORDS
Data privacy; biometrics; recognition; anxieties; dignity; class

Introduction

In India, concerns around data privacy have emerged predominantly around the government's biometric identity project, Aadhaar – the world's largest biometric identity database with 1.2 billion subscribers in 2018. Aadhaar was launched in 2009 with the setting up of the Unique Identification Authority of India (UIDAI) but the first number was rolled out in September, 2010 in Tembhli village in the Western state of Maharashtra (Byatnal, 2010). The UIDAI envisioned Aadhaar as a mode of unique identification for the

CONTACT Pawan Singh pawan.singh@deakin.edu.au

socioeconomically marginalized groups to enable them to access welfare in a transparent manner.

However, from 2012 onwards, numerous legal petitions challenged the constitutional validity of Aadhaar in the Indian Supreme Court (SC hereon) on the grounds that the linkage of Aadhaar to welfare and other services would violate Indian citizens' right to privacy, leading to a surveillance state. In 2018, the SC upheld the constitutional validity of mandatory Aadhaar for the delivery of welfare to the poor while exempting the scheme's mandatory linkage from non-welfare services such as banking and mobile phone communications except taxation. In the mainstream debate on Aadhaar, the privacy question has remained central in various legal challenges to Aadhaar that also pertained to exclusion from benefits, denial of rights, potential for surveillance and coercion to enrol (Bhuyan, 2018).

This paper examines the data privacy debate in India to demonstrate how the privacy interests of Aadhaar's primary beneficiaries or the welfare-dependent groups emerge through the biometric mediation of their identity's recognition. The paper proposes that the privacy interests of the welfare-dependent groups in the mainstream Aadhaar debate have predominantly been framed through universally acknowledged ideas pertaining to individual autonomy (consent to enrol) and surveillance (data security), which provides a limited view of their privacy interests. Instead, the paper argues that a nuanced and grounded understanding of the beneficiaries' privacy interests emerge in the moment of biometric authentication failure or deliberate falsification despite Aadhaar's promise of unique identification. Such a predicament leads to uncertainty over one's identification for the purposes of welfare and benefits, or what the paper calls 'anxieties of recognition' for the beneficiary whose biometrics are not recognized by the scanner owing to a number of technical, human and infrastructural factors. The anxieties of recognition are further experienced in the process of trying to enrol in Aadhaar or update records in order to remain legible to the state for welfare benefits.

By interrogating the promise of unique identification underlying Aadhaar in relation to instances of biometric authentication failure – 2 million according to the State of Aadhaar 2017-18 report based on a survey in three major parts of India[1] – the paper elucidates how anxieties of recognition emerge as a central concern for the welfare-dependent groups who are mandatorily enrolled in Aadhaar. Because these anxieties relate to their efforts to remain legible to the state, their privacy interests materially manifest as a compromise of dignity or dignified living, as affirmed by the SC in 2018.

The next section defines the conceptual framework and key terms followed by, contribution, methods/sources and an overview of Aadhaar in policy and law. The subsequent section examines statements of excluded welfare beneficiaries and their hardships due to Aadhaar. The discussion situates anxieties of recognition within broader debates on biometric identity.

Conceptual framing and key terms

In the legal debate that unfolded in the SC, the government and pro-Aadhaar groups defended Aadhaar as empowering the poor through benefits while in their view, privacy was an 'elite' concern.[2] Lawyers and activists challenging Aadhaar, however, have countered how biometric technology flaws and potential for data breaches render the poor particularly vulnerable to mass surveillance while reducing them to a single number.[3]

The coupling of privacy with class in the Aadhaar debate has emerged along two main positions, one upholding socioeconomic empowerment through unique biometric identification as more important than privacy and the other asserting that privacy matters to all irrespective of class. The paper defines class in the context of Aadhaar by reference to its primary objective i.e., socioeconomic empowerment of the poor, which was upheld by the SC as the legitimate purpose of Aadhaar to give a dignified life to the poor.[4] More specifically, this paper examines the Aadhaar experiences of a demographic defined under the National Food Security Act, 2013[5] as priority households –below poverty line or BPL including homeless, tribal groups and persons with disability among others, and the Antyodya Anna Yojna (AAY) comprising landless and marginal farmers, various artisans without stable income and households with terminally ill widows without any means of sustenance, and others who cannot obtain rations at BPL rates.[6]

Repeated or failed authentication attempts by a beneficiary using fingerprints on the scanner in many cases have led to a denial of benefits despite Aadhaar compliance. These resulted in the experience of attenuated autonomy, feeling of uncertainty over their biometric information and ultimately personal dignity of their identity – the primary purpose of Aadhaar. I take the definition of dignity from the SC's 2018 Aadhaar verdict, which stated that privacy is a postulate of dignity guaranteed by the Indian Constitution under rights to life and liberty. While acknowledging the constitutional basis of dignity in the right to individual autonomy (freedom to choose) and respect for those choices, the court defined dignity as being beyond an individual right, as a matter of common/public good. Drawing upon philosophers like Immanuel Kant and the Universal Declaration of Human Rights (UDHR), the judges based the notion of human dignity on socioeconomic rights recognizing three core facets: 1. Intrinsic value of human beings and their traits, freedom from discrimination and importantly, the right to physical and mental integrity – prohibition of physical harm such as torture, slavery or other degradation and personal honour and image. 2. Autonomy: defined as free will but specifically in the context of welfare, a basic right to the provision of adequate living conditions and the satisfaction of essential needs, and 3. Community Value: the role of state and community in establishing collective goals and restrictions on individual freedoms and rights on behalf of a certain idea of the good life. Dignity, in the court's view, requires balancing individual autonomy with the idea of a dignified living in the context of state welfare programmes.[7] This balancing of autonomy with dignity implies the privileging of dignified living in socioeconomic terms over individual autonomy to personal data submitted under Aadhaar enrolment.

