Crafting “Integrity”: The Implications of Authentication through Unique Identification Databases

S. Shakthi

Electronic version

URL: <http://journals.openedition.org/samaj/6414>

DOI: 10.4000/samaj.6414

ISSN: 1960-6060

Publisher

Association pour la recherche sur l'Asie du Sud (ARAS)

Electronic reference

S. Shakthi, « Crafting “Integrity”: The Implications of Authentication through Unique Identification Databases », *South Asia Multidisciplinary Academic Journal* [Online], 23 | 2020, Online since 30 March 2020, connection on 16 September 2020. URL : <http://journals.openedition.org/samaj/6414> ; DOI : <https://doi.org/10.4000/samaj.6414>

This text was automatically generated on 16 September 2020.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

Crafting “Integrity”: The Implications of Authentication through Unique Identification Databases

S. Shakthi

Introduction¹

- ¹ With the aim of enrolling every Indian resident, the Aadhaar program, overseen by the Unique Identification Authority of India (UIDAI), has been promoted in official discourse as a transformative tool for eliminating “duplicates and fake identities” and ensuring transparency in welfare and service provision to authenticated individuals.² Nandan Nilekani, widely regarded as the architect of Aadhaar, has declared that the national biometric-based identification scheme has saved the Indian government \$9 billion in “fraud and wastage.”³ This emphasis on ensuring authenticity was similarly deployed three years before the creation of the UIDAI and four years before the first Aadhaar number was issued, in another Indian unique identification project with strong connections to Aadhaar. Known as the National Skills Registry (NSR), this database, launched in 2006 by the Indian information technology (IT) industry’s employer association, NASSCOM,⁴ utilizes biometric identification to create individual profiles of current and potential IT employees.
- ² With estimated annual revenue of over 123 billion GBP (NASSCOM 2018), the Indian IT industry is largely populated by college-educated professionals with relatively substantial salaries, middle-class lifestyles, and opportunities to travel and work abroad.⁵ An exploration of practices and policies in the IT industry might therefore appear somewhat removed from an analysis of Aadhaar, which lays particular emphasis on the efficient delivery of welfare schemes and subsidies targeted at the poor (Nilekani and Shah 2015). Yet, even a relatively superficial investigation reveals a

number of *material* connections between the IT industry and the Aadhaar program. Perhaps the most obvious is Nilekani himself. Nilekani, the first Chairman of the UIDAI, is one of India's most famous IT entrepreneurs, having co-founded the country's second-largest IT firm, Infosys. The expansion of Aadhaar's focus towards linking a range of public and private services to this unique identification number has also resulted in the creation of the Indian Software Products Industry Round Table, or iSPIRT. This entity, which describes itself as a think tank, is primarily staffed by former members of NASSCOM, and provides technological tools for the incorporation of Aadhaar into the provision of these services, as well as lobbying on behalf of businesses that utilize Aadhaar (Thaker 2018).⁶

- 3 Beyond these direct linkages, strong parallels to the Aadhaar program can be seen in the proliferation of the NSR. This IT employee database and its vision of safeguarding authenticity have been endorsed by Nilekani in his 2014 book, *Rebooting India*, co-written with another key Aadhaar engineer, Viral Shah (Nilekani and Shah 2015:252).⁷ More broadly, in its attempt to re-invent itself as a "start-up state" (Nair 2019), the government's increasing reliance on neoliberal techniques of governance in the pursuit of its development agenda reminds us that "the private sector often provides the model for efficiency" (Rao and Nair 2019:471) for state practice.
- 4 This paper presents an analysis of the NSR, which, operated by the country's largest private-sector employer, provides a useful comparative framework for evaluating the trajectory and scope of Aadhaar. In particular, by focusing on the industry's attempt at disciplining its workforce through the use of biopower (Foucault 1978), this paper recalls Foucauldian arguments in existing scholarship on the application of Aadhaar in managing targeted populations (Chaudhuri and König 2018; Maringanti 2009; Sarkar 2014). While the surveillance of employees in both conspicuous and subtle ways is commonplace in the industry (Upadhya and Vasavi 2006), I argue that this has been reinforced by the discourse of "integrity" that is frequently deployed to manage employees. The NSR, as a centralized repository of employees' personal, professional and biometric information, becomes a crucial site of enforcing "integrity," allowing companies to not only mark compliant employees as legitimate, but to also potentially contain acts of resistance.
- 5 In the remainder of this paper, I contextualize the study by drawing from literature on surveillance, particularly as a corporate disciplining technique, and the growing body of scholarship on identification systems, citizenship and civil liberties in India. I also provide an overview of the Indian IT industry, the NSR, and the methods used for this study. I then interrogate the surveillance culture of the IT industry and analyze "integrity," or compliance with corporate policies, as a disciplining strategy. Placing the NSR within this framework, I highlight the similarities of the NSR with Aadhaar, while also exploring the emergence of the "NSR blacklist," a rumored compilation of deviant employees in the NSR visible only to employers. In deconstructing the myth-making, misconceptions and self-disciplining generated by the existence of the NSR, I comment on Aadhaar's implications for safeguarding individual privacy, the power of private players under neoliberal capitalism and the increasing ubiquity of surveillance strategies in everyday practices.

