International Journal of Communication 12(2018), 1228–1247 1932–8036/20180005

The Poverty of Privacy: Understanding Privacy Trade-Offs From Identity Infrastructure Users in India

JANAKI SRINIVASAN[1]
International Institute of Information Technology, Bangalore, India

SAVITA BAILUR
EMRYS SCHOEMAKER
Caribou Digital, UK

SARITA SESHAGIRI
Independent researcher, India

What trade-offs in privacy do low-income people make in dealing with state identity systems, and on what basis? We examine perspectives on Aadhaar, a national identification system for Indian residents that assigns a 12-digit number based on biometric identifiers. We draw on qualitative interviews with low-income respondents (*N* = 150) in six sites spanning three Indian states. In their encounters with state identity systems, respondents weigh their privacy concerns against their need to be seen by the state and in light of their previous interactions with the state. They negotiate their privacy practices by gauging what they are offering their data in exchange for and whether the rationale for data collection resonates with them. In parallel, they use their previous interactions with the state to make decisions about when to be visible to the state and when they value their privacy more and in evaluating whether information collectors and their tools are credible. Finally, we find preliminary indications that respondents harbor unique privacy concerns around the networked nature of identity systems such as Aadhaar.

Keywords: networked privacy, India, biometrics, identity systems

Janaki Srinivasan: janaki.srinivasan@iiitb.ac.in
Savita Bailur: savita@cariboudigital.net
Emrys Schoemaker: emrys@cariboudigital.net
Sarita Seshagiri: saritasworld@gmail.com
Date submitted: 2017–02–08

[1] We thank Omidyar Network and Caribou Digital for funding this research. We also thank Ananya Basu, Harish Boya, Monish Khetrimayum, Nazifa Ahmed, Rajiv Mishra, and Supriya Dey for their extensive contributions to the fieldwork and analysis for this research project.

I am a census inquisitor.
I travel about from door to door,
From house to house, from store to store,
With pencil and paper and power galore.
I do as I like and ask what I please.
Down before me you must get on your knees;
So open your books, hand over your keys,
And tell me about your chronic disease.
—*The New York Sun*, 1890, cited in Solove (2006, p.500)

Even if you want to be forgotten, the state is not willing to forget you.
—Attorney General Rohatgi, Indian Supreme Court, May 2017 (Choudhary, 2017, para. 12)

Information collection and identity systems have long been critical for states and their residents. However, the above quotes suggest that these systems are entangled with privacy concerns. Questions of privacy have taken on new meaning with the recent and urgent need for identity infrastructures, including support for the World Bank's Principles on Identification (World Bank, 2017) and proposals in the last two decades to establish and revamp identity infrastructures in various countries, including the United Kingdom, the United States, South Africa, and India (Bhatia & Bhabha, 2017; Maringanti, 2009). Even the proponents of identification systems recognize that without "strong data protection laws, regulatory frameworks, and practices, identification systems may reduce trust and undermine individual rights to privacy and consent regarding the use of their personal information," with vulnerabilities and risks "heightened in an era of digital identification and big data" (World Bank, 2017, p. 5). The rising number of pending and recently passed data protection privacy legislations in the Global South provides another indication of the centrality of privacy (Banisar, 2016).

The debates around privacy and identity systems have frequently asked how low-income and other marginalized populations negotiate such systems (Bhatia & Bhabha, 2017; Gangadharan, 2015; Hosein, Hickok, & Chattopadyay, 2017; Jayaram, 2015; Khera, 2011; Madden, Gilman, Levy, & Marwick, 2017; Maringanti, 2009; Wyber et al., 2015). Often these are the people who most need benefits from the state, and to receive benefits, they must identify themselves (Eubanks, 2011; Maringanti, 2009; Sprague, Schulte, Black, & Eubanks, 2013). Are these people also more vulnerable to harm through their use or nonuse of such systems? More specifically, how are their privacy concerns shaped by the introduction of new, often networked digital identity infrastructures, particularly in the absence of a legal privacy framework?

We examine this question using the case of Aadhaar and other state-based identity infrastructures in India. A national identification system that assigns a unique 12-digit number to each Indian resident based on biometric identifiers, Aadhaar is the largest biometric database in the world, with more than 1.3 billion Aadhaar numbers already assigned. The system has been at the center of controversy since its inception, and recent attempts to make it mandatory for state welfare and other services have intensified these debates (Bhatia & Bhabha, 2017; Greenleaf, 2010; Hickok, 2013). Privacy is at the center of the many concerns raised by the robust debate around Aadhaar's operationalization in

India (Jayaram, 2015; Khera, 2017; Ramanathan, 2017).[2] Using qualitative interviews with 150 low-income individuals in three Indian states, we examine how people evaluate privacy concerns in their use of state identity infrastructures, including Aadhaar. We find people's decisions about privacy are shaped by their experiences transacting with the state, which then inform the trade-offs they are comfortable making and how they engage with new, networked identity infrastructures. We point to a need to reconsider notions of relational privacy in light of the networked nature of new identity systems.

Literature Review

Privacy, Networked Privacy, and the Indian Context

Solove (2006) argues that "Privacy is too complicated a concept to be boiled down to a single essence" (p. 485). Others point out that its cultural translation outside the West further complicates traditional conceptions of privacy, especially around evolving technologies (Ahmed, Hoque, Guha, Rifat, & Dell, 2017; Kumaraguru & Cranor, 2005). While an exhaustive review of the extensive privacy literature is not possible here, we note two debates within it: the focus on individuals and the absence of context in defining privacy. Traditionally, legal models of privacy in the United States have centered on individuals and have been translated to technical contexts through the frame of "personally identifiable information" (Cohen, 2012; Marwick & boyd, 2014). Paradigms of online privacy—including notice-and-consent, informed choice, and the creation of access-control lists on social media—are all based on individualistic conceptions of privacy and emphasize privacy as an individual right (Marwick & boyd, 2014; Nissenbaum, 2011). Critics of individual-centered models argue that privacy practices are highly culturally specific and contextual (Altman, 1977; Marwick & boyd, 2014, Nissenbaum, 2011). Additionally, recent critiques argue that more "collectivist" societies (Kumaraguru & Cranor, 2005) or ones that reuse or practice shared or mediated access to personal devices (Ahmed et al., 2017) can have different cultural conceptions of privacy vis-à-vis technology use than those suggested by individual-centered models. They may also focus on specific domains of activity: A study on attitudes toward privacy in India found that financial and communication privacy (listening in on calls) were the greatest concerns (Kumaraguru & Sachdeva, 2012).