Dignity thus attaches to what scholars have called the narrative dimensions of identity – the social, cultural and economic aspects (Ajana, 2013; Mordini & Massari, 2008), which are often disregarded in the moment of biometric mediation. I trace the compromise of dignity through the hardships faced by welfare beneficiaries as a form of anxieties of recognition, which comprise: 1. hardships faced during Aadhaar compliance i.e., Enrolling in Aadhaar, linking Aadhaar to ration cards and other analogue ID documents and ensuring one's details in the Aadhaar database are up to date, 2. Failed/falsified biometric authentication using fingerprints on an ongoing basis. Because these requirements are subject to factors like accurate biometric capture, easy access to Aadhaar enrolment centres/IT infrastructures and physical conditions of worn-out fingerprints due to age, manual work or disability, they undermine the promise of unique identification, which in turn, attenuates beneficiary's recognition for welfare access.

While fingerprint authentication is the most commonly used modality of verification, other modalities include a one-time password (OTP), which requires a mobile phone, and, the less common, iris scan. The process of authentication entails the flow of biometric data across networks in a particular context, and in instances of biometric authentication failure/falsification, it sometimes violates, what the media studies scholar Helen Nissenbaum (2010) has termed contextually relative informational norms. Nissenbaum observes that it is not so much that people want to control or hide information about themselves; Rather, they expect that the information about them flows appropriately according to context-relative informational norms. By contexts, she means socially structured settings that have historically evolved, and are 'subject to a host of causes and contingencies of purpose, place, culture, historical accident, and more' (p. 130). She defines context-relative informational norms as those that govern the flow of personal information including transmission, communication, transfer, distribution, and dissemination from one party to another or others in given contexts. When information flows according to norms and user expectations, contextual integrity (of recognition) is respected. It is violated when the norms are breached.

In the case of Aadhaar-compliant welfare beneficiaries, such contextually relative informational norms are violated when the Aadhaar-based biometric authentication (ABBA) returns a mismatch to scanned fingerprint or is deliberately falsified, a failure that often results in denial of food rations, wages or liquified petroleum gas. The beneficiaries repeated attempts to fulfil other compliance requirements similarly undermine the timely recognition of their claim on subsistence benefits without which they face starvation, and in some cases, death.

Nissenbaum's theory of privacy as contextual integrity of information is useful in examining Aadhaar-related privacy concerns because instead of approaching privacy as control over information sharing and its regulation through notice and consent type measures, it focuses on the expectations of the subject, types of information and constraints of transmission in a particular context. This speaks to the predicament of an Aadhaar-compliant beneficiary whose enrolment in Aadhaar shifts their privacy interests from consent and data security of biometrics[8] towards concerns of integral recognition that arise when biometrics mismatch, fail or are deliberately falsified. Specifically, this leads to, 1. An uncertainty over one's own recognition on which subsistence depends despite Aadhaar's promise of unique identification. 2. Loss of autonomy: the helplessness experienced when rations and other benefits are denied without recourse to alternative modes of identification and 3. Dignity: Such denial of benefits compromise dignity as defined above in terms of the right to physical and mental integrity pertaining to the intrinsic value of human identity, or recognition.[9]

A legitimate expectation for the beneficiary is the availing of welfare benefits upon successful biometric authentication (integrity of recognition), a process that entails data flows across networks according to specific protocols. Anxieties around one's recognition that question dignity as a privacy interest in Aadhaar also may be understood as a form of intangible privacy harm, or what legal privacy scholars Ryan Calo (2011) and Daniel Solove and Danielle Citron (2017) have called subjective privacy harms that are often difficult to adjudicate and entail experiences of distress, sadness and feelings of uncertainty. The life-long anxiety around proving one's identity to the state when welfare access is made contingent upon biometric authentication results in a legitimate privacy interest pertaining to one's recognition in future instances. Repeated authentication attempts erode the integrity of recognition in terms of beneficiary's agency and confidence about periodic authentication requirements for benefits.

A beneficiary's ability to authenticate also depends on easy access to authentication/enrolment centres, the absence of which entails what this paper calls 'compelled physical mobility' – the hardship of travel to these centres borne by beneficiaries under conditions of inadequate transportation and disability in some cases. In contrast to Aadhaar's promise of social mobility, beneficiaries in many cases are compelled to be physically mobile in order to remain legible to the state in a timely manner for recognition of their welfare claims. Aadhaar's large-scale success notwithstanding, the instances of biometric authentication failure that have led to exclusion from benefits and deaths from starvation from 2012-2018 necessitate an examination of how the project can better fulfil its promise.

Contribution

The Indian privacy debate, which has unfolded in the courtroom and public discourse simultaneously, instantiates how data privacy concerns in particular national contexts are articulated with respect to globally resonant concerns of mass surveillance through IT infrastructures (Monahan, 2010; Zuboff, 2019). The concerns are also communicated and contested publicly in those contexts with attention to local cultural norms and vulnerabilities while drawing upon global formulations of data security (Turow & Ribak, 2003).

This paper demonstrates how privacy neither simply concerns a liberal, autonomous, pre-cultural individual (Cohen, 2013) nor can it be adequately explained in traditional terms of the Big Brother, invasion or secrecy (Solove, 2004) Rather, privacy-related interests emerge from an 'informationization of the body', or the digitalization of physical and behavioural attributes of a person and their distribution across the global information network (Mordini & Massari, 2008, p. 494) that hold the potential to attenuate the integrity of recognition. This paper contributes to the global conversation on data privacy through a discussion of the Indian case, which illuminates the privacy-recognition nexus as understood from the lived experience of welfare beneficiaries under Aadhaar.