Situating Corporate Surveillance and Unique Identification Databases

- 6 This empirical study of the NSR and its socio-political implications draws on the rich body of scholarship on techno-social identities (Amoore 2006; Lyon 2009, 2001; Rose 1999). This research argues that biometric verification systems, operating in the interest of both public agencies and private capital, assume that identity is located within a stable body that can be easily legitimated (Amoore 2006). In the process, these programs create fixed categories that particularly favor state interests over citizen needs (Lyon 2009). Rose (1999) highlights the potential for these systems to result in modes of exclusion that are often predicated on existing lines of identity and difference.⁸ Moreover, Rose addresses the scope of surveillance through unique identification. In the "securitization of identity," as Rose argues, the objective is not to administer *constant* surveillance, but to provide "conditional access to circuits of consumption and civility" (Rose 1999:243). Much of this work builds on, critiques and develops Foucault's influential formulations on governmentality and bio-power (Foucault 1991, 1978). Foucault's theory of governmentality, or the institutional governance of a population through strategies that aim to foster a culture of self-discipline, has provided an important conceptual framework for unpacking surveillance mechanisms. Similarly, the "anatomo-politics" (Foucault 1978) of bio-power—aimed at influencing individual behavior by operating on and through biological characteristics of discrete bodies—allows for further theorization on biometrics as a tool for enforcing productivity through compliance.
- 7 This paper also adds to the diverse body of literature on corporate strategies for controlling and managing employees (Freeman 2000; Kunda 1992; Ong 1987; Salzinger 2000; Upadhy and Vasavi 2006). Ong (1987), in her classic study of female factory workers in Malaysia, found that these women were often referred to as "factory daughters," emphasizing their subordinate status to paternalistic male managers while simultaneously desexualizing them.⁹ In his study of software engineers in Silicon Valley, Kunda (1992) has identified how "normative control" is deployed to maximize productivity. Kunda (1992) defines this as "the desire to bind employees' hearts and minds to the corporate interest" (p.217). This normative control is seen in decentralized practices that encourage employees themselves to be invested in this process. He notes that alongside these modes of normative control, "utilitarian" methods based on vertical operations of power are also prevalent. Moreover, Kunda has observed that the construction of subjectivities within Silicon Valley occurs through both the acceptance *and* the contestation of these power structures, as employees do not unquestioningly imbibe this logic of control. In their study of the Indian IT industry, Upadhy and Vasavi (2006) found a similar blending of extreme "panoptical" systems of control with subjective management techniques, with companies sometimes attempting to create a "fun" atmosphere in order to mask the rigidity, monotony and stress of their work processes.
- 8 Turning to unique identification as a site of analysis, a robust body of literature has emerged in recent years in response to the state's adoption of biometric-based systems of verification. Much of this scholarship has emphasized the shift in state-subject relations that both arises from and has contributed to the implementation of Aadhaar (Abraham 2018; Chaudhuri and König 2018; Maringanti 2009; Rao and Nair 2019;

Shukla 2010). The state’s framing of its operations in the language of the market has led to a “bureaucratic—technocratic—entrepreneurial model of development” (Rao and Nair 2019:474) that closely resembles the structures of the service industry. Within this discourse, residents are framed as “customers” who avail of the government’s services, which are delivered partly in collaboration with private sector resources (Chaudhuri and König 2018:127–128). The transactional nature of Aadhaar, where the state has emerged as a “mediator and facilitator” of the market (Shukla 2010:31), has profound implications for residents’ interactions with state apparatus.

- 9 This literature also explores the intended and material operation of Aadhaar. Sarkar (2014) delineates the principles behind the program, arguing that its binary distinction between legitimate applicants for entitlements and purported pretenders results in the formulation of a “static” system that leaves little room for unforeseen deviations from this model. Simultaneously, as other studies have highlighted (Nair 2018; Rao 2013), a number of contradictions have become visible in the program’s actual implementation, as systems of marginality and exclusion find continuities in its execution.
- 10 The potential for Aadhaar to be utilized by the state as a mode of surveillance has also been commented on in recent scholarship (Khera 2019; Ramanathan 2010). This research delves into the concept of data “convergence” (Ramanathan 2010). It argues that Aadhaar, once “seeded” into a number of other public and private databases, would allow for privacy infringement and individual profiling, with consequences for those posing resistance to the state.¹⁰ In the context of South Africa’s unique identification system, HANIS, Breckenridge (2005) has similarly discussed the privacy-related consequences of “data-creep,” or the ability of a biometric-based identification program to enable the building of individual resident profiles.
- 11 Moreover, a growing body of literature has utilized ethnographic methods to interrogate the social meanings of surveillance. Prasad-Aleyamma (2018) notes that technology utilized for biometric identification is not merely a transformative surveillance mechanism. Rather, surveillance through technology must also be conceptualized as a *consequence* of complex and variegated socio-political strategies. This research also addresses the performativity of negotiations with biometrics (Rao 2018; Solanki 2019). Solanki (2019), in his study of the role of biometric identification in evaluating government employees in a North Indian state, notes that attempts at managing this workforce result instead in the “performance of management.” Rao’s (2018) analysis of two disparate physical sites that utilize biometric identification reveals that contrary to their portrayal as a means of fixing identities, biometric systems are open to manipulation, including by those they are meant to control and categorize. This paper contributes to this scholarship by providing a situated analysis of an industry-specific surveillance mechanism, using ethnographic methods to highlight the constructed nature of surveillance itself.

Field Site and Methodology

- 12 The birth of the Indian IT industry can be traced to the early 1970s, when the central government first began to promote software exports and the inclusion of computer science courses in higher education institutions (Heeks 1996). In 1984, the government under then-Prime Minister Rajiv Gandhi released a “Computer Policy” that officially

recognized software as an industry (Parthasarathy 2005), with subsequent policies further easing restrictions for investors. The launch of the Software Technology Parks of India (STPI) in 1991—a government organization that provides IT companies with well-equipped physical spaces for conducting business—allowed foreign companies to offshore their software and services requirements directly to Indian sites, while domestic companies also benefited from the availability of suitable infrastructure (Upadhyaya and Vasavi 2006). Combined with the economic reforms of the 1990s,¹¹ which significantly reduced barriers to the inflow of foreign capital, and the availability of a technically-educated, relatively cheap, English-speaking labor force, the path was set for the rapid growth of the industry.