Recognizing the contextual nature of privacy and associated harms is a useful step toward understanding privacy practices. However, defining or understanding social contexts is not straightforward, because contexts are "co-constructed by all present and shaped by the affordances of the social technology in play" (Marwick & boyd, 2014, p. 1063). If we understand privacy as a process of boundary management (Marwick & boyd, 2014; Petronio, 1991, 2002) and as an ongoing dynamic negotiation—"a series of strategies that individuals can deploy depending on how appropriate they are to a specific circumstance" (Marwick & boyd, 2014, p. 1054)—then an individual's ability to understand and present contextually appropriate information about him- or herself is critical to this negotiation. When context collapse breaks boundaries (boyd, 2002, 2008; Davis & Jurgenson, 2014; Marwick & boyd, 2011,

[2] Aadhaar has been widely debated in the mainstream Indian press. See Scroll's "Identity Project" series at https://scroll.in/topic/38792/identity-project. The debate on Aadhaar is also in the courts, with the July 2017 *Puttuswamy vs. Union of India* privacy judgment by the Indian Supreme Court highlighting the Aadhaar case.

2014), it is experienced as a violation of privacy (Marwick & boyd, 2014, p. 1054). Thus, the ability to manage the integrity of contextual boundaries is key to privacy (p. 1054) where contextual boundaries are determined by a combination of "audience, technical mechanisms, and social norms" (p. 1062).

To achieve privacy, individuals must be able to both understand and influence the context in which information is being interpreted, either "by co-constructing the architecture of the systems" or "by embedding meaning and context into the content itself" (Marwick & boyd, 2014, p. 1063). How do the introduction of networked ecosystems and their use among low-income users pose particular challenges to this goal? As we move to a networked ecosystem, where "contexts *regularly* blur and collapse" (Marwick & boyd, 2014 p. 1063, emphasis added), individuals may find it even harder to maintain privacy. *Networked privacy* refers to "the ongoing negotiation of contexts" (p. 1063) in networked systems such as Aadhaar.

Furthermore, identity infrastructures may be no exception to the historical exclusion of certain people by advancing technology (Ahmed et al., 2017; Jayaram, 2015; Sethia & Kher, 2016). After all, if those co-constructing the architecture of sociotechnical systems are the most likely to "achieve privacy," then those who are less likely to receive an opportunity to co-construct identity systems—such as low-income populations that are not part of designing them—might find it harder to achieve privacy.

For these reasons, Aadhaar is particularly pertinent for examining privacy in India. Aadhaar aims to eventually link distinct databases of individual identity to enable a single, coherent, state-owned identity platform, and it has already been described as a "networked government platform" (Sethia & Kher, 2016). Debates on the unique privacy challenges of networked systems are ongoing. Maringanti (2014) examines how individuals might be identified through "data convergence" (p.13) as data sets are overlaid by multiple agencies through "data travel" in an Intensive Household Survey. Bhatia and Bhabha (2017) summarize the concerns about "data creep" (p. 75) that have arisen over the linking of databases in various countries. We contribute the perspectives of Aadhaar users to this debate.

Privacy or Legibility?

We begin by looking "for the contours of familiar social activities and structures" (Nissenbaum, 2011, p. 43) in the networked state identity infrastructure. This involves taking into account the history and nature of state-citizen relations in understanding citizens' privacy concerns when interacting with state identity systems. More specifically, we argue that privacy for low-income populations operates in tension with their ongoing needs to become legible to the state.

If a modern state is one "whose ideology encompasses large-scale plans for the improvement of the population's welfare," then it "requires the capacity to locate citizens uniquely and unambiguously" (Scott, Tehranian, & Mathias, 2002, p. 10). The population, in turn, receives certain benefits by becoming legible to the state. As people who have been "watched by default," low-income populations in particular might be attuned to trading their details for welfare benefits (Gangadharan, 2015, p. 13; Sethia & Kher, 2016, p. 17). The routine use of such technologies can also normalize divulging details (Gangadharan, 2015, p. 13). Finally, although technologies such as a state's identity infrastructure can "see" all users, the marginalized find it harder to challenge what is being seen of them (Gangadharan, 2015, p. 14;

Hosein et al., 2017). Even where law, private companies, and technology might be able to provide relief from unfettered monitoring, this is typically achieved after a long wait (Brunton & Nissenbaum, 2011). In the meantime, these populations might have to rely on stealth and obfuscation (Benjamin, 2007, p. 545; Brunton & Nissenbaum, 2011) to resist being consistently visible to the state and to avoid privacy harms. All of these factors are further complicated with networked systems.

Despite a context that Gangadharan (2015) describes as "privacy poor, surveillance rich" (p.12) populations rarely remain constantly visible to the state. We examine how users negotiate their legibility to the state, and to other entities, within the constraints of existing identity systems. This allows us to explore how they think about privacy, when they find it critical, and how they partially protect themselves from privacy harms (Sethia & Kher, 2016, p. 18), especially in view of increasingly networked identity systems.