Methods and sources

The paper is a qualitative inquiry that draws on a close reading of three sets of sources: 1. Government documents including notifications by the UIDAI, 2. Legal sources, and 3. Activist documentation by *Rethink Aadhaar*, a non-partisan campaign[10] that has extensively documented video testimonies of the excluded welfare beneficiaries. Comprising India's eminent intellectuals including economist Reetika Khera, social activists Aruna Roy and Nikhil Dey of another well-regarded social movement Mazdoor Kisan Shakti Sangathan (*Labourers Farmers Power Collective* advocating for the rights of workers), innovator Anupam Saraph, and privacy activist Srinivas Kodali among others, the campaign has documented extensive empirical evidence of Aadhaar-related injustices on the ground in order to provide an impartial assessment of Aadhaar's implementation. In

July 2019, the Digital Empowerment Foundation (DEF) – a globally recognized Indian advocacy organization in the field of information and communication technology for development – nominated Rethink Aadhaar for the 'social media for empowerment' award for its work in communication advocacy and development activism.[11]

These sources were tracked online from 2012-2018, the period of multiple legal challenges to Aadhaar. The SC judgment and the UIDAI Strategy Overview were downloaded from Livelaw.in and uidai.gov.in respectively. The Rethink Aadhaar website was tracked to compile a list of video testimonials under the page EXCLUSION.[12] A hundred testimonials were analysed with attention to statements pertaining to failed fingerprint scans, fraud, means of physical mobility and access to IT infrastructure among others. The videos that were anywhere between 45 seconds and 12 minutes were transcribed except when regional language testimonials could not be translated. The data sources were triangulated by interpreting the configuration of privacy interests by the Indian government and the SC with the testimonies of excluded beneficiaries. The analysis paid attention to beneficiary statements, living conditions, issues of disability and the rural settings in which they were recorded to situate them within the broader socioeconomic context of deprivation. Three themes emerged from the video transcripts: 1. Biometric failure and falsification, 2. Compelled physical mobility and 3. Exceptional circumstances. These are analysed later in the paper.

Aadhaar: identity, data privacy and the law

Aadhaar followed a proposal by the National Democratic Alliance government in 2003 to launch a Multi-Purpose National Identity Card (MNIC), an initiative that was later implemented by the United Progressive Alliance government from 2004 onwards.[13] Aadhaar[14] began as a voluntary scheme in 2009 to offer the Indian poor a unique identity for them to avail of government welfare in a transparent and corruption-free manner. Nilekani and Shah (2016) describe unique identification under Aadhaar as providing a basic right to an acknowledged existence to the invisible poor masses in India without which they would remain ignored and nameless. This section of the population was deemed invisible to the government for want of a legitimate administrative identity. The Unique Identification (UID) or Aadhaar, a 12-digit random number was built around two criteria – 1. A unique basis of identity authentication to eliminate duplicate and fake identities in government benefits databases, and 2. Easy verification and authentication of subscriber credentials in a cost-effective manner (Yadav, 2014).

While the Indian government initially kept enrolment in Aadhaar voluntary, public-sector oil marketing companies made Aadhaar-based verification mandatory in certain states for the refilling of subsidized liquified petroleum gas (LPG) cylinders with a view to bring greater transparency in delivering benefits. Subsequently, for the direct transfer of subsidies to beneficiary bank accounts, banks also started notifying customers via text messages to link their Aadhaar information (H.K., 2018).

From 2014 onwards, Aadhaar's use expanded beyond the delivery of government services as the private sector began to implement mandatory e-KYC (electronic- know your customer) authentication using Aadhaar, making it 'the very basis of life', as a 2017 story in the Indian newspaper *The Economic Times* reports, with Aadhaar mandatory for banking, income tax, mobile phone connections, government scholarships, and the mid-day meal scheme that provides free lunch to government school students.[15] Consequently, multiple petitions filed in the SC challenged Aadhaar's constitutional validity, its mandatory linkage to various services and denial of benefits to welfare-dependent groups for want of Aadhaar. The court then issued notices in 2013 and 2015 directing the government to not deny benefits to anyone for want of Aadhaar.[16] In a press note dated February 2018, the UIDAI announced that no legitimate beneficiary shall be denied any essential services including ration through the public distribution system (PDS)[17], hospitalization and school admissions among others, if Aadhaar verification is not submitted.[18] In 2016, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act was passed as a money bill[19] in the Indian Parliament to provide legislative support to Aadhaar[20], which was also opposed by an Indian Congress party leader in the SC.[21]

The petitioners opposed Aadhaar's personal data collection and its expanding linkages to other databases and data aggregation by private actors that, they argued, held the potential to track an individual's activities leading to mass surveillance (Ramanathan, 2017). The UIDAI's ability to outsource the operations of the Central Data Identities Repository (CIDR) – which stores Aadhaar data – to a foreign or private entity as well as the controversy of mandatory linkage of Aadhaar to non-welfare services added to concerns of data security and identity theft (Greenleaf, 2010). From 2012 onwards, Aadhaar was embroiled in data security issues brought to the government's notice by research think-tanks like the *Centre for the Internet and Society*.[22] These breaches pertained to easy access to the Aadhaar database, duplicate cards, publishing of Aadhaar demographic data on government websites and in one case, use of biometric data to commit financial fraud[23] and, a 2019 breach pertaining to voter ids and Aadhaar in possession of a private firm.[24]

During the Aadhaar hearings in the SC, former Attorney General of India, Mukul Rohtagi argued that Indians did not have an absolute right over their body, and that privacy was a vague concept and an elitist concern, a statement also reiterated by India's then finance minister (|Rajagopal, 2015, 2017). In an interview, Nandan Nilekani, the creator of Aadhaar, also stated that privacy and convenience went hand-in-hand, that Indians trade privacy for convenience of using certain technologies (Ghoshal, 2017). Civil society activists countered Rohtagi's statement with the claim that privacy was an essential aspect of an individual's identity regardless of class status (Khera, 2017). Due to these claims over privacy, the SC decided to examine privacy as an independent question. In August 2017, the SC declared privacy to be a fundamental right subject to certain limitations.[25]

On 26 September, 2018, the SC upheld the constitutional validity of mandatory Aadhaar for the provision of government welfare to the poor (Section 7 of the Aadhaar Act) and for filing taxes.[26] The court exempted Aadhaar linkage to mobile phone services, banking and other non-welfare services while observing that it was difficult to undertake mass surveillance on the basis of Aadhaar. The court observed that the Indian state was authorised to mandatorily identify and enrol populations in welfare through Aadhaar because such benefits were funded from the Consolidated Fund of India (p. 564).

