Surveillance in the Name of Governance: Aadhaar as a Fix for Leaking Systems in India

Kathryn Henne

As other chapters in this book attest, knowledge is often central to the mobilisation of structural power. In focusing on knowledge, it is important to consider *what* and *who* can exercise such power and *how*. Structural power, according to Susan Strange (1998), sits with actors who can influence and exert control over people's livelihoods and security, including the modes of accessing essential services. Here, I examine how two key features of structural power—that is, knowledge and authority—coalesce in the context of social assistance provision. State-supported welfare systems hinge on the collection of significant amounts of personal information, using data to monitor beneficiaries' behaviour and to assess their compliance with the conditions of receiving assistance (Eubanks 2018). Accordingly, they rely on a wide range of technologies and techniques to manage and administer benefits and payments. In short, it depends on surveillance—that is, “the focused, systematic, and routine attention to

K. Henne (✉)

University of Waterloo and Balsillie School of International Affairs,
Waterloo, ON, Canada

Australian National University, Canberra, ACT, Australia
e-mail: khenne@uwaterloo.ca

© The Author(s) 2019

B. Haggart et al. (eds.), *Information, Technology and Control
in a Changing World*, International Political Economy Series,
https://doi.org/10.1007/978-3-030-14540-8_11

223

personal details for purposes of influence, management, protection or direction” (Lyon 2007, 14). Social assistance offers a domain of governance where we can observe, document, and trace both striking and mundane aspects of leveraging knowledge in the exercise of structural power. In this context, governance relies on knowledge about subjects, but it is not complete knowledge of their lived conditions; rather, governance here relies on isolated forms of data that can be extracted through biometric technologies. As this chapter illustrates, surveillance becomes a key mode through which authorities come to know subjects, shaping how they are treated.

While the targeted surveillance of marginalised populations is not new (see Gilliom 2001), the proliferation of monitoring techniques and verification mechanisms in the context of welfare provision has received greater attention in recent years. A number of countries have expanded—and are continuing to expand—their practices of tracking and authenticating social assistance recipients, using a range of technologies to do so. For example, in the United States, mechanisms for discerning welfare recipients’ bought goods, tracking their employment opportunities, and sharing data across administrative agencies are commonplace, as are risk-analysis and predictive tools for assessing their current and future circumstances. The Australian government has proposed expanding trials for welfare card programmes to limit individual purchases and has sought to mandate drug testing as a condition of social assistance. South Africa has added biometric authentication to its social benefits cards, 19 million of which have been supplied to welfare recipients since 2012, with a range of countries—including Ireland, Trinidad and Tobago, and the Philippines—following suit. The Unique Identification Authority of India (UIDAI), established in 2010, has issued over one billion unique identifier numbers (or “Aadhaar”) for use across several government assistance programmes. Although distinct jurisdictions, authorities evoke similar justifications, such as fraud prevention and cost savings, for introducing new monitoring and authentication technologies in the context of social assistance. In doing so, the disproportionate surveillance of citizens who are often poor, vulnerable, and sometimes multiply marginalised becomes enabled through narratives of transparency, accountability, and good governance.

Developments in social assistance, I argue, demonstrate Zeynep Tufekci’s claim that the engineering of social life is “a political process involving questions of power, transparency, and surveillance” (2014, 1). To illustrate how socio-technical entanglements emerge in the form of surveillance and convey structural power, this chapter focuses on the making and maintenance of data-intensive infrastructure to support state social

assistance systems, using India as its central case. Its analysis of Aadhaar examines how surveillance enabled through unique identification numbers constitutes a distinct mode of governance, one that depends on the pursuit of particular kinds of knowledge. After doing so, I consider how these practices evince broader shifts in which state actors, as well as non-state actors working in the service of state interests, create and sustain the conditions for regulating subjects.

Although its focus is on India, the chapter illuminates potential issues with and limitations of these hybridised formations of governance more generally. Hybridity, at least in relation to law and regulation, typically refers to “synergies between binding and non-binding mechanisms” that support governance functions (Trubek and Trubek 2005, 344). In this case, UIDAI is part of an amalgamated machinery that is supposed to streamline service delivery through data collection and verification; however, as elaborated upon in later sections of this chapter, India’s biometric management system has had notable failings. As a networked assemblage, it has the capacity to short-circuit. I use “assemblage” here to flag that although Aadhaar can be thought of as infrastructure, it is actually constituted as a “multiplicity of heterogeneous objects, whose unity comes solely from the fact that these items function together, that they work together as a functional entity” (Patton 1994, 158). Assemblages can materialise through events, but they are not fixed or stable; they can fluctuate along different registers that cross time and space. Thus, in addition to concerns of technocratic utility, the scrutiny of Aadhaar offers a space in which we can glean insight into how nationalist agendas and inequalities inform the terms and conditions of biometric surveillance systems and how they materialise in citizens’ lives in differential ways.

In particular, this chapter discusses how UIDAI’s one-way expectation of transparency, which is aimed at recipients of social assistance, illustrates how knowledge and authority coalesce in the contemporary expression of structural power. It shares Strange’s appreciation of granular analyses, as Germain elaborated earlier in this book, as a necessary mode of interrogating the details of a concern in order to understand its material effects. Here, I consider some of the intricacies through which power is being fashioned while retaining critical focus on the “big picture” as Strange would. However, and distinct from Strange, I do so in a way that accounts for entanglements of technologies, bodies, and social categories of difference, which are reflective of interlocking systems of inequality and oppression that are part of the Indian state. The argument put forth here departs

from traditional Strangean analyses found in International Political Economy. Unlike Strangean analyses' tendency to overlook questions of gendered inequality, I embrace feminist calls to look at how "surveillance is integral to many of our foundational structural systems, ones that breed disenfranchisement, and that continue to be institutionalized" and to critically attend to how "underlying structures of domination" inform surveillance activities (Dubrofsky and Magnet 2015, 7). This chapter therefore attends to a wider range of structural formations of difference, including race and racism as well as gender and sexuality, as it examines the exercise of state power.