Methods

To understand how low-income populations think about privacy in the use of identity systems, we talked to 30 expert informants on identity systems worldwide, conducted 150 interviews of about an hour each with users of identity credentials, and observed 30 identity-based transactions in the states of Assam, Delhi, and Karnataka—the states with the lowest, highest, and mid-level Aadhaar saturation percentages in India[3] and all with significant histories of migration, which has implications for identity. The study was conducted between November 2016 and May 2017. In each state, our interviews were split between urban, periurban, and rural sites. Respondents were recruited from public spaces, especially markets and commonly used venues for identity enrollment and transactions such as driving license offices, Aadhaar enrollment centers, and village-level administrative offices. We used snowball sampling to recruit additional respondents. The occupational profile of respondents included street vendors, domestic helpers, factory workers, auto drivers, and security guards. A team of eight researchers followed a semistructured guide to interview respondents mainly in Hindi, Kannada, and Assamese (and sometimes in Bengali, Sylheti, Telugu, and Tamil). Interviews took place at the venues where respondents were recruited and, occasionally, at their residences.

Through the interviews, we tried to understand how people obtained and used IDs. Whereas studies on networked privacy typically focus on the information processing and information dissemination stages from Solove's (2006) taxonomy of privacy, given the centrality of the collection phase to state identity systems, we also examined how privacy concerns were evaluated at the information collection stage. To explore issues about privacy, we used a variety of techniques, including asking respondents whether they had ever lost their IDs and the implications of such a loss; whether they worried that their IDs could be misused and how; and how much they knew or cared about who handled and maintained their details for an ID system. In general, respondents were open and willing to talk (especially once we showed our credentials as academic researchers). However, when we asked one respondent if he was

[3] As of April 15, 2017, Delhi led the list (119%), Karnataka was 20th (94%), and Assam was last (7%). The relative positions of the states stayed the same in December 2017, though the saturation percentages had changed (see Unique Identification Authority of India, 2017).

worried about sharing his details with the government, he answered, "Well, I don't know you, and you are also asking me all these questions. I don't know what you will do with it."

We faced two major challenges in discussing privacy. The first was translating the concepts of identity and privacy from English to other languages. Further, questions about privacy never allowed a soft entry for discussions. Second, the interviews delved into such intangible concepts that we sometimes had to ask hypothetical questions that not only introduced discomfort in the rapport between interviewer and interviewee but, occasionally, fears ("Does this mean I should be worried about my data?"). Although asking hypothetical questions often worked to elicit responses, it also meant that our research team had to introduce and explain privacy to respondents, possibly skewing responses.

Findings

Overall, we found that low-income populations care about privacy in their encounters with the state, but this concern is weighed against their need to be seen by the state and tempered by their previous interactions with it. Instead of starting with the binary of "I care about privacy" or "I do not care about privacy," respondents mentioned several reasons they arrived at their privacy concerns and practices, including:

- I will get something in return.
- It is for our own safety.
- I don't have any money anybody could take.
- I don't have anything to hide.
- The computer is safer than paper records.
- I can't do anything about it anyway.
- I don't know about it (I'm not educated).
- I don't want to know about it.
- At least the government is better than the private sector.

We now examine how respondents arrived at this list. Although we include quotes from only a few respondents, the themes and instances we emphasize resonated across all interviews.

Relationship With One's Data

How do people relate to their data, and in what ways do they value its privacy? Respondents valued privacy less when it was related to personally identifiable information or their "data" and valued it more when they could link privacy to cultural norms and the harms caused by their transgression. This meant they valued different types of data (financial, health, address, photographs, etc.) differently because the cultural norms associated with the use of each were different. Further, respondents were more concerned about losing their ID cards than about the data on their cards: They knew from past experience what the loss of an ID would entail, whereas the consequences of the loss or misuse of data were unclear.

When we asked Mansoor,[4] a street trader of woolens at a Bangalore market, whether anyone had ever misused his data, he appeared amused. He said, "No. I have nothing with me. What will they make me do? If it were someone with a house or a car . . . then they could do that. But we have nothing." Mansoor believes that people with greater assets would have more reason to be concerned. Devi, a peanut seller in front of a Bangalore temple, also linked the value of data to levels of individual wealth. When asked whether he had ever worried about losing his ID, he responded:

> I don't understand how anyone else could misuse it. And that's why I was quiet. But if it is a rich person who has lost his ID, it will matter a lot to him and his money. If a poor man's ID, like my ID, is lost, it doesn't matter that someone else at the most will get to know my address and where I live and come and find me. I have nothing to lose. I have no money.

Overall, Mansoor, Devi, and many others linked the value of their identification credentials to their financial status: If they had wealth, their data and privacy would have greater value. They did not view the identification data itself as valuable, but rather that the loss of control over it might compromise personal wealth.

However, when they described the harms that might arise from privacy breaches involving the exposure of information that broke cultural norms, respondents from similar economic backgrounds placed greater value on their data and its privacy. Ganga, a craftswoman from Rajasthan at a crafts bazaar in Delhi who wore a *ghunghat* (veil), and her son, Rahul, spoke about their discomfort in having to share their photographs and addresses to get an Aadhaar card made. Rahul felt that

> Photographs should not be open like this in these IDs. . . . Even the wife of our village head wears a ghunghat in front of him. Other women also wear the ghunghat in front of their men and other men. There is no problem with names and other details being shared. But now everyone gets to see everyone's photograph by way of ID cards.

Ganga added, "There is a difference when you see someone face-to-face and now you see their photo on the cards." Rahul continued, "We feel that this photograph should not be seen. Address is okay. It can be any address." For Ganga and others, the display of a photograph was perceived to breach cultural norms around gender and cause privacy harms.

Finally, another view on the value of data and privacy was expressed by respondents who believed that only people who had something to hide needed to worry about privacy. The elected president of a resident welfare association in a refugee settlement colony in Delhi offered that only those who were "up to some mischief" would think twice about getting an Aadhaar made or about posting on social media. For him, no one other than these "antisocial elements" had anything to worry about. This framing of the "nothing to hide" argument from an elected representative follows a narrow understanding of privacy that, "in the end, has nothing to say" (Solove, 2011, p. 32). Although it is not uncommon for

[4] All respondent names are pseudonyms.

mass personal data collection to be justified in these terms, none of the other respondents suggested that privacy is only for those "up to some mischief."