- 13 The IT industry has demonstrated a particular reliance on foreign clients (Chandrasekhar 2005; Kumar 2005). As Patibandla, Kapur and Petersen (2000) have argued, the very foundation of the industry was built on exports, which has deeply influenced its institutional growth. Moreover, the industry has received considerable state support since its inception, with both the central and state governments providing numerous incentives to encourage its expansion. In turn, the industry has demonstrated its ability to exert influence over policymaking (Parthasarathy 2005); NASSCOM which was founded in 1988, played a key role in establishing the STPI (Upadhyaya and Vasavi 2006).
- 14 Software and services companies have begun to contribute significantly to Chennai's economy in recent years, operating alongside more established industries such as automobile and electronics manufacturing, healthcare, and financial services. As one of India's largest IT centers and the capital of the southeastern state of Tamil Nadu, Chennai has witnessed rapid urban development over the last decade to accommodate and facilitate the expansion of the industry. Most major Indian and foreign companies operating in India are represented in sprawling, self-contained office complexes and IT parks dotted throughout the city. Tamil Nadu has nearly 600 engineering colleges, with around 250,000 new students entering these institutions every year (Government of Tamil Nadu 2015). There are also several arts and science colleges that feed into the industry. The availability of a large pool of potential employees can be viewed as a major reason for the expansion of the IT industry in the city.
- 15 This paper derives from a broader research project that analyzed the construction of middle-class subjectivities through employment in Chennai's IT industry. Between 2015 and 2016, I spent nine months conducting fieldwork in Chennai, where I interviewed IT employees, managers, and executives, some of whom were NASSCOM office-bearers. I also spoke with a number of people indirectly connected to the industry, such as union leaders, labor activists, diversity and recruitment consultants, and bureaucrats. While gaining extended access to companies proved to be difficult, I was able to conduct ethnographic observation in spaces associated with the industry, such as IT conferences. Moreover, for this paper, a detailed reading of reports issued by the government and by NASSCOM, and of the NSR website, in particular, informs much of the analysis. With a view of documents as "'social facts' [that are] produced, shared and used in socially organized ways" (Atkinson and Coffey 2010:79), triangulating interview and observation data with documentary analysis provided deeper insights into the implications of the industry's adoption of a unique identification system for employees.
- 16 Before proceeding, a brief overview of the NSR is called for. The NSR is now used by most major IT firms in the country (although it has not been uniformly adopted across

the industry), with 341 companies having subscribed to it thus far, according to its official website.¹² While not all of my respondents had registered with the NSR (and a few were not even aware of its existence), all of my younger informants at major IT firms had been required to do so. Major companies such as Infosys, Wipro and Tata Consultancy Services have made registration compulsory as a pre-condition of employment. There are currently over 2.6 million individuals registered in the database, of whom over 1.7 million have submitted their biometric information.

- 17 Registration with the NSR consists of two stages: first, employees must fill out the registration form on the NSR website, where they are required to provide information including their present and previous addresses, phone number(s), father's name, mother's maiden name, spouse's name, passport information and PAN card¹³ details (provided the employee is in possession of these documents), along with their educational and employment histories. Following this, they must visit a "Point of Service" (POS),¹⁴ where they are required to pay the registration fee,¹⁵ provide photo ID for verification of their profiles, and submit their fingerprints. While the NSR website does not mention this, two of my respondents also claimed to have had their retinas scanned for additional biometric information. Once these steps have been completed, the system generates a unique number for the registered employee, known as an ITPIN.

16

Locating Integrity

- 18 The extent of direct, visible surveillance within the workspaces of the IT industry is striking, perhaps reflective of the broader trend towards the rise of routinized surveillance in modern society (Lyon 2001). When visiting IT offices to conduct interviews, I was generally required to pass through multiple layers of security before being allowed in. I was usually asked to enter my name, whom I was there to meet and which "company" I was from in a log book, and was often asked to surrender my laptop before entering the premises. At some companies, a sticker was pasted over my phone camera. One of my respondents, Murali,¹⁷ an employee at a mid-sized company described the level of protection around these companies as being akin to a fort in the Chola Empire.¹⁸ I was told that this level of scrutiny was required to prevent data theft and keep confidential material secure, as companies often handle sensitive information for their clients.
- 19 These surveillance techniques also manifest in more subtle forms, having become embedded in the work culture of the industry (Upadhya and Vasavi 2006), with a host of actors having been co-opted into the process of surveilling each other and themselves.¹⁹ Besides managers and IT employees, this includes administrative, security and cleaning staff. I met one of my informants, Sonam, at an IT park where her company was located. A busy HR executive, Sonam suggested I interview her in the building's food court, to avoid having to surrender my laptop and cell phone. Yet, a few minutes after opening my laptop, I was told by a member of the cleaning staff that it was not allowed on the premises and was made to put it away.
- 20 Similarly, the use of identity cards by employees to "swipe-in and swipe-out" of offices demonstrates the level of daily scrutiny that they are placed under. Employees wear their ID cards around their necks, or clipped to their belts, which they scan at automated turnstiles before entering or leaving their office premises. This process is

not only meant to prevent “outsiders” from freely entering these complexes, but also allows companies to maintain a record of the number of hours employees have spent at work, which can then be linked to employee appraisals. The declaration by two different executives that their companies “study” employees in a “360-degree” manner during these appraisals, underscores the importance placed on an overarching, panoptical view of employees. Some companies have also introduced written examinations as part of their appraisals, thereby informing employees that their productivity is being surveilled, scrutinized, and, literally, tested.

- 21 With the aim of maximizing productivity, these strategies of surveillance have given rise to a discursive construction referred to as “integrity.” Specifically aimed at fostering a culture of discipline in the IT workforce, the idea of “integrity” (or a perceived lack thereof), was explained to me by Pranav, a software developer at a major company:

They keep sending flyers [email notices] on two things. One is on workplace harassment, and the other is on *integrity*. You shouldn’t wear someone else’s ID card and swipe it at the office, or if you take leave, you should update it. The company calls these administrative issues “integrity,” and they keep updating us on that [emphasis added].

In this context, “integrity” refers to employee *adherence* to corporate policies aimed at creating a disciplined workforce. While the promotion of integrity is undoubtedly connected with a broader emphasis on productivity, I would argue that it must nevertheless be conceptualized as a distinct construct. Within the language of integrity is encoded the insidious message of employees’ untrustworthiness. As a result, employees who conform to companies’ disciplining strategies are marked as having integrity; conversely, acts of resistance can be framed as demonstrating a *lack* of integrity. In a climate where IT professionals have slowly begun to take collective action against employers (Shakthi 2018), the discursive binary of compliant/disruptive mediated through the deployment of “integrity” imbues companies with further authority to censure employees. Thus, we observe that subversive behavior aimed at resisting corporate hegemony can be co-opted by those in power to further their own agenda (Gupta in Elias 2005:213).