The Aadhaar ruling configured privacy differentially for different groups. While enrolment in Aadhaar is still voluntary for all residents, the court stated that Aadhaar 'becomes compulsory for those who seek to receive any subsidy, benefit or service under the welfare scheme of the Government expenditure.' (p. 564). They held that Aadhaar's promise of a unique identity to the individual was 'unparalleled' and it was a 'document of empowerment', particularly for those who are 'illiterate and living in abject poverty without shelter'

(p. 529-30). The court framed their privacy in the language of human dignity, and as a matter of public good to offer socio-economic rights that emphasize 'the role of community in establishing collective goals and restrictions of individual freedoms and rights on behalf of a certain idea of good life.' (p. 538). Eminent economist Jean Dreze (2018) notes that the judgment perpetuates double standards in the way Aadhaar is imposed on the poor and the privileged in that the poor must mandatorily submit biometrics to the state for benefits while the middle-classes were exempted from linking Aadhaar to mobile phones and bank accounts.

The Aadhaar verdict's formulation of the privacy of welfare-dependent groups prioritized dignity of living over individual autonomy pertaining to biometric data ownership. The next section examines the UIDAI's vision and how the formulation of privacy as dignity has unfolded through the lived experience of Aadhaar's excluded welfare beneficiaries.

Aadhaar authentication: anxieties of recognition and privacy interests

The anxieties of recognition brought on by biometric identity verification pertain to the gap between the promise of unique identification and dignified living in the implementation of Aadhaar on the ground. The UIDAI Strategy Overview of April 2010 notes the problem of identity verification of the poor who often lack proper documents in order to avail of the benefits and subsidies. Highlighting the practice of multiple identity documents for multiple benefits as costly, inconvenient and cumbersome, the Strategy Overview envisions a unique identity mechanism based on demographic and biometric information of citizens and residents in order to eliminate fraud and corruption by purging duplicate and ghost entries from identity databases of government services. The UID is presented as a pro-poor identity verification mechanism that would prevent individuals from representing themselves 'differently to different agencies' (UIDAI, 2010, p. 1). Thus, the vision of unique identification mechanism to enable direct access to welfare for the poor is primarily rationalized in terms of their lived realities of socio-economic marginalization, a logic affirmed in the 2018 Aadhaar verdict.

It must be noted that the UIDAI does not certify the documents submitted to issue an Aadhaar card. A right to information request (RTI) filed by Dr. Anupam Saraph – an eminent expert in the governance of complex systems – with the Indian Ministry of Electronics and Information Technology revealed that the UIDAI does not acknowledge, certify or take responsibility for the identification of a person (Saraph, 2018). The agency does not certify identity, address, date of birth and residential status during Aadhaar enrolment. The UIDAI admitted in response that the biometric data of any individual does not pull up a unique record. The Authority simply accepts the enrolment packets sent by the private enrolment agencies for a payment (Kumar, 2018). By replacing uncertified identification documents such as passport, driver's license or voter id with Aadhaar, Dr. Saraph notes that the UIDAI is enabling the addition of fake documents to the system for issue of Aadhaar while undermining the integrity of real and legitimate official documents that are replaced by Aadhaar. The UIDAI's admission under the RTI fundamentally attenuates the entire concept of unique identification, which, from the outset does not distinguish between genuine and possibly forged paper identities used for Aadhaar enrolment.

Despite this foundational vulnerability underlying the notion of unique identification, the larger question remains: How has enrolment in mandatory Aadhaar transformed the lives of welfare-dependent sections? According to the State of Aadhaar report 2017-18, Aadhaar project has enrolled 1.2 billion people of which 87% of rural residents surveyed from three Indian states approved of mandatory linkage of Aadhaar with government services. The survey found that Aadhaar did serve as a tool for financial inclusion through the quick opening of bank accounts for the poor; however, majority (67%) used the analogue version of the Aadhaar letter of enrolment as a means of identification verification. Based on the results from the states of Andhra Pradesh and Rajasthan, the report found greater approval of Aadhaar among respondents who perceived that Aadhaar prevented identity fraud. However, they found the system to be inflexible in disallowing a family member to serve as a proxy in accessing benefits (this was possible under the ration card) when the Aadhaar beneficiary themselves couldn't authenticate in person. A total of 2 million beneficiaries were reported to be excluded monthly across Rajasthan, West Bengal and Andhra Pradesh owing to various factors including those related to Aadhaar-based technical glitches. These facts attest to the broader acceptance of Aadhaar in parts of India. However, the issue of welfare exclusion is equally compelling and significant.

The activist campaign, *Rethink Aadhaar*, has documented instances of exclusion from welfare benefits in rural India – Jharkhand, Rajasthan and Madhya Pradesh – where beneficiaries have struggled to authenticate their identities on various grounds. Three main themes emerged from an analysis of the testimonials that are identified by their number in the playlist sequence on the Rethink Aadhaar website.[27] These are examined below:

1. **Biometric authentication failure/falsification**: Forty-nine of the hundred testimonials analysed pertained to biometric failure or falsification suffered by families, elderly single women who had lost their family, men and women of various ages up to 80. These individuals lived in mud-and-thatch homes in villages where they had been able to get their rations under the old system locally. But now they had to make repeated trips to authenticate only to be turned away because their biometrics would not match. In the video testimonials, some beneficiaries including men and women appeared frail and unwell, and just rubbed their fingers to convey that they could not authenticate, often unable to fully articulate why. Some were hard of hearing and their bodies shook as they spoke. Their rations had been fully or partially denied for anywhere between 2-8 months. For instance, a Muslim woman Hameeda Khatoon, age 75, is shown trying to unsuccessfully authenticate (No. 6). She says in Hindi, 'I don't have a husband or son. My daughter gets rations for me. Do I enjoy doing this!' (colloquial meaning: it's not a dignified thing for women her age to have to do this). As she says this, she is on the verge of tears and tries another finger but it doesn't match. She depends on her daughter who was in school at that time and Hameeda looks helplessly at the interviewer. Madhubabu from East Godavari (Andhra Pradesh) reports that his biometrics are linked to his brother's name so he has to rely on him to get his rations (No. 30), a reality for many that directly questions the Supreme Court's formulation of privacy as dignified living and empowerment through unique identification. Nandudevi, when denied rations, fought with the dealer who threatened her with violence (No. 46). She was defrauded of her rations through falsification of successful authentication attempts which were recorded in the system as ration disbursed. Further reporting that this happened to 85 other families in her village, she said corruption hasn't stopped despite Aadhaar. In the case of Kiran and Revti Dawa from

Nokha village in Rajasthan (No. 66), their repeated authentication attempts were falsified but recorded as ration disbursed while they were told that the online records showed they were marked dead and names struck off. A similar experience is reported by Daakhubai from Kushalpura in Rajasthan (No. 9), a frail old woman with a trailing voice sitting on a cot in a dimly lit room. She says that when her son went to the Bhim district to find out why her pensions had stopped after Aadhaar enrolment, he was informed that she had died (possibly because she could not link her Aadhaar with the pension database). She looks helplessly at the camera as a statistic rolls on the screen with the text: Daakhubai along with 2, 95000 other pensioners have been marked dead and struck off the rolls of Rajasthan's social security pension. From unique identification to being marked dead or erroneously linked records, the implementation of Aadhaar has led to denial of benefits, a direct violation of the Supreme Court's definition of dignity as well their orders for benefits to not be denied for want of Aadhaar.

2. **Compelled physical mobility**: The promise of a dignified living by Aadhaar seeks to improve social mobility of the welfare-dependent groups. However, just to enrol and authenticate on an ongoing basis, they are required to travel long distances from their village to the nearest district (which may be 10 kilometres or further away) under extenuating circumstances including inadequate transportation, absent network connectivity in the village and making a choice between forgoing wages to go to the Aadhaar centre or deprivation. Ashwin, a ration dealer from Panchmahal, Gujarat (No. 24), uses a data card with limited data on his laptop with limited battery to authenticate users in the event of a power cut reports that 1in 10 user authentication fails and this failure is mostly among older individuals and farm workers. Other reasons include errors during Aadhaar enrolment and in order to correct those, the beneficiary has to travel a distance of 45 kilometres to the central office on a weekday, an option that implies loss of wages. Another old woman with wizened features in Alwar, Rajasthan (No. 25) states in a tremulous voice that she has no option but go to the bank to get her pensions. When asked whether she likes going to the bank (at her age), she expresses helplessness and says it's not a question of choice, no one wants to take her so she has to pay part of her pension to a motorbike driver for a ride. Other women squatting around her reveal that sometimes they are forced to walk and their hearts race. The helplessness of old age is also expressed by many others like Kankudevi (No.36) who coughs while speaking and spends Rs. 200 ($2.91) to go to Bhim district bank for her pensions and Vardidevi (No.39) who travels 10 kilometres to the bank because the machine in the village fails to authenticate their fingerprints. Many of these individuals, who are very old, disabled and without means of transport, are required to travel long distances to authenticate themselves or rectify their records. For enrolment and record rectification, some queue up as early as 4 or 5 am with their children because of no childcare (No. 52-55) to beat the rush and forgo daily wages. Similar cases abound as some suggest that their benefits should be disbursed under the pre-Aadhaar system. While they only narrate their woes regarding loss of benefits due to Aadhaar authentication, enrolment and corruption issues, the denial of benefits combined with hardships of compelled physical mobility, especially for those who are illiterate, partially disabled or simply old, demonstrate the cost of trying to become legible to the authorities. Their hopes of better social mobility through dignified living

remains unfulfilled as they are compelled to depend on others who may or may not offer them transportation to reach the enrolment centre.

3. **Exceptional situations**: Tukaram Malawe from Madhya Pradesh (No.86) recounts the case of a pregnant woman in labour who was asked for Aadhaar before admission in the hospital near her village. Her husband had to run home for Aadhaar without which the hospital refused to start delivery preparations while the woman was in labour. The hospital even refused a birth certificate without the Aadhaar of the newly-born. Another man from Delhi outskirts (No. 77) lost his Aadhaar enrolment slip issued in December and another one was issued for a fee but he had to keep visiting the enrolment centre only to be told to go to Central Delhi for further enquiry. In an agonizing tone he says the bank is threatening him with closure of his account if he does not submit Aadhaar. Another lower-class man sits on the floor, waiting outside the enrolment centre to get an Aadhaar for his children who have also accompanied him (No. 78). He visited the day before only to be told to come the next day, which he did at 7 am after leaving home at 4. The school authorities had told him to bring his children's Aadhaar or else keep them at home. His child cries grabbing his arm as he agonises waiting for his turn.

These videos are representative of the hardships of many to access not just their welfare entitlements but also education and health. Threatened with violence, expulsion and ill-treatment, their dignity and autonomy stand severely compromised as their efforts to be legible via Aadhaar to lead a dignified life result in greater anxieties of recognition.

The discussion situates these narratives and the privacy-recognition coupling within the broader debates on biometric technologies and mass surveillance.

Discussion

A recurring caution in the Aadhaar privacy debate, which continues to unfold in India in the context of an impending data protection legal framework[28], highlights mass surveillance of citizens through aggregation of their data as a privacy risk. However, in the case of mandatory Aadhaar, the SC justified a balancing of individual privacy with advancing the larger, collective goal of advancing socio-economic rights/dignity of a vulnerable section of society comprising both above and below poverty line (APL, BPL), the class demographic whose experiences this paper has analysed.