Relationship With One's ID Cards

Respondents attached much greater value to the physical ID cards than to the privacy of their data when framed as personally identifiable information. Most ID cards (Aadhaar, voter ID, permanent allotment number [PAN] card) are kept safe at home, and respondents only carried photocopies.[5] Mansoor, the woolens trader, said he keeps all his IDs "underneath the mattress" once he is home. Similarly, Devi, the peanut seller in Bangalore, only carried laminated photocopies—a common practice. Additionally, because there is no legal requirement to report lost photocopies (whereas the loss of original cards must be reported), it is considered okay to lose photocopies. Nalin, a dairy shop owner in his 40s in Kesarpur, a working-class settlement in the periurban Delhi site, said he kept only his driver's license with him, leaving his Aadhaar card and ration card at home. When asked whether he kept the cards as safe as his money, he responded, "Yes, even more than that."

Jairam, a retired farmer, now owner of a small cycle shop in Garudahalli, a village north of Bangalore, said:

> It is difficult if any of these cards is lost. If it is lost, I will have to walk up and down to the *taluk* [a revenue administration division] office in Madhugiri [11 miles from Garudahalli]. There they will tell me something, and whatever they say has to be done. And then they will say, "Go and bring this and bring that. Do this and do that." All that is a problem. Losing any card is a problem.

In Kesarpur, Nalin confessed that the loss of his ID documents would pose the most problems, "because I have to run again to get the ID document made, I have to pay money, like for the Aadhaar card, again I would need to pay 200 rupees." A middle-aged auto driver in Delhi, Rohan, also drew on his experiences to explain what the loss of an ID entailed:

> Once I was robbed at night at knifepoint. Right here, at night. They snatched my license and everything in the process of snatching my money. I got a police complaint registered. Then the police called me on my number and said we found your IDs here, come fetch them.

Rohan believed that the police were in cahoots with the thieves and that is why they were able to find the IDs so quickly. When the police returned his IDs, Rohan says, "They were asking me to give them 200 rupees for drinks. I refused. Why should I pay them?" Rohan eventually got his IDs back without paying a bribe: "Yes, why not? I had registered a police complaint," he said indignantly.

---

[5] Permanent allotment numbers are issued by the Income Tax Department. They are used in filing taxes and also act as proof of name and address.

What is striking in this example is Rohan's simultaneous trust in the formal process and his lack of trust in its bureaucrats. Equally important is that he could precisely deconstruct what might have happened and what he could and could not get away with, based on his understanding of how processes worked. These granular understandings of their relationships with the state explain why respondents fear losing their ID cards, even as they appeared to worry much less about the loss of the details on their cards.

Relationships With Data Collectors and Their Tools

Respondents' need for privacy also was connected to the nature of the relationship with the data collector and the means of collection. Some placed their faith in the computer or in the card to safeguard them. Dhanraj in Kesarpur described how he received his Aadhaar card:

> I had to provide some proof of identity, like my voter ID or a bank passbook. And those who don't have any previous documents need to get a letter signed and stamped by their village head . . . acknowledging that she or he is a resident of the village for these many number of years.

When we asked Dhanraj whether he worried about these details falling into the wrong hands, he replied, "No, what can anyone do even if they have my information? There is a record of my fingerprints which is unique to me, so no one else will be able to misuse the information."

The faith in fingerprints as a unique identifier came up again in speaking with Rajesh Bhatia, a trader in his late 50s in a wholesale market in Delhi:

> Obviously, Aadhaar card is better than everything else. Because it goes with fingerprints. . . . For anyone to check identity in thoroughness, Aadhaar is at the top. Because everything else only has photo on it. Aadhaar has fingerprint also.

The material form of ID systems was thus an important component of how respondents gauged the credibility of information collection for that system and whether they anticipated privacy harms from it.[6]

For others, the issue of who collected their details was critical. A number of respondents felt differently about sharing personal information with the government than with private-sector organizations. For example, in Guwahati, Assam, Sheetal stated that she was very concerned about maintaining the privacy of her personal information. A teacher at a fashion institute, Sheetal had limited identity credentials—a PAN card and a passport. She stated she would be very concerned about sharing her personal information, especially health and financial information, with any identity system as a general principle. However, she confessed to being slightly more comfortable sharing it with the government than

[6] Other research, too, finds that the material form of government documents is critical to how bureaucrats and users evaluate them (Finn, Srinivasan, & Veeraraghavan, 2014; Hull, 2012; Srinivasan & Johri, 2013). However, none of this research focuses specifically on how material form may shape privacy concerns.

with private companies: "The government is always there, but private companies are like fire, they come and then they go." If a company collapsed, she would have no control over what would happen to her information.

Nalin in Kesarpur echoed Sheetal's sentiment: "I did my Aadhaar enrollment because the government was saying to get Aadhaar made. . . . I thought [my data] will be with the government." Respondents seldom knew where or how their data would be stored by the government or whom it might be shared with in the relatively new Aadhaar process. We heard refrains of "I do not know where my information goes" and that "nobody had told us what would happen with regard to access to my information." Nalin hazarded a guess: "I think it's with the bank people now, but when I did my first registration I thought it was with the enrollment people. But apart from this, I do not know where my information goes, what happens to it."

Nevertheless, most respondents differentiated between the government and the private sector and expressed greater confidence in sharing information with the former than the latter, which they justified in terms of the relative durability of the state as well as their previous encounters of submitting personal data in return for welfare (Corbridge, Williams, Srivastava, & Véron, 2005; Gangadharan, 2015).