The remainder of the chapter proceeds in four parts. The first section discusses the longer trajectory of states using knowledge about its residents as a central method of governing populations within its jurisdiction. A reflection on specific contours and features of India's national identification initiative follows. The next section considers the specifics of Aadhaar in relation to insights gleaned through the literatures on surveillance, transparency, and governance, explaining specific contributions from the Indian example. I conclude by contemplating this case study's implications for how we think of knowledge, particularly its role in the growing range of practices that can be understood as *biogovernance*, which generally speaking, is the governance of populations and individual humans through science and technology.

1 HOW STATES COME TO KNOW AND GOVERN CITIZENS

Nation-states have longstanding practices of identifying, monitoring, and sorting their residents, employing various mechanisms to do so. Their strategies have involved individual identification and authentication techniques, such as biometric-based technologies, as well as population-based approaches. For example, reflecting on the United States, David Theo Goldberg (1997, 33) explains that "the national census is as old as the republic itself" and that delineating different groups within the population is central to governing apparatuses, particularly "the distribution of federal resources." Goldberg (1997) emphasises that while these practices are often framed as being for the benefit of the nation, they often reaffirm difference, particularly racial difference, among subjects. Simone Browne (2015) elaborates upon this observation in relation to historical and contemporary modes of surveillance. Specifically, she states, surveillance operates as a "technology of social control" that "exercise[s] a 'power to define

what is in or out of place” (Browne 2015, 16). In other words, population governance through surveillance can be thought of as an articulation of structural power, one that can reproduce and perpetuate inequalities. On the surface, this foundational form of biogovernance may appear objective and apolitical; however, upon further reflection, it demonstrates the shaping of the agendas and institutional terms through which states, peoples, and other actors can relate to each other. It ultimately reflects the ability to “decide how things shall be done” (Strange 1998, 24–25).

The expansion of national identification systems offers an opportunity to further explore the tensions that emerge in the push to collect and analyse data about individual members of the population. Today, many states maintain elaborate identification systems to track and distinguish citizens and non-citizens, with widely accepted documents, such as passports, serving as longstanding tools of authentication (Torpey 2009). To buttress these systems, many jurisdictions have embarked on “modernising” them by including practices of biometric authentication (Lyon 2013), which use data collected to document a person’s unique physiological characteristics—most commonly, fingerprints, facial features, irises, and retinal veins—to verify identity. The enthusiasm for new national systems of biometric identification across jurisdictions, according to David Lyon (2013), has enabled new approaches to population management, many of which rely on unprecedented levels of digitised data generation. Part of a broader post-9/11 trend in which governments are expanding the biometric verification of both foreign- and native-born residents (Gates 2011), this shift has led to greater private, corporate, and non-state involvement in the creation and sharing of information about individuals. In doing so, writes Btihaj Ajana (2010, 237), “bio-digital samples” of human beings have become the basis for evaluating subjects, their identities, and their relationship to the state. The enhancement of identification systems may promise more stable modes of population management through claims of accuracy and objectivity; however, they come with risks that are especially relevant to groups who occupy marginalised social positions—even though such risks are not always evident in everyday life. With the expansion of surveillance, we need to cultivate a “critical biometric consciousness” that is attentive to the unintended effects of these technologies (Browne 2010, 132). This issue is particularly important as such technologies posit truth-claims about bodies and identities in ways that may direct attention away from larger issues of inequality.

Concerns of inequality are especially relevant to the surveillance of social assistance recipients and arguably the poor more generally. Many people who receive welfare are subject to multiple regulatory systems that collect and triangulate data on their individual needs, consumption patterns, access to resources, and compliance with the rules and conditions of receiving social assistance benefits. These arrangements, according to Torin Monahan (2017, 193), can “regulate the practices and subjectivities of the various ‘clients’ they serve,” often making moral assessments that can underscore “the stigma of being on welfare” and “suspicion of deficiencies with one’s character.” With the collection and tabulation of data, suspicion can become embedded in ways that can have problematic outcomes for those who are subject to multiple forms of surveillance. For example, Virginia Eubanks (2018) has documented how governments’ embrace of automated systems can result in judgments based on errors in data collection and analysis, with life-threatening implications for those who are dependent upon social services. Social assistance recipients in particular are entangled within the fabric of these networked schemes, which Eubanks (2018, 175–190) describes as constituting a “digital poorhouse” that is woven together by fibre-optic strands. By this, she means the surveillance of those most in need of services prompts the threads to wrap more closely—and potentially more tightly—around them. Just as importantly, while individual circumstances may change or there may be errors in the data collected, the data do not necessarily change or disappear accordingly. The imprint may remain hardwired in the network. Representations of social assistance recipients can render them hypervisible to authorities, especially compared to other citizens who do not have their data harvested and cross-checked by other surveillance systems on a regular basis. It therefore increases the likelihood of losing support for noncompliance or becoming subject to other forms of state control.

Browne (2015), Monahan (2017), and Eubanks (2018), like many other scholars of surveillance (e.g., Magnet 2011; Staples 2014; Guzik 2017), stress the potentially dangerous consequences of data-driven population governance, emphasising how their reliance on monitoring individuals often perpetuates structural inequalities. In contrast, advocates for Aadhaar, the unique identification number (UID) for residents of India, argue the opposite point: that the tracking and verifying of residents can help to counteract and alleviate persistent inequalities by ensuring they receive essential services. Specifically, the introduction of Aadhaar responds to failures in social assistance delivery and allegations of identity fraud. The programme assigns

a 12-digital UID to collect demographic and biometric data, including iris scans, facial pictures, and fingerprints, which can be linked to access services, such as food rations, subsidies, pensions, and other financial services. International observers have praised the programme's sophistication, attributing Aadhaar with making "it simpler and more secure for poor people to do business with banks" (Bill and Melinda Gates Foundation 2017) and for supporting cost savings of up to US\$11 billion per year (World Bank 2016, 195). In fact, experts, such as Paul Romer, a former World Bank Chief Economist, have promoted it as a model for other countries to adopt (Doshi 2018). With widespread support and seemingly evident need, does Aadhaar—a programme introduced in a country where some speculate that only half of births are registered—overcome the critiques that scholars have levied at data-driven governance? The next section of this chapter outlines some of the purported strengths and limitations of Aadhaar by considering its establishment, its expansion, and its technocratic malfunctions.