- 22 The use of “integrity” to either legitimize employees, or to depict them as unreliable, irresponsible or deceitful, has, in turn, allowed companies to adopt more forceful and visible disciplining practices. For example, when I spoke to Uttara, a software engineer at an offshore support center for a major bank, she began to tell me about a “resting room” at her office, where she went to lie down when she was feeling tired during both her pregnancies. As she recounted,

Initially when I was pregnant, I didn’t have to tell my managers or anything. I just had to tell the security staff to open the room [when] I needed to rest, and I had to enter [my details] in the register. It was initially like that. Later on, they changed the process. Prior to taking even a nap, I have to send an email to my manager, who sits in Hyderabad, he has to approve it, and then I have to show that letter to the security people, then only they will open it.

Uttara was thus required to receive an official authorization to utilize this facility from her manager, who works in a different city. When I asked her why this change had been implemented, she mused that people might “misuse” the resting room. Here, we can

observe the complex interplay between discipline and integrity, with more severe policies being justified as preemptive measures to counter a perceived lack of integrity.

Verifying Integrity

- 23 The NSR, as a centralized database that categorizes employees as verified professionals, might be viewed as a crucial site for crafting “integrity.” According to the NSR website, the purpose of the database is as follows:

National Skills Registry is a NASSCOM initiative to have a robust and credible **information infrastructure** about all persons working in the industry. This develops **trusted and permanent fact sheet of information** about each professional along with background check reports. This is a **security best practice** for the industry and **assures identity security**, [and] **industry acceptance to [sic] honest professionals** [words in bold in original].²⁰

Like Aadhaar, the NSR emphasizes uniqueness, robustness, credibility, and permanence: a single, verified profile that will last one’s entire lifetime. Consequently, one of its key “benefits,” as listed on its website, is that it “*creates an environment of discipline*” [emphasis added].²¹ In the case of the NSR, both companies and employees have the option of carrying this verification forward further through background checks on the information listed in employees’ profiles, which are conducted by “Empaneled Background Checkers” (EBCs). These EBCs are private data verification companies that have been authorized by NASSCOM to undertake this task. The EBCs employ a range of verification methods; the employee’s listed current address, for example, is verified by a member of the EBC physically travelling to the address, while educational qualifications are cross-checked against listed educational institutions. If a background check is conducted, the results will be officially recorded in the employee’s profile.²²

- 24 As with Aadhaar, the purpose of the NSR is not simply to establish the identity of prospective or current employees, but to authenticate, and therefore legitimize, the identity they claim to occupy (Nayar 2012:17). The concern over fake credentials is a prevalent discourse in the industry; in their book, Shah and Nilekani claim that a fifth of resumes circulating in the IT industry are fake (Nilekani and Shah 2015:249).²³ The NSR website insists that registration allows employees to “join the league of registered and trusted professionals,” which will eliminate the risk of “other persons with fake/inflated details” vying for the same positions.²⁴ This recalls the focus of Aadhaar on preventing fraud,²⁵ as asserted by the UIDAI, which identifies challenges in the execution of welfare schemes being largely due to the pervasiveness of “fake and ghost identities.”²⁶ Through this emphasis on accreditation through biometric identification, the NSR is used to ensure that the “integrity” of the IT workforce is maintained.
- 25 Moreover, the IT industry’s anxieties over upholding “integrity” seem to stem, at least in part, from the industry’s relationship with foreign clients. This is articulated explicitly in multiple places on the NSR website. Explaining why the project was launched, the NSR website laments that the absence in India of a “**central and public database of its citizens**” is a cause for concern for the industry’s “**global clients**” [words in bold in original].²⁷ By compiling this information, the stated purpose of the NSR is to establish the credibility of the Indian IT workforce, thereby assuring clients that their sensitive data will be protected.²⁸ Falling within the spectrum of “biopolitical

strategies that categorize modern bodies" (Harcourt 2009:21), the NSR's use of biometric data is its trump card, ensuring employee uniqueness, and consequently, "integrity," in the global marketplace. The establishment of the NSR must also be considered in the context of the industry's importance in the Indian economy. While no comprehensive data protection law currently exists in India,²⁹ a set of rules³⁰ prescribed by the central government for corporations outlines security and privacy guidelines for "sensitive" data such as biometric information. Yet, the actual practices that companies adopt to collect this data have thus far escaped scrutiny, with the NSR being projected, much like Aadhaar, as merely a "technical solution to the problem of uncertainties of identity" (Sarkar 2014:525). The ability of NASSCOM, a trade association for private companies, to collect biometric information from employees and store this in a centralized database, brings to mind Ong's theory of "graduated sovereignty" (Ong 2006). As Ong has noted, "governments adjust political space to the dictates of global capital, giving corporations an indirect power over the political conditions of citizens" (Ong 2006:78). Thus, any ethical consideration of the NSR appears to have been overlooked to accommodate the demands of the transnational capitalist system.

Enforcing Integrity

- 26 When asking my respondents about the NSR, a number of them, primarily those who were active in the IT unions that have recently emerged in the city, mentioned an "NSR blacklist." Discussions on social media and online forums reveal that this "blacklist," or the "blacklisting" of employees on the NSR, is also debated among broader sections of the IT workforce. Yet, none of my respondents were willing to definitively confirm that an actual blacklist even existed, or that they could provide proof to this effect. The process of blacklisting was, instead, *visualized* as the addition of a "black mark" to an employee's NSR profile by their company, or, alternatively, of placing the employee and their NSR profile on a virtual "blacklist." In this narrative, employees would not be aware that they had been placed on a "blacklist." This was envisioned as a mechanism through which employers could inform other registered companies that a particular employee had exhibited transgressive behavior (the nature of which was itself not clearly defined), effectively rendering them unemployable.
- 27 Certainly, there are other aspects of the NSR that plainly reveal the power imbalance between employers and employees in the industry. If a company has lodged a complaint with the police or has initiated court proceedings against an employee registered in the NSR, for example, the database permits the company to mention this on the employee's profile, even if a verdict has not been arrived at.³¹ In contrast, the disciplinary force of the blacklist emerges from uncertainty; with the truth of its existence remaining unclear, the nature of indiscretions that could potentially result in being placed on the blacklist has also been left unspecified. Thus, rather than the blacklist itself, the *fear* of being blacklisted appears to be more compelling within the wider framework of the NSR and employee integrity. My discussions with IT union leaders in Chennai revealed their concerns that some employees' anxiety over being placed on the blacklist was contributing towards preventing them from participating in collective action. In my conversation with Hemant and Venkat, both members of a local IT union, they expanded further on the imagined utility of the NSR for employers in creating compliance within the workforce:

Venkat: They [companies] access NASSCOM's database, so they check if everything you say is true, using their data. The big fear everyone has is, if they find out they are in a union, they will blacklist them, so when they apply to another company, there will be a problem—their whole life will be ruined [...]