Some respondents were resigned to sharing their details even when the collector did not particularly inspire trust. When asked whether he thought his details were safe with the government, Nalin responded, "No, I don't think it could be safe in the hands of government, given how the government works," at which point he and the people around him broke into laughter. He went on to clarify:

> They can do wrong things with someone, anything can happen; for example, someone can get access to someone else's data record by paying bribes to people who are doing Aadhaar-related work. Previously, the voter ID card had only had a black-and-white photo on it. But with Aadhaar card, there are biometrics that can be accessed by someone for doing something wrong. It is very dangerous, anyone can get it, anyone can pay money and get access to the data and information. That's why I am saying that it is not safe with the government. But I never tried to think too much about it, about what someone will do with my data and information.

A slightly different kind of resignation came from respondents who did not feel qualified to judge how secure their data was. Dhanraj, whom we met earlier, said that he did not

> know anything about who is using the information or where it has reached. I am busy maintaining my shop and I am also not well educated. . . . I left my studies and started working at the shop. In case you want more information, then you need to ask someone who is more educated, like someone who can operate computers.

These debates illustrate that the nature of the relationship with the data collector, and how the data were collected, shaped respondents' privacy concerns and their estimation of privacy harms. But in

the absence of a clear sense of the process, the reasons that the government offered for the data collection also appeared to be important for respondents.

Relationship With the Reasons for Data Collection

Suresh Singh, the owner of an Ayurvedic shop and Aadhaar enrollment center in Kesarpur, explained his thoughts about the collection of personal data:

> Yes, there is some amount of trepidation, and I have asked at times why so many different documents are required to make one card. And then I have been told that these are required for verification purposes. Once you know the reason, then your mind is at ease. It makes sense that one would need to verify one's address. One will obviously have to share details of where one lives; how will the other person verify otherwise? But if one doesn't have an address, then it becomes a challenge.

Like Suresh, many respondents appeared comfortable if the rationale for collecting data was personal or national security. In Kesarpur, ex–garment factory worker Rumina endorsed the need for collecting details from tenants:

> It definitely makes sense. For example, landlords keep tenants. Who knows what kind of people live as tenants? What if some tenant kills someone and runs away? With the Aadhaar card documentation, at least he'll be caught wherever he goes.

When we asked Rumina how someone could be caught by the Aadhaar card, she said "because all the details are in the computer" and that "Aadhaar has more meaning than the voter ID because it keeps a record of fingerprints. All the details of the person from photo to fingerprints are recorded in the Aadhaar ID." Rumina's husband, Asif, also a factory worker, said he had no issues providing these details since the "details that are recorded will be useful when doing a check on someone, where is a person from, where does the person stay, what kind of a person is he, and so on" and that such details would be useful in "catching criminals." Others, including auto driver Rohan in Delhi, mentioned Aadhaar as an effective way to keep "terrorists" in check.

We should note that none of the respondents provided concrete examples from their lives to back up their perceptions linking personal data and personal safety or national security. In fact, a few respondents added that identity systems are not foolproof. Rohan noted that terrorists are "very smart these days. They get fake passports. And our people [Indians] are also mixed up in getting them these." Rajesh Bhatia expressed a similar sentiment; in the context of Aadhaar being a secure ID because of fingerprints, he said, "But this is India—you get a duplicate for everything!" Despite these misgivings and a lack of examples from their own lives, the respondents appeared to echo popular justifications for data collection in safety and security.

Trade-Offs in Transactional Relationships

> For me all cards [are important]. . . . Whenever I need to register something or apply, they will ask me for my Aadhaar card. . . . I will say all my ID cards are important at one point or the other. It depends on what I need to use it for at a particular time. Now when I need to link my Aadhaar card to get ration, they will need my ration card too. And if I do not possess a voter's card, I cannot cast my vote. So there is nothing that is not needed or not important. It is really about when I will need it and who asks for it. (Sumana, garment factory worker, Kesarpur)

We noted earlier that respondents seemed resigned to providing their data to the state. Sumana, a widow and mother of two, provides an alternative explanation: For many, providing that data is the only way to receive state benefits. Aadhaar's quasi-mandatory status for many types of transactions, especially for public benefits, might be responsible for this widespread feeling. Others have pointed out that populations used to being under surveillance—in this case, for public benefits—may not even consider their personal details private in that context (Gangadharan 2015). The trade-offs are implicit. When asked about the documents he was asked for in obtaining his voter ID, farmer Jairam in Garudahalli responded: "They just went door to door and collected people's names, age, and then their photographs. People gave their details to them." Another respondent stated that when he was asked for personal details in an Aadhaar enrollment center, he shouted them across the counter because everyone else was doing so.

But we also observed various strategies that respondents employed to control what the state saw of them while negotiating for their benefits and how they managed their data to preserve their relationships. Devi, for instance, maintained several IDs spread across two states (his home state of Tamil Nadu and where he was selling peanuts, in Karnataka). He transacts with the state and various other actors in both states for loans and needs to prove his identity while he travels between them. Devi managed to obtain voter IDs and ration cards in both states, in addition to an Aadhaar, driver's license, and PAN card in Karnataka. Meanwhile, Biswaroop, a sari seller on a Bangalore street, wanted to be illegible to the state, and this approach backfired. He recounted a theft when he used to have a shop: "A woman [who used to come to clean] wiped our cash clean and went absconding." When we asked Biswaroop whether he had filed a complaint with the police, he retorted: "What is the point of complaining to the police? We didn't even have a trade license for that shop back then." Biswaroop worried that a visit to the police station would reveal the deficient paperwork on his shop and land him in more trouble than any benefits he might have gained from effective police action against the theft.

These questions of negotiating one's visibility in relation to the state only become further complicated in the case of networked systems, which we turn to next.

Data, Relationships, and Privacy

The privacy of relationships is as complex as the privacy of artifacts such as IDs, and we saw this type of privacy actively protected. Mansoor, the woolens vendor in Bangalore, did not mind sharing his Aadhaar card, but he would not share the pocket diary where he kept track of his lending and borrowing.

He was keen to safeguard the privacy of his relationship and the identity of his moneylender, because he said he has known him for several years and did not want anything untoward to happen.