The narratives documented by Rethink Aadhaar provide stark evidence of how, the promise of greater inclusion under Aadhaar as well as the SC's elaboration of privacy as residing in the collective rights of the poor to have a good life and access to basic amenities, is severely compromised in various ways. The cases in which vulnerable women pensioners are unable to link Aadhaar to their pension records due to various hardships are marked dead and struck off the record. In lieu of a dignified living through unique identification, they are simply erased. Others whose demographic information under Aadhaar is inaccurately linked to another record have to find other ways to have their benefit claims validated through the botched mechanisms of biometric recognition. Some who are threatened with violence if they make a fuss have to literally fight for their share of entitlements and lose dignity, an affordance that the UIDAI and the SC consistently maintained, Aadhaar is meant to provide.

These instances substantiate how in many cases, Aadhaar's unique identification for the poor supplants their previous paper identities while disregarding their socio-economic context, access to IT and transport infrastructure and power relations through which Aadhaar is administered on the ground. The anxieties of recognition pertaining to extraordinary hardship to adapt to a new system may also be understood to be a result of what Donna Haraway calls 'corporeal fetishism' – the privileging of biological information as telling the truth of the body over social networks of interrelationships (Magnet, 2011). As such, the body's particularities are omitted and transcoded into an arrangement of static knowledges. The body's lived realities, or a 'heterogenous relationality' are converted into an objective view (Cheney-Lippold, 2017, p. 122) that supersedes those realities.

The deeply problematic implementation of mandatory Aadhaar in many rural parts of India, however, has gone beyond corporeal fetishism in disregarding identity's lived realities of faded fingerprints, lack of infrastructural access and disability. The deliberate falsification of successful authentication by the ration shop dealer while misappropriating their share of grains is yet another iteration of an anxiety around who one is in the eyes of the state when one's recognition as a legitimate beneficiary through biometrics is constantly put under question and attenuated by corrupt practices. These remain unaccounted for despite Aadhaar's objective of eliminating corruption. On the contrary, these practices have been enabled by manipulating Aadhaar authentication.

In the deployment of Aadhaar as a means improving social mobility of the poor, those residing in rural areas that lack network coverage or are not well-connected to the enrolment/authentication centres are compelled to find ways to make the difficult journey. The elderly and disabled without necessary economic means must depend on others' kindness as evidenced in the testimonials. These groups can only hope for better social mobility provided they are physically mobile, a condition that many cannot meet. This dependency on the mercy of others too may be understood as a compromise of dignity and individual autonomy. Compelled physical mobility is exacerbated in non-welfare cases in which mandatory Aadhaar for education and health means children – who cannot give meaningful consent – too must submit their biometrics or suffer the indignity of sitting at home, as narrated by a father waiting to get Aadhaar for his children outside the enrolment centre.

The testimonials analysed above raise a critical question for the Aadhaar privacy debate that has predominantly focused on the important issue of data-based mass surveillance of citizens: What are the legitimate expectations of the mandatorily enrolled Aadhaar beneficiaries for access to their benefits? From the testimonials, it would be reasonable to conclude in the context of their Aadhaar compliance that beneficiaries would expect the demographic and biometric information submitted at enrolment to flow appropriately across networks in the moment of authentication, or to quote Nissenbaum (2010), according to context-relative informational norms that govern the integrity of information flows across networks. They would expect to receive their benefits in a transparent manner as intended by Aadhaar without having to suffer the indignities of threats of violence, falsification of authentication, dependency on others and in some cases being struck off the records entirely, implying a kind of civil death. Already under the welfare-net of surveillance, the privacy expectations of their information contained in Aadhaar link to integrity of recognition i.e., not just a successful biometric authentication but the recognition of their identity as a person with dignity who is entitled to government welfare in their socioeconomic contexts. Many of the beneficiaries in their testimonials complained that the pre-Aadhaar system had worked fine under which they had received their benefits without much hardship. If Aadhaar is purported to be a more efficient, transparent and easier system of identification than the one it has replaced, then it must address the anxieties of recognition that highlight how dignity of living is an integral part of the privacy for those who have no choice but to enrol.

Ursula Rao (2013) in her study of the UID/Aadhaar implementation among urban homeless populations on the margins of New Delhi for enabling their access to banking argues that the implementation of a biometric identity scheme must concern itself with socially relevant constructions of identity. Her study revealed that the UID brought the homeless into the fold of identification through their registration with Homeless Service. When it came to opening a bank account for the homeless, the bank managers were more concerned with social standing, trust and desirability of a relation with potential customers rather than the physical attributes of a UID. What enabled the homeless populations to open a bank account was not the UID but their prior registration with Homeless Service that could vouch for them in the bank. The UID as an identity card did offer them protective recognition shielding them from police harassment.

While Rao's study demonstrates how the vulnerable groups are included, not by UID as a miracle technology, but by the social engagement of specific actors who mediate the relations between state institutions and marginalized populations, the key takeaway from her study for the purposes of this paper is how UID 'can discriminate between compliant and non-compliant bodies on the basis of programmed code, but cannot establish trust … ' (p.75). Or meaningful recognition of identity in its context often demands going beyond the biometric coding of human body based on a universal biology.

The integrity of recognition as emerging from the expectations of Aadhaar-enrolled welfare beneficiaries about their biometric data may also figure as what scholars of development and public policy have termed 'data justice' or the advancement of social justice in a datafied society (Dencik, Hintz, Redden, & Treré, 2019). Data justice in the context of urban development in the Global South may be understood as a 'data assemblage' of 'discourse, institutions, social relations, material resources, etc. within which a data system is embedded' to address data-related outcomes (Heeks & Shekhar, 2019, p. 995). In the Indian context of Aadhaar-enabled beneficiary access to rations through PDS, the data justice framework illustrates the socially embedded nature of technology through a consideration of the beneficiaries' lived realities (Masiero & Das, 2019) – which this paper has framed as anxieties of recognition illuminating dignity as a privacy interest.