Shakthi: But is there proof that they are blacklisting?

V: No, that fear is there. But they are definitely maintaining a database.

Hemant: A lot of HR managers tell their employees, "Your name will be included in the blacklist." When they say something like that, we can't get a hard copy of proof. But people say this happens in a lot of places...Suddenly, one fine morning, if they are given a pink slip, and they no longer have that salary, they can't even imagine that. They can't survive for even one week, and they can't join another job. So, with that fear alone, these companies control everything.

We observe through these statements that the actual existence of the blacklist is irrelevant to its utility as a disciplining mechanism. Through the creation of this centralized employee repository, the industry is imbued with the ability to control employees through nothing more than the perceived *risk* of sanction. As Murali, a software engineer at a mid-sized company and a member of another IT union explained, "How they threaten is, we are all one entity. Anywhere you go, we will find you out. They say that at the beginning itself, we will check all this." This is not to suggest that such efforts have gone unchallenged, with the "blacklist" being discussed as a possible site for collective action by all the IT union leaders I spoke with. In effect, the ambiguity around the list has overshadowed the NSR itself as a source of contestation within the "new regimes of surveillance" (Rao 2018:69) facilitated by the emergence of biometric verification.

- 28 The possibly mythical existence of the blacklist, viewed through the lens of fraud/integrity, presents an important site for understanding how Aadhaar might be deployed to manage residents. While thus far, there does not appear to be a construct commensurate with the NSR blacklist that has been generated by the introduction of Aadhaar, it nevertheless holds the potential to give rise to a similar system of intimidation, partial information and centralized control (Khera 2019). As Aadhaar continues to seep into deeper corners of everyday life, we might note that, as with the NSR blacklist, the *fear* of censure through surveillance alone might emerge as an increasingly visible tool for curbing dissent against the state.

Conclusion

- 29 This paper utilizes the framework of the National Skills Registry, a centralized, permanent database that aims to collect and compile data on Indian IT employees, to comment on the possibilities for unique identification systems to influence their target populations. It analyzes the discourse of "integrity" in the Indian IT industry, situating it within its entrenched culture of surveillance. This discursive construction classifies employees as either legitimate inhabitants of IT workspaces, or as unsuitable to be engaged in IT employment. Mediated through the NSR, "integrity" becomes a quality that can be catalogued and verified. The threat of being placed on the NSR "blacklist," an unconfirmed compilation of disobedient employees, exposes the fundamental challenge to civil liberties contained within systems such as Aadhaar. What forms

might the discourse of "integrity" assume in the state's narratives around authenticity and fraud? As this paper has argued, the very existence of databases that operate through the centralization of information can result in forms of self-disciplining through the fear of exclusion.

- 30 The state's shift towards operating like a "platform" for the delivery of services contingent on Aadhaar verification shows strong parallels with IT-based configurations (Rao and Nair 2019). Indeed, given the critical role of prominent members of the Indian IT industry in the Aadhaar project, the structures and practices of the industry have undoubtedly influenced the formulation and implementation of Aadhaar. Moreover, the existence of the NSR itself is representative of the power of private capital in the new economy, and of the interconnected nature of state-market relations, with the IT industry being a particularly influential player in this setting.³² The government's attempts at linking all essential services, whether public or private, to Aadhaar, underscores the influence of market concerns in its implementation.
- 31 The possibility of Aadhaar serving as a tool for surveillance, and to discipline and manage residents, must then be contextualized within the wider system of techno-social formations in Indian society. Both the NSR and Aadhaar are part of a range of public and private biometric techniques in India that include fingerprinting technology to mark attendance in private companies (Rao 2018) and the impending launch of the world's largest facial recognition system by the country's crime data bureau.³³ As biometric data collection becomes ubiquitous in the lives of Indian residents, ethnographic studies that pay attention to its everyday practices are crucial for understanding its socio-political implications. While the potential for "data-creep" is clearly embedded in Aadhaar, this paper moves beyond the materiality of surveillance to interrogate specific forms of discursive control. Using the NSR as its site of analysis, it demonstrates how the language of surveillance both shapes and is constructed by the structures within which it operates. Thus, by placing Aadhaar within this framework, we can locate new, situated configurations of the broader culture of techno-surveillance.

BIBLIOGRAPHY

- Abraham, Itty. 2018. "Prehistory of Aadhaar: Body, Law, and Technology as Postcolonial Assemblage." *East Asian Science, Technology and Society: An International Journal* 12:377–92.
- Amoore, Louise. 2006. "Biometric Borders: Governing Mobilities in the War on Terror." *Political Geography* 25(3):336–51.
- Atkinson, Paul and Amanda Coffey. 2010. "Analyzing Documentary Realities." Pp. 77–92 in *Doing Qualitative Research: A Practical Handbook*, edited by D. Silverman. London: SAGE.
- Breckenridge, Keith. 2005. "The Biometric State: The Promise and Peril of Digital Government in the New South Africa." *Journal of Southern African Studies* 31(2):267–82.