Respondents also described how they protected their relationships by transposing the established norms of boundary management when they moved or started using new technologies. For Ganga, the experience of having her photograph taken for a ration card constituted a break from her norms of privacy (vis-à-vis wearing a veil and avoiding contact with men):

> Once we took off our ghunghat, we let only women take our photographs. Say someone like you who is sitting at the photo studio, we will have our photographs taken by her. Not by men sitting there. See, it is a single room. Men will not be allowed inside. So we sit there and a woman takes our photographs.

Ganga's son, Rahul, said the men at the center also did not aid Ganga with recording fingerprints for Aadhaar enrollment: "Women themselves will press their fingers on the machine. Men don't touch them." About being asked for her personal ID details at the time of Aadhaar enrollment, Ganga said:

> At that time, when I was asked to mention my details, my husband was with me. I was not alone. So he gave his mobile number and our address. He handled it. I did not have to answer all those queries.

She added:

> See, even here on my card [business card], which I have given you . . . it has my son's mobile number and contact. And on this side, it has my husband's contact details. Nowhere is my mobile number mentioned. My mobile number [showing a feature phone] is only for my children. My phone is just for the family. My number is not for public.

Ganga describes how she manages the visibility of her personal information according to changing contexts. The need to have her photograph taken is part of a "new" system that she associates with urban norms that stand in contrast to her village-based norms, including the use of veils and rules of contact between men and women. Once Ganga got a phone, she transposed some of these norms by restricting her phone number to her family. During the Aadhaar enrollment process, she managed by being photographed by a woman and by having her husband give out his details rather than hers. In this way, Ganga's account highlights how she decides what information to share with whom to protect her relationships in her home community, even as she deals with new technologies and state processes.

My Networked Data and Privacy

> I have a PAN card to pay taxes, a voter ID card to vote, a bank card for the ATM, a ration card for the public distribution system. Why do I need Aadhaar? Why do I need to link them together? What does the government want? (Dilip, juice shop owner, Shillong, Meghalaya)

Dilip's query (and Sumana's quote earlier) reveal that he understands his relationship with the state as constituted through multiple systems and institutions rather than a monolithic, singular entity. In this context, what potential privacy harms might arise from the deployment of networked identity systems? In this final section of our findings, we examine how individuals' privacy practices and their capacity to manage how the state sees them are further complicated when identity systems are conceptualized as a network. Such identity systems can challenge the ability of Mansoor, Ganga, and Rahul to achieve privacy the same way they did before. The data relationships entailed in networked identity systems test the relational nature of privacy described so far and push us to think about the links between relational and "networked privacy."

Jafar, a coordinator at a migrants' rights center in Kesarpur, expressed concern about the surveillance potential of a networked ID system:

> For example, I'm getting messages from the bank to link my Aadhaar card to the account, but I haven't done it yet. The government has made it compulsory in many places, so this scares me a little. For me, this card is a tracking device. When someone asks me for the ID and specifically Aadhaar, I always ask what other proof can work.

Jafar, who is an activist and is security-conscious, illustrates specific concerns and mitigation measures for dealing with networked identity systems. However, it is difficult to establish how systems are networked and who is able to access what details, making networked identity systems—and individuals' perceptions about them—hard to comprehend. Indeed, few respondents were aware of the networked nature of identity systems such as Aadhaar. Nevertheless, we attempted to understand respondents' concerns about the privacy harms of such a networked environment. We asked how they would feel about credential systems in which information shared as part of one relationship would be shared with other parts of the state—a key element of identity systems such as Aadhaar, which create relationships between data in different systems. Because the networking of Aadhaar with other systems is still being rolled out, we asked respondents about *potential* harms that might arise from the networking of data, including the collapse of contexts in which specific identities exist (e.g., health and finance).

We asked women respondents to identify the sensitive data they were concerned to protect and relationships in which those data were currently shared. We then explored attitudes toward the networking of the data and the very small risk of the data leaking out. Ayesha, a community health worker who lived on the shifting Chars (sandbanks) on the Brahmaputra River in northeast India, noted, "Pregnancy is very sensitive, especially for the fourth or fifth pregnancy. People are ashamed. They tell their doctor but keep it private from their community until maybe the sixth month." Ayesha speculated that if Chars-dwelling women knew that using a single identity credential with the doctor might mean that information held by the doctor was linked to information held by people in different contexts, they might be reluctant to share the information with the doctor at all. Yet, as a health worker, Ayesha also said she understands the value of sharing this information.

Ayesha's example shows how awareness of the networked nature of an identity credential and the possibility that it may break the integrity of relationally defined contextual boundaries were perceived

as a risk with implications for women's use of medical advice. Although these findings are speculative, given that Aadhaar's networking is recent and ongoing, they highlight the importance of an individual's capability to manage the sharing of information in specific contexts and of maintaining contextually specific, relationally defined privacy practices. Networked platforms erode this capability by shifting agency away from the individual toward the platform and those that control the platform, including both the state and other entities.

Discussion and Conclusion

This article frames the privacy concerns of Aadhaar users through a contextual and networked privacy lens that takes into account power differentials and user agency. Contrary to suggestions that some cultures and specific populations, including low-income demographics, do not value privacy,[7] our examples reveal that privacy is indeed valued. This becomes especially apparent once our questions are reframed in terms of privacy harms and by conceptualizing privacy as always relational, even when it is networked.

Privacy can only be understood in the context of the relations within which it operates; in the case described in this article, the most important component of this context, perhaps, is the population's relationship with the state. This includes their desire to negotiate when the state could "see" them and when it could not, whether by staying under the radar or by actively obfuscating how the state saw them. We observed this in Biswaroop's example, where he refused to visit the police station to lodge a complaint, and with Devi, who obtained multiple IDs with different credentials. At the same time, we do not wish to overstate the agency that respondents—particularly from the groups we interviewed—could exert. We found that the power dynamic between the state and users definitely circumscribed the extent to which users could decide to withhold data.