It must be acknowledged again that Aadhaar has by and large succeeded in accomplishing its mission leading to the creation of a digital infrastructure for greater financial inclusion according to a World Bank report (Banerjee, 2016). It would be instructive to shift the tenor of the privacy debate from the broader narrative of mass surveillance to understand how integrity of recognition if respected by Aadhaar can afford dignity as a form of privacy to the excluded beneficiaries. When these groups continue to strive to become legible through Aadhaar to the state, it is the integrity of recognition that determines their dignity and not necessarily data-based mass surveillance as the route to undermining privacy.

Notes

1. For a detailed understanding, see https://stateofaadhaar.in
2. Harsh V. Nair. 'Aadhaar hearing: Right to life more important than elite class' privacy concerns, says Centre.' India Today, July 27, 2017. https://www.indiatoday.in/mail-today/story/aadhaar-hearing-privacy-supreme-court-1026499-2017-07-27
3. See, 'Aadhaar is an electronic leash, will hollow out the Constitution: Shyam Divan in Supreme Court, Daily O. 17 January, 2018. https://www.dailyo.in/variety/aadhaar-data-breach-biometric-data-supreme-court-right-to-privacy-shyam-divan/story/1/21799.html
4. Justice K.S. Puttaswamy (Retd.) vs. Union of India. Writ Petition (Civil) No. 494 of 2012 & connected matters, September 26, 2018.
5. See, http://www.egazette.nic.in/WriteReadData/2013/E_29_2013_429.pdf
6. https://www.lopol.org/article/nfsa-ration-card-categories-antyodaya-aay-priority-phh-non-priority-nphh-state-priority
7. https://www.supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf
8. Aadhaar has been the subject of numerous data breaches and security concerns over the past decade. See, Aadhaar Leaks: A continuously updated list of all Aadhaar data leaks. https://www.medianama.com/2018/05/223-aadhaar-leaks-list/ Medianama, May 4, 2018.
9. See, Megha Mandavia & Nilesh Christopher. 'Aadhaar ID provides dignity to marginalized.' The Economic Times, September 27, 2018. https://economictimes.indiatimes.com/news/politics-and-nation/aadhaar-id-provides-dignity-to-marginalised/articleshow/65973695.cms
10. https://rethinkaadhaar.in/about
11. See, http://sm4e.org/communication-advocacy-development-activism/
12. See, https://rethinkaadhaar.in/testimonials?offset=1497094768640
13. For a detailed history of Aadhaar, see Seetha (2015, July 29). There is a Privacy Issue with the Aadhaar Card. *Swarajya*. Retrieved from https://swarajyamag.com/politics/there-is-a-privacy-issue-with-the-aadhar-card
14. For a deeper understanding of Aadhaar, see, 'What is Aadhaar?: Know all about Aadhaar Bill 2016 in 11 slides. https://www.financialexpress.com/photos/budget-gallery/223860/what-is-aadhaar-bill-all-you-want-to-know-in-5-points/ Also see, https://uidai.gov.in.
15. See, '10 Reasons why Aadhaar has now Become the very Basis of Your Life.' The Economic Times, Oct 21, 2017.https://economictimes.indiatimes.com/news/economy/policy/10-reasons-why-aadhaar-has-now-become-the-very-basis-of-your-life/articleshow/61160289.cms
16. Rajagopal, Krishnadas (2016). Don't Insist on Aadhaar, Warns SC. The Hindu, Sept 6, 2016. https://www.thehindu.com/news/national/aadhaar-not-mandatory-sc-reiterates/article6999924.ece
17. The PDS is an Indian network of fair price shops that distribute food grains and cooking oil to the poor.
18. See, UIDAI Press Note. As per Aadhaar Act, No Denial of Benefits for Want of Aadhaar: UIDAI. February 10, 2018. https://uidai.gov.in//images/news/press_note_on_no_denials_100218.pdf
19. A money bill concerns matters of borrowing and lending of money, tax laws and prevention of black money in India.
20. For a detailed account of these developments, see, Varun H.K. (2018). SC's Aadhaar verdict: Privacy vs identity. Deccan Herald. https://www.deccanherald.com/national/aadhaar-act-verdict-history-693614.html
21. See, 'Aadhaar as money bill: SC to hear Jairam Ramesh's plea challenging speaker's decision in November.' *Livemint*, September 1, 2017. https://www.livemint.com/Politics/ezr9RyS3cHMAIZVhBOr3gJ/Aadhaar-as-money-bill-SC-to-hear-Jairam-Rameshs-plea-chall.html
22. See, https://cis-india.org/internet-governance/news/india-today-may-4-2017-aadhaar-data-of-130-millions-bank-account-details-leaked-from-govt-websites-report

23. See *Firstpost*, Aadhaar Security Breaches: Here are the Major Untoward Incidents that have Happened with Aadhaar and what was Actually Affected.
24. See, Aadhaar data leak: Details of 7.82 Cr Indians from AP and Telangana found on IT Grids' database. FirstPost, April 17, 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
25. *Justice K.S. Puttaswamy (Retd.) and Another vs. Union of India and Others*. Writ Petition (Civil) No. 494 of 2012.
26. See, note vii.
27. See, note xv.
28. Neha Alawadhi (July 4, 2019). Lok Sabha passes Aadhaar bill amid opposition protest over privacy. Business Standard, Retrieved from https://www.business-standard.com/article/current-affairs/lok-sabha-passes-aadhaar-bill-amid-opposition-protest-over-privacy-119070401237_1.html

Disclosure statement

No potential conflict of interest was reported by the author.

Notes on contributor

Pawan Singh is a New Generation Network Scholar (NGN) in contemporary histories at Deakin University and the Australia India Institute from 2016-2019. He attained a doctorate in Communication from the University of California San Diego. His work, which has been funded by the Toyota Foundation's grant "Exploring New Values for Society" and the Digital Identity Research Initiative of the Indian School of Business, Hyderabad, examines the interplay of identity, privacy, representations and media technologies in relation to universal notions of social justice and empowerment.