- Chandrasekhar, C.P. 2005. "The Diffusion of Information Technology and Implications for Development: A Perspective Based on the Indian Experience." Pp. 40–92 in *ICTs and Indian Economic Development: Economy, Work, Regulation*, edited by A. Saith and M. Vijayabaskar. New Delhi; London: Sage.
- Chaudhuri, Bidisha and Lion König. 2018. "The Aadhaar Scheme: A Cornerstone of a New Citizenship Regime in India?" *Contemporary South Asia* 26(2):127–42.
- Cohen, Lawrence. 2019. "India as Database: Response to Reetika Khera." *Contributions to Indian Sociology* 53(2):328–40.
- Cohen, Lawrence. 2017. "Duplicate." *South Asia: Journal of South Asian Studies* 40(2):301–4.
- Corbridge, Stuart and John Harriss. 2008. *Reinventing India: Liberalization, Hindu Nationalism, and Popular Democracy*. Cambridge: Polity.
- Datta, Saikat. 2017. "The End of Privacy: Aadhaar is Being Converted into the World's Biggest Surveillance Engine." *Scroll.in*, March 24. Retrieved July 4, 2019 (<https://scroll.in/article/832592/the-end-of-privacy-aadhaar-is-being-converted-into-the-worlds-biggest-surveillance-engine>).
- Dixit, Pranav. 2017. "India's National ID Program May Be Turning the Country into a Surveillance State." *BuzzFeed News*, April 4. Retrieved July 4, 2019 (<https://www.buzzfeednews.com/article/pranavdixit/one-id-to-rule-them-all-controversy-plagues-indias-aadhaar>).
- Elias, Juanita. 2006. "The Gendered Political Economy of Control and Resistance on the Shop Floor of the Multinational Firm: A Case-Study from Malaysia." *New Political Economy* 10(2):203–22.
- Foucault, Michel. 1991. "Governmentality." Pp. 87–104 in *The Foucault Effect: Studies in Governmentality with Two Lectures by and an Interview with Michel Foucault*, edited by G. Burchell, C. Gordon and P. Miller. Chicago: University of Chicago Press.
- Foucault, Michel. 1979. *Discipline and Punish: The Birth of the Prison* (translated from the French by A. Sheridan). London: Penguin.
- Foucault, Michel. 1978. *History of Sexuality, Volume 1: An Introduction*. New York: Pantheon.
- Freeman, Carla. 2000. *High Tech and High Heels in the Global Economy: Women, Work and Pink-Collar Identities in the Caribbean*. Durham, NC; London: Duke University Press.
- Government of Tamil Nadu. 2015. *Tamil Nadu Global Investors' Meet 2015: IT & ITes Sector Profile*.
- Harcourt, Wendy. 2009. *Body Politics in Development: Critical Debates in Gender and Development*. London: Zed.
- Heeks, Richard. 1996. *India's Software Industry: State Policy, Liberalization and Industrial Development*. New Delhi; London: SAGE.
- Khera, Reetika. 2019. "Aadhaar and Privacy." Pp. 72–85 in *Dissent on Aadhaar: Big Data meets Big Brother*. Hyderabad: Orient BlackSwan.
- Kumar, Nagesh. 2005. "Indian Software Industry Development: National and International Perspectives." Pp. 93–130 in *ICTs and Indian Economic Development: Economy, Work, Regulation*, edited by A. Saith and M. Vijayabaskar. New Delhi; London: Sage.
- Kunda, Gideon. 1992. *Engineering Culture: Control and Commitment in a High-Tech Corporation*. Philadelphia: Temple University Press.
- Lyon, David. 2009. *Identifying Citizens: ID Cards as Surveillance*. Cambridge and Malden, MA: Polity Press.

- Lyon, David. 2001. *Surveillance Society: Monitoring Everyday Life*. Buckingham; Philadelphia: Open University Press.
- Magnet, Shoshana Amielle. 2011. *When Biometrics Fail: Gender, Race, and the Technology of Identity*. Durham, NC: Duke University Press.
- Maringanti, Anant. 2009. "Sovereign State and Mobile Subjects: Politics of the UIDAI." *Economic and Political Weekly* 44(46):35–40.
- Nair, Vijayanka. 2019. "Governing India in Cybertime: Biometric IDs, Start-Ups and the Temporalized State." *South Asia: Journal of South Asian Studies* 42(3):519–36.
- Nair, Vijayanka. 2018. "An Eye for an I: Recording Biometrics and Reconsidering Identity in Postcolonial India." *Contemporary South Asia* 26(2):143–56.
- National Association of Software and Services Companies. 2018. *Catalyzing the Ecosystem for a Trillion Dollar Digital Economy*. February 20. Retrieved April 10, 2018 (<http://www.nasscom.in/sites/default/files/NASSCOM-annual-guidance-fy-2018.pdf>).
- National Skills Registry. "About Us." Retrieved July 7, 2019 (<https://nationalskillsregistry.com/aboutus.htm>).
- National Skills Registry. "Companies / FAQs." Retrieved February 22, 2018 (<https://nationalskillsregistry.com/faq-for-companies.htm>).
- National Skills Registry. "Companies / NSR Benefits." Retrieved February 23, 2018 (<https://nationalskillsregistry.com/companies-nsr-benefits.htm>).
- National Skills Registry. "Homepage." Retrieved July 6, 2019 (<https://nationalskillsregistry.com>).
- National Skills Registry. "Knowledge Professional / Background Verification." Retrieved July 6, 2019 (<https://nationalskillsregistry.com/background-verification.htm>).
- National Skills Registry. "Knowledge Professional / Participate in NSR." Retrieved July 6, 2019 (<https://nationalskillsregistry.com/companies-participating-in-nsr.htm>).
- National Skills Registry. "National Skills Registry / NSR Context." Retrieved July 5, 2019 (<https://nationalskillsregistry.com/nsr-context.htm>).
- National Skills Registry. "National Skills Registry (NSR) Tour for Subscriber Companies." Retrieved July 7, 2019 (<https://nationalskillsregistry.com/doc/nsrtour-subscribercompanies.pdf>).
- Nayar, Pramod K. 2012. "'I Sing the Body Biometric': Surveillance and Biological Citizenship." *Economic and Political Weekly* 47(32):17–22.
- Nilekani, Nandan and Viral Shah. 2015. *Rebooting India: Realizing a Billion Aspirations*. New Delhi: Penguin.
- Ong, Aihwa. 2006. *Neoliberalism as Exception: Mutations in Citizenship and Sovereignty*. Durham, NC: Duke University Press.
- Ong, Aihwa. 1987. *Spirits of Resistance and Capitalist Discipline: Factory Women in Malaysia*. Albany, NY: State University of New York Press.
- Parthasarathy, Balaji. 2005. "The Political Economy of the Computer Software Industry in Bangalore, India." Pp. 199–230 in *ICTs and Indian Economic Development: Economy, Work, Regulation*, edited by A. Saith and M. Vijayabaskar. New Delhi; London: Sage.