2 THE ASPIRATIONS AND SHORTFALLS OF NATIONAL IDENTIFICATION SYSTEMS IN INDIA

When the Congress Party-led government launched Aadhaar in 2009, it promoted biometric identification, verification, and authentication as a voluntary option, one that would benefit those seeking welfare benefits and food subsidies. Previously, the other major party, the Bharatiya Janata Party (BJP), had criticised the programme when it was in opposition. Since coming to power after the 2014 election, the BJP has actually expanded Aadhaar and its use. In fact, verifiable UIDs became a requirement for accessing various public services and for conducting many private financial transactions. Authorised under the *Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016* ("Aadhaar Act 2016"), UIDAI, the statutory authority tasked with the programme's oversight, has a mandate to issue UIDs to all residents of India; to eliminate duplicate, false, or otherwise inaccurate forms of identification; and to ensure that cost-effective and user-friendly modes of authentication are in place (Government of India 2016). An ambitious project, Aadhaar covers 1.12 billion people, nearly 99 per cent of the adult population in India (Digital Dawn 2017), making it the largest biometric identification programme in the world. It is also a visible, and arguably foundational, component of the Indian government's "Digital India" initiative to

enhance the nation's online infrastructure and to expand internet access across the country. To understand how Aadhaar is an expression of structural power therefore requires considering its place within and alongside state agendas.

2.1 *Establishing a National Identification Authority in India*

Recognising that a large number of people in need of services were either not registered at birth or lacked basic identity documents, the Indian government opted for a biometric system to establish verifiable identities. The programme was meant to be a comprehensive response to a widespread problem often referred to as “leakage,” meaning that funds did not reach the correct beneficiaries, with some being taken by someone acting on their behalf (Singh 2017). In fact, one estimate suggested that only 27 per cent of funding went to the correct recipients. The incentive for individuals to enrol in Aadhaar was the promise that it would ensure the streamlined and guaranteed delivery of welfare provisions while also removing fraudulent information and go-betweens who may take a cut of funds intended for the recipient. Critics of Aadhaar, including noted Hindu nationalist Narendra Modi before he became prime minister in 2014, characterised it as a “political gimmick” at worst (Narendramodi 2014) and too expensive to be practical at best (Singh 2017). Despite these challenges, the programme proceeded with Nandan Nilekani, an entrepreneur who co-founded and co-chaired Infosys Technologies, as the chairman of UIDAI.

The choice of Nilekani to lead the UIDAI is interesting, but not necessarily surprising. In his 2009 book, *Imagining India*, Nilekani discusses the benefits of UIDs, characterising them as a foundational reminder of citizens’ “rights, entitlements, and duties” and the state’s obligations to provide them. He also frames them as the potential way to enable more Indians to open bank accounts and participate in more economic activities. His presentation of UIDs is a direct response to earlier government ideas that promoted an identification programme in the interests of border security.

The development of Aadhaar—which means “foundation” in Hindi—embraced Nilekani’s more liberal envisioning, which became reflected in its branding: a fingerprint logo in the shape of the sun. Distinct from other welfare-delivery programmes, it did not advance overt or “new paternalist” platforms observed elsewhere (e.g., Australia, the United States), which often use surveillance to monitor and enforce conditions on social assis-

tance recipients under the guise of encouraging more responsible behaviours among them (see Dee 2013). In contrast, Aadhaar was not so much about monitoring or scrutinising the actions of the poor, but instead, ensuring the validation of identities so that all Indians could receive their allotted entitlements. Those allowances were—and still are—far from generous, though, as India only spends 1.7 per cent of its GDP on social support, which is much lower than its lower-middle income neighbouring countries (3.4 per cent) and China (5.4 per cent) (Drèze 2014).

Aadhaar, as a large-scale digital infrastructure project, required both technical and political labour. With the establishment of the agency in Delhi and the technological branch in Bangalore, Nilekani's team included bureaucrats as well as engineers with experience working in Silicon Valley and for major multinational technology companies, such as Google and Intel (Parker 2011). In order to verify biometric information, the design of the system relies on the ability to millions of comparative alignments, which requires the use of algorithmic assessment enabled through partnerships with Accenture, LI, and Morpho (*ibid.*). At its core, Aadhaar is a hybrid. Even though it is led by UIDAI, a state authority promoting state interests, it draws heavily from private-sector expertise and tools.

2.2 *Implementing and Expanding Aadhaar*

The rollout of the national identification scheme was a notable success in terms of its reach, with authorities registering participants at a rate much faster than anticipated in initial targets (Sathe 2014). The issuing of the first Aadhaar number in September 2010 to a woman living in rural Maharashtra received much publicity, even though she later reportedly stated that her UID had little value if the provisions it ensured were not enough to end one's hunger (Parker 2011). By mid-2013, the government had issued UIDs to 350 million people and established 500 operational service centres, with plans for doubling the number of centres nationwide before the year's end (Kumar 2013). By March 2014, the average authentication rate was 300,000 identities per day (Sathe 2014). Additionally, authorities expanded verification through mobile-based password services and business authorisation services (*ibid.*). There were, however, stated concerns about whether Aadhaar would actually undermine the Public Distribution System (PDS), which provides subsidised goods to the poor. As the biometric system requires delivering money into bank accounts rather than providing foodstuffs directly, it placed new demands on banks that had

previously not had to service a wide range of customers, and many recipients had to start paying market prices (Parker 2011). In hindsight, these shifts in service provision were only the beginning of the changes enabled by Aadhaar.

Although designed to support social assistance delivery, the use of Aadhaar has expanded significantly in recent years. By early 2017, the BJP-led government had mandated its use for various programmes and schemes, including for tax compliance, bank account usage, educational scholarship awards, public Wi-Fi access, pension payments, and maternity benefits (Ghoshal 2017). Prime Minister Modi, previously a vocal opponent of the UID system, has shifted his stance to actively promote efforts to make Aadhaar mandatory for accessing most government services. In fact, Aadhaar has emerged as a foundational component of the BJP's governance plans, which include the wider digitisation of services, particularly through its suite of software applications, which are bundled as together as India Stack, a digital application project interface intended, according to its website, to enable "governments, businesses, startups and developers to utilise an unique digital infrastructure to solve India's hard problems towards presence-less, paperless, and cashless service delivery" (India Stack 2018).