References

Ajana, B. (2013). *Governing through biometrics: The biopolitics of identity*. New York: Palgrave Macmillan.

Banerjee, S. (2016). Aadhaar: Digital inclusion and public services in India. World Development Report. Retrieved from http://pubdocs.worldbank.org/en/655801461250682317/WDR16-BP-Aadhaar-Paper-Banerjee.pdf

Bhuyan, A. (2018, January 18). Aadhaar isn't just about privacy. There are 30 challenges the govt. is facing in the Supreme Court. *The Wire*. Retrieved from https://thewire.in/government/aadhaar-privacy-government-supreme-court

Byatnal, A. (2010, September 29). Tembhli becomes first Aadhaar village in India. *The Hindu*. Retrieved from https://www.thehindu.com/news/national/Tembhli-becomes-first-Aadhar-village-in-India/article13673162.ece

Calo, R. (2011). The boundaries of privacy harm. *Indiana Law Journal*, *86*(3), 1131–1162.

Cheney-Lippold, J. (2017). *We are data: Algorithms and the making of our digital selves*. New York: NYU Press.

Cohen, J. (2013). What privacy is for? *Harvard Law Review*, *126*(7), 1904–1933.

Dencik, L., Hintz, A., Redden, J., & Treré, E. (2019). Exploring data justice: Conceptions, applications and directions. *Information, Communication & Society*, *22*(7), 873–881.

Dreze, J. (2018, October 2). Ill fares Aadhaar. *The Indian Express*. Retrieved from https://indianexpress.com/article/opinion/columns/privacy-surveillance-pan-card-ill-fares-aadhaar-link-5381698/

Ghoshal, D. (2017, April 15). Interview: Aadhaar is being demonized because it's so transparent, says Nandan Nilekani. *Quartz*. Retrieved from https://scroll.in/article/834524/interview-aadhaar-is-being-demonised-because-its-so-transparent-says-nandan-nilekani

Greenleaf, G. (2010). India's national ID system: Danger grows in a privacy vacuum. *Computer Law & Security Review*, *26*, 479–491.

Heeks, R., & Shekhar, S. (2019). Datafication, development and marginalised urban communities: An applied data justice framework. *Information, Communication & Society*, *22*(7), 992–1011.

H.K., V. (2018, September 20). SC's Aadhaar verdict: Privacy vs identity. *Deccan Herald*. Retrieved from https://www.deccanherald.com/national/aadhaar-act-verdict-history-693614.html

Khera, R. (2017, November 13). Why ABBA must go: On Aadhaar. *The Hindu*. Retrieved from http://www.thehindu.com/opinion/lead/why-abba-must-go/article20353913.ece

Kumar, N. (2018, February 10). Aadhaar does not maintain unique records: UIDAI. *Sunday Guardian Live*. Retrieved from https://www.sundayguardianlive.com/news/12742-aadhar-does-not-maintain-unique-records-uidai

Magnet, S. (2011). *When biometrics fail: Gender, race, and the technology of identity*. Durham: Duke University Press.

Masiero, S., & Das, S. (2019). Datafying anti-poverty programmes: Implications for data justice. *Information, Communication & Society*, *22*(7), 916–933.

Monahan, T. (2010). Surveillance as governance: Social inequality and the pursuit of democratic surveillance. In K. D. Haggerty & M. Samatas (Eds.), *Surveillance and Democracy* (pp. 91–110). New York: Routledge.

Mordini, E., & Massari, S. (2008). Body, biometrics and identity. *Bioethics*, *22*(9), 488–498.

Nilekani, N., & Shah, V. (2016). *Rebooting India: Realizing a billion aspirations*. New Delhi: Penguin.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy and the integrity of social life*. Stanford: Stanford University Press.

Rajagopal, K. (2015, July 23). Privacy not a right, Aadhaar legit: Centre. *The Hindu*. Retrieved from http://www.thehindu.com/news/national/privacy-not-a-right-aadhaar-legit-centre/article7452839.ece

Rajagopal, K. (2017, June 9). Centre's affidavit in Supreme Court: 'welfare of masses trumps privacy of elite'. *The Hindu*. Retrieved from https://www.thehindu.com/news/national/centres-aadhaar-affidavit-in-supreme-court-welfare-of-masses-trumps-privacy-of-elite/article18951798.ece

Ramanathan, U. (2017, May 16). Coercion and silence are integral parts of the Aadhaar project. *The Wire*. Retrieved from https://thewire.in/136102/coercion-aadhaar-project-ushar/

Rao, U. (2013). Biometric marginality: UID and the shaping of homeless identities in the city. *Economic & Political Weekly*, *XLVIII*(13), 71–77.

Saraph, A. (2018, August 25). UIDAI has no skin in the system. *Sunday Guardian Live*. Retrieved from https://www.sundayguardianlive.com/news/uidai-no-skin-system

Solove, D. (2004). *The digital person: Technology and privacy in the information age*. New York: NYU Press.

Solove, D., & Citron, D. (2017). Risk and anxiety: A theory of data breach harms. *Texas Law Review*, *96*(737), 1–38.

Turow, J., & Ribak, R. (2003). Internet power and social context: A globalization approach to web privacy concerns. *Journal of Broadcasting & Electronic Media*, *47*(3), 328–349.

Unique Identification Authority of India (UIDAI) Planning Commission, Govt. of India. (2010, April). UIDAI Strategy Overview. Retrieved from http://www.thehinducentre.com/the-arena/current-issues/article10034082.ece

Yadav, V. (2014). Unique identification project for 1.2 billion people in India: Can it fill institutional voids and enable 'inclusive' innovation? *Contemporary Readings in Law and Social Justice*, *6*(1), 38–48.

Zuboff, S. (2019). *The Age of surveillance capitalism: The fight for a human future at the frontier of power*. New York: Public Affairs.