Because it is relational, we found that privacy is also relative: Rather than evaluating it as important or not, or as present or absent, the people we spoke with saw it as a more or less important concern traded off against multiple other concerns, including the maintenance of their relationships with their local community and the state. They also had different privacy concerns about different types of data (photographs were different than home address, which was different than health or financial details). Here, too, using a contextual understanding of privacy allowed us to discover how respondents thought about privacy, when they found it important, and in what ways they partially protected themselves from privacy harms (Sethia & Kher, 2016, p. 18).

In brief, then, respondents made decisions to provide their personal information in the context of and against the backdrop of their relations with the state but also with their community. This meant that their privacy concerns were (a) weighed against their need to be seen by the state and (b) tempered by their previous interactions with it and with other entities. With their need to be seen by the state, individuals gauged what they were offering their data in exchange for and whether the rationale for data

[7] A recent Supreme Court case that describes the desire for a right to privacy as an "elitist bias" is a good example (see Singh, 2017).

collection resonated. Their previous interactions with the state shaped how they made decisions to be visible to the state or to obfuscate their identity, how they valued their privacy, why they valued the physical ID cards over the details on them, their decisions to protect their relationships over their IDs, and even whether they saw their information collectors and their tools as credible.

Using a contextual analysis allowed us to understand how respondents arrived at decisions to share their information rather than categorizing their decisions as caring about privacy or not. This allows us to broaden the debate around privacy. Solove (2007), for example, has argued against the conception of privacy in terms of hiding information, arguing that such a view "myopically views privacy as a form of concealment or secrecy" (p. 764). One of the risks of taking this view of privacy is that it reduces the debate to a question of concealment and excludes the many alternative conceptions of privacy that have meaning and value. This would exclude from the debate around identification technologies many of the conceptions of privacy that less privileged users articulate as being meaningful and important.

Our final point is about privacy in networked systems. Following Marwick and boyd's (2014) account of privacy in relation to "the location of individuals in contexts and networks" (p. 1051), we adopted a lens of networked privacy to analyze how people drew on their relationships with the state when they encountered a new *networked* ID system whose workings they did not fully understand. Although the networking of identity systems is nascent at this time in India, we tried to understand how users were learning to manage the integrity of their contextual boundaries in their encounters with these technologies. We found that, within these networked contexts, control over what information is shared with whom shifted from the individual to the agency that controlled the network. Because attitudes toward the sharing of information and the use of identity credentials are informed by perceptions of control, as well as trust in the other party in the relationship, we found that this shift in control made people wary of systems that might erode the integrity of contextual boundaries. A relational understanding of privacy can help us better understand how people negotiate networked identity systems even as their agency to maintain contextual boundaries is potentially eroded.

The people who shared their experiences and perspectives with us described specific practices and concerns relating to the privacy implications of identity technologies that are becoming ubiquitous in everyday life. When reframed from individualist, personally identifiable information notions of privacy to relational, harms-based notions of privacy, those at the margins articulated very real concerns about the maintenance of agency over personal privacy.

References

Ahmed, S. I., Hoque, M. R., Guha, S., Rifat, M. R., & Dell, N. (2017). Privacy, security, and surveillance in the Global South: A study of biometric mobile SIM registration in Bangladesh. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (pp. 906–918). New York, NY: Association for Computing Machinery. doi:10.1145/3025453.3025961

Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific? *Journal of Social Issues*, *33*(3), 66–84.

Banisar, D. (2016). National comprehensive data protection/privacy laws and bills 2016. *SSRN.* doi:10.2139/ssrn.1951416

Benjamin, S. (2007). Occupancy urbanism: Ten theses. In M. Narula, S. Sengupta, J. Bagchi, & R. Sundaram (Eds.), *Sarai reader 07: Frontiers* (pp. 538–563). Delhi, India: Center for the Study of Developing Societies.

Bhatia, A., & Bhabha, J. (2017). India's Aadhaar scheme and the promise of inclusive social protection. *Oxford Development Studies*, *45*(1), 64–79.

boyd, d. (2002). *Faceted ID/entity: Managing representation in a digital world* (Master's thesis). Massachusetts Institute of Technology, Cambridge, MA.

boyd, d. (2008). Why youth heart social network sites: The role of networked publics in teenage social life. In D. Buckingham (Ed.), *Youth, identity, and digital media* (pp. 119–142). Cambridge, MA: MIT Press.

Brunton, F., & Nissenbaum, H. (2011). Vernacular resistance to data collection and analysis: A political theory of obfuscation. *First Monday*, *16*(5).

Choudhary, A. A. (2017, May 3). Citizens don't have absolute right over their bodies: Government. *The Times of India.* Retrieved from http://timesofindia.indiatimes.com/india/citizens-dont-have-absolute-right-over-their-bodies-government/articleshow/58486260.cms

Cohen, J. (2012). Configuring the networked citizen. In A. Sarat, L. Douglas, & M. M. Umphrey (Eds.), *Imagining new legalities: Privacy and its possibilities in the 21st century* (pp. 129–154). Stanford, CA: Stanford University Press.

Corbridge, S., Williams, G., Srivastava, M., & Véron, R. (2005). *Seeing the state: Governance and governmentality in India*. Cambridge, UK: Cambridge University Press.

Davis, J. L., & Jurgenson, N. (2014). Context collapse: Theorizing context collusions and collisions. *Information, Communication & Society*, *17*(4), 1–10. doi:10.1080/1369118X.2014.888458

Eubanks, V. (2011). *Digital dead end: Fighting for social justice in the information age.* Cambridge, MA: MIT Press.