With the stated aim of bringing more Indians into the formal economy, India Stack is supposed to remove barriers and "friction" they may face in terms of access. It entails four layers, the first of which is the "presenceless layer," which is facilitated through the achievement of a "universal biometric digital identity" enabled by Aadhaar, the foundation that would enable verification of anyone so that they can access a service from any location in the country (India Stack 2018). The second layer is "paperless," which is intended to remove challenges associated with the storage and reliance on physical paper for documentation and verification, while the third layer is "cashless," a measure to broaden access to bank accounts—a move framed as "democratizing payments" (ibid.). The fourth layer, "consent," is to ensure to the free and secure movement of data, including personal biometric information and other relevant linked information.

Critics have described Aadhaar, particularly its role within the wider digital architecture, as the foundation of a surveillance state (e.g., Ganesh 2018; Khera 2018). They have been quick to cite research indicating that Aadhaar has not fixed problems of social assistance delivery; rather, in some areas, it has exacerbated food insecurity (see Khera 2018). In contrast, within two years of implementation, government reports indicate a

cost savings of US\$8 billion, which reportedly far surpass the US\$1 billion cost of Aadhaar (Digital Dawn 2017). Regardless of outcomes, it is clear that the use of UIDs now extends well beyond their originally stated purpose. This development fits scholarly assertions that surveillance measures targeting the poor are often the precursor for future practices targeting the public more generally (Eubanks 2018).

As Aadhaar becomes linked to more databases through the delivery of public services, the completion of private transactions, and increased digital interconnectivity, the likelihood of other entities accessing identifying information too increases. The 2016 *Aadhaar Act* permits this practice, as a “requesting entity” (any “agency or person” willing to pay the required fee) can ask for demographic information related to one’s identity as long as it is not the actual biometric data collected (UIDAI 2016). Given the embeddedness of Aadhaar, few Indians can refrain from using it—certainly not the poor who need access to essential services and rations.

Although many residents must use Aadhaar, it does not mean doing so is always easy. As Reetika Khera (2018) observes, the fact that one has to have a UID and ensure that it was linked correctly to different accounts can be an obstacle when trying to obtain social assistance. There are multiple reports of services being denied, including food, medical services, and education, because the intended recipient cannot authenticate their identity, which can be the result of administrative errors, failed biometric verification, inconsistent internet connections, or simply an individual’s inability to link accounts. Khera (2018), for instance, recounts the death of an 11-year-old girl after being removed from the subsidies registrar due to the government’s failure to link her Aadhaar to her ration card. Others cite the case of the man who was able to get an Aadhaar for his dog (e.g., Dixit 2017a). Further, older and disabled populations can no longer rely on someone else to obtain their rations, since verification now requires their physical presence.

There are also positive stories associated with the expanded use of UIDs, such as reports that poor residents felt that Aadhaar had an equalising influence: since more affluent residents had to sign up on their own (as servants cannot complete the enrolment process for them), they were forced to do so alongside Indians of different backgrounds and social status (see Sathe 2014, 86). In a country that still has rigid social divisions, some of which are solidified through caste, the notion that all residents would have Aadhaar and that it would be a means for giving the poor greater access to financial institutions had symbolic meaning for some. It

offered a seemingly more “open” approach to a historically closed society (ibid.). Further, more residents can have bank accounts and thus access income through direct and confirmable deposits. Regardless, while some reports emphasise these benefits alongside claims of cost savings and successful anti-corruption reforms, Aadhaar has come with unforeseen and undesirable trade-offs, which the next section describes.

2.3 *Short-Circuits in the National Identification Infrastructure*

The widespread implementation of UIDs has faced both legal and technical obstacles. On three separate occasions between 2013 and 2015, the Supreme Court of India reaffirmed that Aadhaar was to remain a voluntary programme (Ghoshal 2017). Thus, the ruling countered the BJP-led government’s efforts to mandate UID verification for many services. Unfortunately, though, it followed the widespread practice of doing so. More recently, in August 2017, a ruling by the Supreme Court took a stronger stance relevant to Aadhaar: it asserted for the first time that privacy is “an intrinsic part of Article 21 that protects life and liberty.”¹ In doing so, the Court overturned two previous rulings that aligned with government assertions that privacy is not a fundamental right—and thus not a relevant concern for the current or expanded use of Aadhaar. In contrast, the recent decision, which was a unanimous ruling by a nine-judge panel, framed privacy as an expansive protection that applies to one’s home life and domestic relationships, sexual orientation, and bodily integrity (Guruswamy 2017). It not only may have bearing on the 30 ongoing challenges specific to Aadhaar, but it also enshrines a legal right that may provide a defence against other government actions, now and in the future, given the current political climate in India. The BJP, which has been in power since 2014, has sought to regulate—and arguably control—various intimate and embodied practices related to gender and sexuality, marriage, religion, and food (ibid.). While the full implications of this ruling are not yet realised, it paves the way for various constitutional challenges, including the successful overturning of Section 377 of the Indian Penal Code in 2018, which decriminalised homosexuality across India, and prohibitions on alcohol and beef consumption in some parts of the country.

¹ *Justice K. S. Puttaswamy (Retd.) and Anr. vs Union of India and Ors* (2017) 10 SCC 1. Specifically, it holds that the right to privacy is protected under Articles 14, 19, and 21 of the Constitutions.

Beyond legal contestations around Aadhaar, technical issues have given rise to other concerns, with more recent developments fuelling worries about access, privacy, and the security of personal data. For example, in terms of access, when it became mandatory for Aadhaar to be linked with PAN (the Permanent Account Number given to each taxpayer in India), complications emerged for citizens who do not fit in binary gender categories. Whereas Aadhaar captured transgender identities, the PAN application form only allowed for “male” and “female” options (Sharma 2018). As such, an entire group of citizens²—those whose have registered their identity as transgender with Aadhaar—could not comply with the new requirement. Additionally, in 2017, researchers discovered a website that contained the UIDs and demographic information of more than 500,000 minors enrolled in Aadhaar (Dixit 2017a). In the same year, reports revealed that more than 200 government websites shared personal details about millions of citizens, some of which was accessible through a basic internet search (Goel 2018). In response to these unauthorised disclosures, sceptics drew attention to a critical point about the *Aadhaar Act* (2016): that it enables levying sanctions for “illegal access” but does not contain adequate provisions for preventing breaches (Dixit 2018). The leaking of data thus drew attention to fundamental flaws in a system that was presented to the public as foolproof.