- Patibandla, Murali, Deepak Kapur and Bent Petersen. 2000. "Import Substitution with Free Trade: Case of India's Software Industry." *Economic and Political Weekly* 35(15):1263–70.
- Prasad-Aleyamma, Mythri. "Cards and Carriers: Migration, Identification and Surveillance in Kerala, South India." *Contemporary South Asia* 26(2):191–205.
- Ramanathan, Usha. 2010. "A Unique Identity Bill." *Economic and Political Weekly* 45(30):10–14.
- Rao, Ursula. 2018. "Biometric Bodies, or How to Make Electronic Fingerprinting Work in India." *Body & Society* 24(3):68–94.
- Rao, Ursula. 2013. "Biometric Marginality: UID and the Shaping of Homeless Identities in the City." *Economic and Political Weekly* 48(13):71–7.
- Rao, Ursula and Vijayanka Nair. 2019. "Aadhaar: Governing with Biometrics." *South Asia: Journal of South Asian Studies* 42(3):469–81.
- Rautray, Samanwaya. 2019. "SC Notice on Plea Challenging Law on Private Entities using Aadhaar." *The Economic Times*, November 23. Retrieved December 10, 2019 (<https://economictimes.indiatimes.com/news/politics-and-nation/sc-notice-on-plea-challenging-law-on-private-entities-using-aadhaar/articleshow/72192940.cms>).
- Rose, Nikolas. 1999. *Powers of Freedom: Reframing Political Thought*. Cambridge: Cambridge University Press.
- Salzinger, Leslie. 2000. "Manufacturing Sexual Subjects: 'Harassment', Desire and Discipline on a Maquiladora Shopfloor." *Ethnography* 1(1):67–92.
- Sarkar, Swagato. 2014. "The Unique Identity (UID) Project, Biometrics and Re-Imagining Governance in India." *Oxford Development Studies* 42(4):516–33.
- Sethi, Aman. 2017. "Right to Privacy: Data Shows States using Aadhaar to Build Profiles of Citizens." *The Hindustan Times*, August 25. Retrieved July 4, 2019 (<https://www.hindustantimes.com/india-news/despite-govt-denials-states-building-databases-for-360-degree-profiles-of-citizens/story-qnSLHGyZIXiZiO4ce84UuO.html>).
- Shakthi, S. 2018. "What Makes a Modern Indian Profession? Corporate Policies and Middle-Class Subjectivities in Chennai's Information Technology Industry." PhD dissertation, Pembroke College, University of Cambridge.
- Shukla, Ravi. 2010. "Reimagining Citizenship: Debating India's Unique Identification Scheme." *Economic and Political Weekly* 45(2):31–6.
- Shukla, Sandeep. 2018. "Aadhaar Verdict: Why Privacy Still Remains a Central Challenge." *The Economic Times*, September 27. Retrieved July 5, 2019 (<https://economictimes.indiatimes.com/news/politics-and-nation/aadhaar-verdict-why-privacy-still-remains-a-central-challenge/articleshow/65970934.cms>).
- Solanki, Aakash. "Management of Performance and Performance of Management: Getting to Work on Time in the Indian Bureaucracy." *South Asia: Journal of South Asian Studies* 42(3):588–605.
- Surabhi. 2017. "Aadhaar has Helped Govt Save \$9 b from Being Lost to Fraud, Wastage: Nilekani." *The Hindu Business Line*, October 13. Retrieved February 15, 2018 (<https://www.thehindubusinessline.com/news/aadhaar-has-helped-govt-save-9-b-from-being-lost-to-fraud-wastage-nilekani/article9902030.ece>).
- Thaker, Aria. 2018. "The New Oil: Aadhaar's Mixing of Public Risk and Private Profit." *The Caravan*, May. Retrieved June 1, 2018 (<https://caravanmagazine.in/reportage/aadhaar-mixing-public-risk-private-profit>).

Unique Identification Authority of India. "About your Aadhaar: What is Aadhaar." Retrieved July 6, 2019 (<https://uidai.gov.in/my-aadhaar/about-your-aadhaar.html>).

Unique Identification Authority of India. "Frequently Asked Questions: Your Aadhaar–Aadhaar Features, Eligibility." Retrieved July 6, 2019 (<https://uidai.gov.in/286-faqs/your-aadhaar/aadhaar-features,-eligibility.html>).

Upadhyay, Carol and A. R. Vasavi. 2006. *Work Culture and Sociality in the Indian IT Industry: A Sociological Study*. Final Report submitted to Indo-Dutch Program for Alternatives in Development. Bangalore: National Institute for Advanced Studies.

NOTES

1. I am grateful to Professor Pier Giorgio Solinas for organizing the panel at ECSAS in 2018 that provided the initial impetus to write this article, and the other participants for their feedback and comments. I would also like to thank the three anonymous reviewers for their suggestions. I must, of course, thank my respondents for their time and generosity.
2. Unique Identification Authority of India. "About your Aadhaar": <https://uidai.gov.in/my-aadhaar/about-your-aadhaar.html>.
3. Surabhi (2017): <https://www.thehindubusinessline.com/news/aadhaar-has-helped-govt-save-9-b-from-being-lost-to-fraud-wastage-nilekani/article9902030.ece>.
4. National Association of Software and Services Companies.
5. Here, I refer primarily to the sectors of the industry devoted to software development, testing, support and maintenance, as well as to knowledge process outsourcing work, which constituted the main sites of my study. My study did not include the segments of the industry focused on call center support and related back office services.
6. The 2018 ruling by the Indian Supreme Court on the constitutionality of the Aadhaar Act decreed that private corporations should not be given access to Aadhaar data. However, new laws passed in 2019 have allowed companies to use Aadhaar for authentication, provided individuals give their consent. At the time of writing, the constitutional validity of the new legislation is being challenged in the Supreme Court. See Rautray (2019): <https://economictimes.indiatimes.com/news/politics-and-nation/sc-notice-on-plea-challenging-law-on-private-entities-using-aadhaar/articleshow/72192940.cms>.
7. Moreover, one of the registrars authorized to collect residents' data for Aadhaar is a central securities depository known as the NSDL, a subsidiary of which manages the NSR database for NASSCOM.
8. For a detailed analysis of how the mechanics of biometric identification itself can be fallible, see Magnet (2011).
9. Salzinger (2000) demonstrates in her study of a Mexican maquiladora that sexual desire, and the consequent sexualization of surveillance, became an actual "force of production" that was embedded in the factory's relations of power.
10. Concerns over privacy and surveillance have also attracted a significant amount of interest in popular writing. See Shukla (2018): <https://economictimes.indiatimes.com/news/politics-and-nation/aadhaar-verdict-why-privacy-still-remains-a-central-challenge/articleshow/65970934.cms>; Datta (2017): <https://scroll.in/article/832592/the-end-of-privacy-aadhaar-is-being-converted-into-the-worlds-biggest-surveillance-engine>; Dixit (2017): <https://www.buzzfeednews.com/article/pranavdixit/one-id-to-rule-them-all-controversy-plagues-indias-aadhaar>; Sethi (2017): <https://www.hindustantimes.com/india-news/despite-govt-denials-states-building-databases-for-360-degree-profiles-of-citizens/story-qnsLHGyZIXiZiO4ce84UuO.html>.