Finn, M., Srinivasan, J., & Veeraraghavan, R. (2014). Seeing with paper: Government documents and material participation. In *Proceedings of the 47th Hawaii International Conference on System Sciences* (pp. 1515–1523). Washington, DC: IEEE Computer Society. doi:10.1109/HICSS.2014.195

Gangadharan, S. P. (2015). The downside of digital inclusion: Expectations and experiences of privacy and surveillance among marginal Internet users. *New Media & Society*, *19*(4), 1-19. doi:10.1177/1461444815614053

Greenleaf, G. (2010). India's national ID system: Danger grows in a privacy vacuum. *Computer Law and Security Review*, *26*, 479–491. doi:10.1016/j.clsr.2010.07.009

Hickok, E. (2013). Unique identification scheme (UID) and national population register (NPR), and governance [Web log post]. Retrieved from http://cis-india.org/internet-governance/blog/uid-and-npr-a-background-note

Hosein, G., Hickok, E., & Chattopadyay, S. (2017, March). Six principles for openness and privacy in the time of data revolution: A critical data approach. In M. L. Smith & K. M. A. Reilly (Eds.), *Open development: Networked innovations in international development*. Chapter draft presented at the International Development Research Center and University of Cape Town authors' workshop, Cape Town, South Africa.

Hull, M. S. (2012). Documents and bureaucracy. *Annual Review of Anthropology*, *41*(1), 251–267.

Jayaram, M. (2015, August 15). Aadhaar debate: Privacy is not an elitist concern—It's the only way to secure equality. *Scroll*. Retrieved from https://scroll.in/article/748043/aadhaar-debate-privacy-is-not-an-elitist-concern-its-the-only-way-to-secure-equality

Khera, R. (2011). The UID project and welfare schemes. *Economic and Political Weekly*, *46*(9), 1–7.

Khera, R. (2017, July 19).The different ways in which Aadhaar infringes on privacy. *The Wire*. Retrieved from https://thewire.in/159092/privacy-aadhaar-supreme-court/

Kumaraguru, P., & Cranor, L. (2005, May–June). *Privacy in India: Attitudes and awareness.* Paper presented at the Workshop on Privacy Enhancing Technologies (PET 2005), Dubrovnik, Croatia.

Kumaraguru, P., & Sachdeva, N. (2012, November). *Privacy in India: Attitudes and awareness v 2.0* (PreCog-TR-12-001). Retrieved from http://precog.iiitd.edu.in/research/privacyindia/

Madden, M., Gilman, M., Levy, K., & Marwick, A. E. (2017). Privacy, poverty and big data: A matrix of vulnerabilities for poor Americans. *Washington University Law Review*, *95*(1), 53–125.

Maringanti, A. (2009). Sovereign state and mobile subjects: Politics of the UIDAI. *Economic and Political Weekly*, *44*(46), 35–40.

Maringanti, A. (2014). Telangana survey and the question of privacy. *Economic and Political Weekly*, *49*(36), 13–15.

Marwick, A. E., & boyd, d. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society*, *13*(1), 114–133. doi:10.1177/1461444810365313

Marwick, A. E., & boyd, d. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, *16*(7), 1051–1067.

Nissenbaum, H. (2011). A contextual approach to privacy online, *Daedalus*, *140*(4), 32–48.

Petronio, S. (1991). Communication boundary management: A theoretical model of managing disclosure of private information between marital couples. *Communication Theory*, *1*(4), 311–335.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Albany, NY: State University of New York Press.

Ramanathan, U. (2017, March 30). A shaky Aadhaar. *The Indian Express.* Retrieved from http://indianexpress.com/article/opinion/columns/aadhar-card-uid-supreme-court-a-shaky-aadhaar-4591671/

Scott, J. C., Tehranian, J., & Mathias, J. (2002). The production of legal identities proper to states: The case of the permanent family surname. *Comparative Studies in Society and History*, *44(*1), 4–44.

Sethia, A., & Kher, N. (2016, September). *The Indian identity platform ("Aadhaar"): The implications for citizen-government relationships in a developing country context.* Paper presented at the Internet, Policy and Politics Conference, Oxford, UK. Retrieved from http://ipp.oii.ox.ac.uk/2016/programme-2016/track-a-politics/government-i-civic-technologies/aradhya-sethia-nimoy-kher-the-indian

Singh, M. (2017, June 11). Plea against UID reflects elitist bias: Centre to SC. *The Times of India*. Retrieved from http://timesofindia.indiatimes.com/india/plea-against-uid-reflects-elitist-bias-centre-to-sc/articleshow/59090822.cms

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, *154*(3), 477–560.

Solove, D. J. (2007). "I've got nothing to hide" and other misunderstandings of privacy. *San Diego Law Review*, *44*, 745–772.

Solove, D. J. (2011). *Nothing to hide: The false tradeoff between privacy and security.* New Haven, CT: Yale University Press.

Sprague, A., Schulte, B., Black, R., & Eubanks, V. (2013, December 16). *In poverty, no privacy?* [Asset Building podcast]. Washington, DC: New America Foundation. Retrieved from https://www.newamerica.org/asset-building/podcasts/in-poverty-no-privacy

Srinivasan, J., & Johri, A. (2013). Creating machine readable men: Legitimizing the "Aadhaar" mega e-infrastructure project in India. In *Proceedings of the Sixth International Conference on Information and Communication Technologies and Development* (pp. 101–112). New York, NY: Association for Computing Machinery. doi:10.1145/2516604.2516625

Unique Identification Authority of India. (2017). *State-wise Aadhaar saturation*. Retrieved from https://uidai.gov.in/images/StateWiseAge_AadhaarSat_24082017.pdf

World Bank. (2017). *Principles on identification for sustainable development: Toward the digital age.* Retrieved from http://documents.worldbank.org/curated/en/213581486378184357/Principles-on-identification-for-sustainable-development-toward-the-digital-age

Wyber, R., Vaillancourt, S., Perry, W., Mannava, P., Folaranmi, T., & Celi, L. A. (2015). Big data in global health: Improving health in low- and middle-income countries. *Bulletin of the World Health Organization*, *9*, 203–208. doi:10.2471/BLT.14.139022