Security problems persisted into 2018. An investigative report by journalist Rachna Khaira, published in the Indian newspaper, *The Tribune*, documented how she was able to access personal information collected by UIDAI through an agent for merely Rs 500 (approximately US\$8) (Khaira 2018). Government representatives denied claims that Aadhaar data was not protected or secure, with the BJP initially characterising the report as “fake news” and UIDAI officials stating her actions were “illegal” and a “major national security breach” (Dixit 2018). Further, the UIDAI’s deputy director filed a criminal complaint that implicated Khaira and the newspaper, asserting offences that included forgery and cheating (Safi 2018). The move attracted notable criticism from onlookers who framed it as an attack on independent journalism and freedom of the press, claims to which officials later responded, stating that UIDAI named multiple parties in the complaint, which primarily targeted the unidentified actors who purportedly accessed and sold the data (ibid.).

² According to the 2011 Census, 488,000 Indians are transgender.

Authorities such as Ajay Panday, Nilekani's successor as head of UIDAI, have framed system breaches as "inevitable" problems that the agency can fix, while others have reduced their reliance on Aadhaar. For instance, in Delhi, the government has removed Aadhaar as a requirement for food rations (Goel 2018). Irrespective of these responses, the accessibility of private data seemingly confirms privacy advocates' fears. Moreover, they have been exacerbated as companies reportedly planned to follow Microsoft's lead by implementing plans to access demographic information through Aadhaar as part of the conditions of their service provision (Dixit 2017b). These developments have prompted speculation over the nature of Aadhaar's future, even though the national government has yet to step back from plans for its intended expansion of the programme. However, a September 2018 ruling by the Indian Supreme Court³ suggests that Aadhaar may be here to stay, but likely with some qualifications and possible limits: upholding the constitutionality of the *Aadhaar Act*, including the requirement of a UID as a condition for receiving public benefits and filing taxes, the Court did put limits on how private companies use Aadhaar by striking down Section 57 of the *Act*.

In practice, the 2018 Supreme Court decision means services, such as mobile phone service or banking, cannot be denied on grounds that a customer does not provide a UID, nor can companies and schools disclose UIDs (Bhattacharya and Anand 2018). There are, however, no prescribed remedies provided for those who have already enrolled and submitted UIDs for various public- and private-provided amenities and have had their data shared. Notably, a dissenting judgment,⁴ written by Justice D.Y. Chandrachud, addressed data retention, stating that data should be kept for no more than six months, especially in the absence of mechanisms to hold UIDAI accountable for leaking data and ensuring its security. Further, Justice Chandrachud took issue with the majority holding that Aadhaar gives dignity to marginalised citizens, asserting, "One right cannot take away another. Dignity to the marginalised cannot do away with right of a person to bodily autonomy." The 2018 ruling, particularly the

³ Reports by *The Hindu* and *The Indian Express* include the full text of the ruling, which is available at <https://indianexpress.com/article/india/aadhaar-verdict-full-text-judgment-supreme-court-order-5374794/>.

⁴ Justice Chandrachud stated that the Section 7 of the *Aadhaar Act* is unconstitutional on the grounds that it makes Aadhaar mandatory for state subsidies. Also referring to it as a "fraud on the Constitution," he acknowledged that enshrined guidelines for a Money Bill, indicating that the *Aadhaar Act* exceeds the limits they put forth.

dissenting judgement, highlights that concerns around Aadhaar are still linked to fundamental questions of personhood, citizenship, and bodily integrity, even though its focus on persons are socio-technical and abstracted as data.

3 INSIGHTS ABOUT SURVEILLANCE AS/AND GOVERNANCE

In less than a decade, Aadhaar has surpassed its original mandate as a fix for a leaky social assistance system. Instead, it has become a central piece within a larger push to modernise India's digital infrastructure and service delivery—one that builds in knowledge about and verification of Indian identities as the foundation for governance. It fits into a longer pattern of states identifying and delineating subjects in the name of providing for them. Even though the deployment of technologies, be they Aadhaar or other ways of distinguishing subjects, emerges as logical and even productive and beneficial, it is nonetheless an exercise of state power. These practices are not simply about *knowing* subjects, but also about *laying claim* to subjects. They are, according to Allen Feldman (1991, 115, emphasis in original), central to state maintenance: “(m)other bodies in order to engender itself. The production of bodies—political subjects—is the self-production of the state.” Although employing newer technologies of regulation, Aadhaar continues longer, biopolitical processes of state (co)production. Modi's popularised narratives about Aadhaar, for instance, are quite explicit about the centrality of the biopolitical management to state preservation: it emerges as a foundational aspect of the articulations *and* infrastructure of “Digital India.” Biogovernance is a core feature of the state apparatus. In this case, the Indian government purports technological innovation as a key component of its continued development, suggesting it supports a growth-oriented and sustainable trajectory of governance.

While the observation of states using techniques to know and document their subjects is not new, the socio-technical assemblage that constitutes India's changing approach to population governance—of which Aadhaar is a part—is distinct and worth unpacking. Consider, for instance, as Strange would suggest, the materiality of the digital infrastructure involved, including its implications. Recent developments reveal that Aadhaar, as a fix, is itself actually leaky—a feature that is not something that a technical adjustment can remedy. Instead, its problems stem from its materiality, which is, at its core, digital. This digital materiality makes Aadhaar more of a “thing” than an “object”: that is, as others have

reflected on in relation to data from self-tracking technologies (Pink et al. 2017, 9), a process that is “always incomplete” and ongoing, something that is open, not closed, a set of relationships that are in process and are being processed. Aadhaar is more than giving UIDs to residents and using data collected about them for verification purposes; it is also more than a national ID initiative. As explained by Maya Indira Ganesh (2018), it “is also a public-private partnership and a government project, critical public infrastructure, a complex socio-technical system, a biometric database, a contested legal subject, and now, a flagrant security risk.” In other words, Aadhaar, as a thing, is multiple—and thus so is its leakiness, as it spills into other spaces through verification and sharing, with the prospect of implicating multiple domains of everyday life. The infrastructure itself might be framed as a technically sound whole with tiered layers, but it, including its shortcomings and vulnerabilities, is more diffuse in practice.