11. See Corbridge and Harriss (2008) for an analysis of the impact of the 1991 economic reforms on the Indian economy.
12. National Skills Registry. "Homepage": <https://nationalskillsregistry.com>.
13. In India, a PAN, or Permanent Account Number, is a unique identifier issued by the Indian government's Income Tax Department to tax-paying individuals or entities for financial transactions. Those in possession of a PAN number are given a PAN card, which is considered a valid identity document.
14. There are several of these verification centers in every city with a major IT presence; some companies also have their own POS booths within their premises.
15. The registration fee is currently Rs.400. It is expected that employees will then pay a further Rs.100 every year to renew their membership, although this is not enforced.
16. Registered employees can only view their own profiles and do not have access to other registrants' information. An employer can view the profiles of registered employees at their own company, as well as the profiles of other IT professionals who have granted them access (which might happen, for example, if they are hoping to procure a job at the authorized company).
17. All respondents have been given pseudonyms.
18. The Chola dynasty was at its peak between the tenth and twelfth centuries CE, when it ruled large parts of South India, as well as regions in neighboring countries, such as Sri Lanka, and was known for its military might.
19. Executives themselves can, at times, feel surveilled. Sriram, an executive at a major ITES company, while speaking to me about his company's diversity initiatives, reflected on how his own diversity-related actions were constantly being watched and judged by his employees: "I am sitting in [my office] like I am a zoo exhibit, except for that kind of opaque stuff [indicates the frosted glass wall]. I'm exhibit number one."
20. National Skills Registry. "Companies / NSR Benefits": <https://nationalskillsregistry.com/companies-nsr-benefits.htm>.
21. National Skills Registry. "Companies / NSR Benefits": <https://nationalskillsregistry.com/companies-nsr-benefits.htm>.
22. National Skills Registry. "Knowledge Professional / Background Verification": <https://nationalskillsregistry.com/background-verification.htm>.
23. The NSR website refers to this as the "menace of bloated resume" [sic] and 'CV faking'. See National Skills Registry. "Companies / FAQs": <https://nationalskillsregistry.com/faq-for-companies.htm>.
24. National Skills Registry. "Knowledge Professional / Participate in NSR": <https://nationalskillsregistry.com/companies-participating-in-nsr.htm>.
25. As Cohen (2019; 2017) has argued, "de-duplication," rather than service delivery itself, is the central aim of Aadhaar.
26. Unique Identification Authority of India. "Frequently Asked Questions": <https://uidai.gov.in/286-faqs/your-aadhaar/aadhaar-features,-eligibility.html>.
27. National Skills Registry. "National Skills Registry / NSR Context": <https://nationalskillsregistry.com/nsr-context.htm>.
28. It is interesting to note that while concerns over the leakage or misuse of Aadhaar data have attracted both media and scholarly attention, the stated purpose of the NSR is to prevent precisely this sort of data breach for clients.
29. At the time of writing, the Personal Data Protection Bill, a proposed piece of legislation that would provide a legal framework for data privacy and security in India, was being discussed in Parliament.
30. These are the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, notified under the Information Technology Act, 2000.

31. National Skills Registry. "National Skills Registry (NSR) Tour for Subscriber Companies": <https://nationalskillsregistry.com/doc/nsrtour-subscribercompanies.pdf>.
 32. The NSR website states that the industry has agreed to extend the NSR to the country's banking and finance sectors. See National Skills Registry. "About Us": <https://nationalskillsregistry.com/aboutus.htm>.
 33. The National Crime Records Bureau has recently issued a tender to launch the National Automated Facial Recognition System. The aim of this project is to combat crime and collect evidence by collating facial images from a range of sources, including government agencies, CCTV footage and newspapers.
-

ABSTRACTS

Supporters of Aadhaar, the unique identification scheme that aims to use biometric information and a 12-digit number to catalogue every Indian resident, have often commented on the tremendous amount of "fraud" that this program has curtailed since its introduction nearly a decade ago. Four years before the first Aadhaar number was issued, this discourse of ensuring authenticity was similarly deployed by the Indian information technology (IT) industry's employer association, NASSCOM, which inaugurated its own unique identification project to verify potential and current employees. Known as the National Skills Registry (NSR), this database utilizes biometric identification to create individual profiles of IT employees, each of whom is assigned a unique number called an ITPIN.

In this paper, I draw on interview and observation data collected during nine months of fieldwork in Chennai's IT industry, as well as a detailed analysis of industry reports and documents, to dissect employee and corporate narratives on the NSR. I interrogate the overarching discourse of employee "integrity" operating within the industry to deconstruct the myth-making, misconceptions and self-disciplining generated by the existence of this database. As a result, I provide a comparative framework through which to conceptualize Aadhaar's implications for safeguarding individual privacy, while also commenting on the power of private players under neoliberal capitalism and the increasing ubiquity of surveillance strategies in the lives of Indian residents.

INDEX

Keywords: Aadhaar, India, biometrics, surveillance, IT industry, integrity

AUTHOR

S. SHAKTHI

Department of Humanities and Social Sciences, Indian Institute of Technology Madras