The multiplicity of Aadhaar cannot be separated from its entanglements. Harvesting and using knowledge about individual residents takes shape in and becomes part of a larger ecosystem that includes embedded inequalities, such as India’s caste system and its reinforcement through endogamy and social exclusion. For example, Right to Food researchers have reportedly tried to track deaths from starvation that could be linked to the denial of food rations following the introduction of Aadhaar (Bhatia 2018). While specific reasons may vary, due either to technical or authentication errors or the inability to be verified in person, a notable pattern emerges, one in which marginalised members of Indian society, “including Muslims, Dalits, and members of remote tribes,” are more likely to be among the dead (Bhatia 2018). Such cases reveal what Ganesh (2018) warns about: the “untidy, imperfect interconnections between digital technology, privacy, and the contestations and manipulations of identity” can position Aadhaar as “a tool to perpetuate long-standing and deep-rooted forms of discrimination.” Even if well intended, Aadhaar can still be used to serve pernicious agendas, such as the misrecognition of gender minorities or the BJP’s promotion of Hindu nationalist beliefs and its enabling of religious fundamentalism. The broader implications are important: that the introduction of technological tools does not necessarily ensure objective or even outcomes. In fact, their implementation alone cannot escape or overcome inequality.

Understanding Aadhaar as leaky and inseparable from historical and contemporary tensions that have shaped the Indian state aids in understanding this particular form of surveillance as an approach to governance.

The embrace of surveillance accompanies a broader shift in governance, which others have described as the rise of the “regulatory state” (Braithwaite 2000). This term captures the increasing tendency of states to exercise power “through a regulatory framework, rather than through the monopolization of violence or the provision of welfare” (Walby 1999, 123). While Aadhaar may challenge this distinction drawn by scholars (since its introduction comes through social assistance provision, not a regulatory framework as such), its wider deployment demonstrates how regulatory frameworks emerge as the formations through which states wield power. As mentioned previously, this case of biogovernance reveals that the preoccupation with authenticating identities is about more than about delivering services; it is about marking political subjects. Knowledge about subjects is a foundation for governance; however, it is not complete knowledge. Rather, as scholars of surveillance have long observed (e.g., Haggerty and Ericson 2000), surveillance enables flows of data, which must be assembled and re-assembled for analysis and intervention. More surveillance, monitoring, and data triangulation may assist those processes, but analysis and intervention rely on representational findings that cannot fully capture human experience in context. In short, the state comes to know its subjects through mediated means, from data that are both extracted and abstracted through technical means. As a result, the nature of state knowledge is incomplete.

Perhaps what is striking about Aadhaar is the state’s openness in terms of framing it as a nationalist project. Other studies of state surveillance highlight how a regulatory focus on individualised bodies often draws public attention away from the machinery that continues or perpetuates inequalities, stigmatisation, or oppression (see Lyon 2013; Browne 2015; Dubrofsky and Magnet 2015). Citizens are expected to be transparent, yet the systems making them as such, as well as their beneficiaries, are rarely rendered fully visible. The short-circuiting of Aadhaar—through breaches exposing its technical vulnerabilities and pushback from legal and civil-society actors—shines a particularly critical light on this nationalised architecture. This power imbalance, combined with the aforementioned disparities of Aadhaar experienced in everyday life illustrates that it, as a socio-technical assemblage, maps onto the state’s existing “geographies of belonging and exclusion” that “privilege particular subjects’ positioning while simultaneously rendering other bodies vulnerable” (Moore et al. 2003, 14). This observation is an important reminder that contemporary articulations of structural power cannot be separated from their socio-technical conditions and interlocking systems of marginalisation.

4 CONCLUSION

So, what does an analysis of Aadhaar tell us about the relationships between knowledge, governance, and state power? On the one hand, it showcases how the pursuit of knowledge about subjects is central to exercising structural power. On the other, it enables scrutiny of how these practices are part of state maintenance. More importantly, though, it demonstrates how the two concerns are inextricably linked, with surveillance working in the service of both. Strange's theorising helps us to see that knowledge is foundational, but it does not provide the appropriate lens for tracing the relationships that shape the terrains of governance in which Aadhaar is enrolled and deployed. In contrast, poststructural insights, which Strange expressed scepticism about, aid in correcting how to focus on structural power; they have long been attuned to how biogovernance, inequality, and state authority coalesce in ways that are not limited to political economy's traditional areas of emphasis. As Paul Langley (2009, 128) acknowledges, Strange may have disrupted "previously settled conceptions of power[,] ... raising questions about the significance of knowledge in the materialization of the global political economy," but she also "contributed to the insulation or estrangement of the field from debates about power taking place across the social sciences, debates in which poststructuralism and Michel Foucault's (1980) work on 'power-knowledge' loomed large." Poststructural insights have since brought attention to how nation-state biopolitics bring about diverse material effects, including human experience, into stark relief, to which Strange does not attend.

A remaining challenge is how to account for the shifting techniques of biogovernance that Aadhaar reveals, especially as an assemblage of state, non-state, and hybrid entities operate—and will continue to operate—in ways that extract and utilise data on Indian subjects. While recent Indian Supreme Court rulings may weigh in on the appropriate use of UIDs, they may have little bearing in terms of influencing the nature of the architecture already in place. In fact, they explicitly stop short of doing so, drawing boundaries around the existence of privacy rights and whether companies can compel citizens to disclose their UIDs in the future. Thus, rather than reflect on what government actors have or have not done to check the exercise of structural power in this context, this chapter concludes with a reflection on how the fashioning of Aadhaar reflects a shift in how regulatory webs are woven.

As Eubanks (2018) writes in relation to the role that new technologies have played in welfare provision in the United States, the increased reliance on tools for monitoring compliance and for assessing and predicting risk has meant that already marginalised people are not only more likely to be surveilled more closely than other citizens, but they are also more prone to becoming ensnared by webs weaved by the socio-technical systems. That is, instead of technologies ensuring beneficiaries receive necessary provisions, they render already vulnerable subjects more susceptible to punitive measures. Although greater transparency before the state may promise better service delivery, it does not necessarily ensure it. It does, however, mean such subjects are exposed—and thereby become easier targets—for different facets of structural power. This observation is a reminder that state power is a violent force, even when it is not asserted through blunt measures. Be it within or beyond the borders of India, the United States, or elsewhere, the digital materiality of social assistance interventions, such as Aadhaar, means that knowledge about citizens passes through data-sharing webs that blur private and public domains. In doing so, it facilitates flows of structural power, which can concentrate around, target, and even fixate on subjects who are made more visible through these practices. Further, as the India case illustrates, its materiality facilitates the expansion of regulatory webs to encompass a wider range of residents—and rapidly so.

As argued here, Aadhaar as a fix for a leaking social assistance system has actually led to the institutionalisation of leakiness. Through the embrace of digital data for the purposes of regulation, leakiness is becoming a structural feature of governance. Although Strange passed away before the information society came fully into its own, her work nonetheless gives us a starting point for thinking through the foundational relationship between state power and knowledge, particularly in this current digital moment. In fact, further analysis in relation to other dimensions of Strange's framework could aid in eliciting how other structures come to bear on the case at hand. In order to make sense of how these entanglements operate, we cannot rely on Strange's ideas around structural power alone. We must look to scholarship that Strange herself did not appreciate, particularly as feminist and critical race scholarship has been central to illuminating how interlocking systems of oppression and social categories of difference work in tandem to make some subjects more vulnerable to the punitive aspects of state power than others. Moreover, by sharing Strange's commitment to granularity, we do not lose sight of the embodied aspects and effects of governance.

REFERENCES

- Ajana, Btihak. 2010. Recombinant Identities: Biometrics and Narrative Bioethics. *Journal of Bioethical Inquiry* 7 (2): 237–258.
- Bhatia, Rahul. 2018. How India's Welfare Revolution Is Starving Citizens. *The New Yorker*, May 16. <https://www.newyorker.com/news/dispatch/how-indias-welfare-revolution-is-starving-citizens>.
- Bhattacharya, Ananya, and Nupur Anand. 2018. Aadhaar Is Voluntary—But Millions of Indians Are Already Trapped. *Quartz*, September 25. <https://qz.com/india/1351263/supreme-court-verdict-how-indias-aadhaar-id-became-mandatory/>.
- Bill and Melinda Gates Foundation. 2017. *Financial Services for the Poor: India*. Accessed December 29, 2018. <http://stash.globalgoals.org/goalkeepers/datareport/case-studies/financial-services-for-the-poor-india/>.
- Braithwaite, John. 2000. The New Regulatory State and the Transformation of Criminology. *British Journal of Criminology* 40 (2): 222–238.
- Browne, Simone. 2010. Digital Epidermalization: Race, Identity, and Biometrics. *Critical Sociology* 36 (1): 131–150.
- . 2015. *Dark Matters: On the Surveillance of Blackness*. Durham, NC: Duke University Press.
- Dee, Mike. 2013. Welfare Surveillance, Income Management, and New Paternalism in Australia. *Surveillance & Society* 11 (3): 272–286.
- Dixit, Pranav. 2017a. India's National ID Program May Be Turning the Country into a Surveillance State. *Buzzfeed News*, April 4. <https://www.buzzfeed.com/pranavdixit/one-id-to-rule-them-all-controversy-plagues-indias-aadhaar>.
- . 2017b. Airbnb, Uber, and Ola Are Considering Using India's Creepy National ID Database. *Buzzfeed News*, July 19. https://www.buzzfeed.com/pranavdixit/airbnb-uber-and-ola-may-start-using-aadhaar-indias?utm_term=.sxVVwn0xMV#.bhGZwNmx0Z.
- . 2018. India's National ID Database with Private Information of Nearly 1.2 Billion People Was Reportedly Breached. *Buzzfeed News*, January 4. <https://www.buzzfeed.com/amphhtml/pranavdixit/indias-national-id-database-with-private-information-of>.
- Doshi, Vidhi. 2018. India's Biometric ID Program Was Supposed to End Welfare Corruption. But the Neediest May Be Hit Hardest. *Washington Post*, March 25. https://www.washingtonpost.com/world/asia_pacific/indias-vast-biometric-program-was-supposed-to-end-corruption-but-the-neediest-may-be-hit-hardest/2018/03/24/bb212a86-289c-11e8-a227-fd2b009466bc_story.html?utm_term=.79f45c7dc264.
- Drèze, Jean. 2014. On the Mythology of Social Policy. *The Hindu*, July 8. <http://www.thehindu.com/opinion/lead/on-the-mythology-of-social-policy/article6186895.ece>.

- Dubrofsky, Rachel E., and Shoshana Amielle Magnet. 2015. Feminist Surveillance Studies: Critical Interventions. In *Feminist Surveillance Studies*, ed. Rachel E. Dubrofsky and Shoshana Amielle Magnet, 1–17. Durham, NC: Duke University Press.
- Eubanks, Virginia. 2018. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York: St. Martin's Press.
- Feldman, Allen. 1991. *Formations of Violence: The Narrative of the Body and Political Terror in Northern Ireland*. Chicago: University of Chicago Press.
- Foucault, Michel. 1980. *Power/Knowledge: Selected Interviews and Other Writings, 1972–1977*. New York: Pantheon Books.
- Ganesh, Maya Indira. 2018. Data and Discrimination: Fintech, Biometrics, and Identity in India. *Cyborgology*, January 25. <https://thesocietypages.org/cyborgology/2018/01/25/fintech-aadhaar-and-identity-in-india/>.
- Gates, Kelly A. 2011. *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. New York: NYU Press.
- Ghoshal, Devjyost. 2017. The World's Largest Biometric ID Programme Is a Privacy Nightmare Waiting to Happen. *Quartz India*, March 28. <https://qz.com/943102/aadhaar-for-dummies-why-right-thinking-indians-should-be-worried-over-the-slow-death-of-privacy/>.
- Gilliom, John. 2001. *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy*. Chicago: University of Chicago Press.
- Goel, Vindu. 2018. 'Big Brother' in India Requires Fingerprint Scans for Food, Phones, and Finances. *New York Times*, April 7. <https://www.nytimes.com/2018/04/07/technology/india-id-aadhaar.html>.
- Goldberg, David Theo. 1997. *Racial Subjects: Writing on Race in America*. New York: Routledge.
- Government of India. 2016. Your Aadhaar. *Unique Identification Authority of India*, 2016. Accessed December 29, 2018. <https://uidai.gov.in/your-aadhaar/about-aadhaar.html>.
- Guruswamy, Menaka. 2017. India's Supreme Court Expands Freedom. *New York Times*, September 10. <https://www.nytimes.com/2017/09/10/opinion/indias-supreme-court-expands-freedom.html>.
- Guzik, Keith. 2017. *Making Things Stick: Surveillance Technologies and Mexico's War on Crime*. Berkeley: University of California Press.
- Haggerty, Kevin D., and Richard V. Ericson. 2000. The Surveillant Assemblage. *British Journal of Sociology* 51 (4): 605–622.
- India Stack. 2018. *What Is India Stack?* Accessed December 29, 2018. <http://indiastack.org/about/>.
- Khaira, Rachna. 2018. Rs 500, 10 Minutes, and You Have Access to Billion Aadhaar Details. *The Tribune*, January 3. <http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html>.

- Khera, Rachna. 2018. Why India's Big Fix Is a Big Flub. *New York Times*, January 21. <https://www.nytimes.com/2018/01/21/opinion/india-aadhaar-biometric-id.html>.
- Kumar, Hari. 2013. Unique ID Program Introduces Instant Verification Services. *The New York Times*, May 24. <https://india.blogs.nytimes.com/2013/05/24/aadhar-program-introduces-instant-verification-services/>.
- Langley, Paul. 2009. Power-Knowledge Estranged: From Susan Strange to Poststructuralism in British IPE. In *Routledge Handbook of International Political Economy (IPE): IPE as a Global Conversation*, ed. Mark Blyth, 126–139. New York: Routledge.
- Lyon, David. 2007. *Surveillance Studies: An Overview*. Cambridge: Polity Press.
- . 2013. *Identifying Citizens: ID Cards as Surveillance*. Cambridge: Polity Press.
- Magnet, Shoshana A. 2011. *When Biometrics Fail: Gender, Race, and the Technology of Identity*. Durham: Duke University Press.
- Monahan, Torin. 2017. Regulating Belonging: Surveillance, Inequality, and the Cultural Production of Abjection. *Journal of Cultural Economy* 10 (2): 191–205.
- Moore, Donald S., Anand Pandian, and Jake Kosak. 2003. The Cultural Politics of Race and Nature: Terrains of Power and Practice. In *Race, Nature, and the Politics of Difference*, ed. Donald S. Moore, Jake Kosak, and Anand Pandian, 1–70. Durham, NC: Duke University Press.
- Narendramodi. 2014. On Aadhaar, Neither the Team That I Met Nor PM Could Answer My Qs on Security Threat It Can Pose. There Is No Vision, Only Political Gimmick. *Twitter Post*, April 8. Accessed December 29, 2018. <https://twitter.com/narendramodi/status/453543852175925248>.
- Nilekani, Nandan. 2009. *Imagining India: The Idea of a Renewed Nation*. New York: Penguin.
- Parker, Ian. 2011. The I.D. Man. *The New Yorker*, October 3. <https://www.newyorker.com/magazine/2011/10/03/the-i-d-man>.
- Patton, Paul. 1994. Metamorpho-Logic: Bodies and Powers in *A Thousand Plateaus*. *Journal of the British Society of Phenomenology* 25 (2): 157–169.
- Pink, Sarah, Shanti Sumartojo, Deborah Lupton, and Christine Heyes La Bond. 2017. Mundane Data: The Routines, Contingencies, and Accomplishments of Digital Living. *Big Data & Society*, Online First. <https://doi.org/10.1177/2053951717700924>.
- Safi, Michael. 2018. Reporter Who Exposed India Data Breach Named in Criminal Complaint. *The Guardian*, January 8. <https://amp.theguardian.com/world/2018/jan/08/reporter-who-exposed-huge-indian-data-breach-rachna-khaira-named-in-government-criminal-complaint>.
- Sathe, Vijay. 2014. Managing Massive Change: India's Aadhaar, the World's Most Ambitious ID Project. *Innovations* 9 (1/2): 85–111.

- Sharma, Pankul. 2018. Only Male or Female Can Get PAN Card, Transgender Told. *Times of India*, March 15. <https://timesofindia.indiatimes.com/india/only-male-or-female-can-get-pan-card-transgender-told/articleshow/63321785.cms>.
- Singh, Manish. 2017. Is India's Central Database with Biometric Details of Its Billion Citizens a Privacy Nightmare? *Mashable*, February 14. <https://mashable.com/2017/02/14/india-aadhaar-uidai-privacy-security-debate/#ZgQ0T5iIwOqc>.
- Staples, William G. 2014. *Everyday Surveillance: Vigilance and Visibility in Postmodern Life*. 2nd ed. Lanham, MD: Rowman & Littlefield.
- Strange, Susan. 1998. *States and Markets*. London: Pinter.
- Targeted Delivery of Financial and Other Subsidies, Benefits and Services (Aadhaar) Act, 2016. https://uidai.gov.in/images/the_aadhaar_act_2016.pdf.
- The Economist. 2017. Digital Dawn. *The Economist*, April 15, 32–33.
- Torpey, John. 2009. *The Invention of the Passport: Surveillance, Citizenship, and the State*. Cambridge: Cambridge University Press.
- Trubek, David M., and Louise G. Trubek. 2005. Hard and Soft Law in the Construction of Social Europe: The Roles of the Open Method of Co-ordination. *European Law Journal* 11 (3): 343–364.
- Tufekci, Zeynep. 2014. Engineering the Public: Big Data, Surveillance, and Computational Politics. *First Monday* 19 (7). <https://doi.org/10.5210/fm.v19i7.4901>.
- Walby, Sylvia. 1999. The New Regulatory State: The Social Powers of the European Union. *British Journal of Sociology* 50 (1): 118–138.
- World Bank. 2016. Enabling Digital Development: Digital Identity. *World Development Report 2016*. <http://pubdocs.worldbank.org/en/822821519686607466/9781464806711-WDR2016-Spot4-Rev-Oct2017.pdf>.

Open Access This chapter is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, duplication, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, a link is provided to the Creative Commons licence and any changes made are indicated.

The images or other third party material in this chapter are included in the work's Creative Commons licence, unless indicated otherwise in the credit line; if such material is not included in the work's Creative Commons licence and the respective action is not permitted by statutory regulation, users will need to obtain permission from the license holder to duplicate, adapt or reproduce the material.