



**Data
Governance
Network**

Anchored by IDFC Institute

November 2020

Working Paper 12

***“I took Allah's name and stepped out”:
Bodies, Data and Embodied
Experiences of Surveillance and
Control during COVID-19 in India***

Radhika Radhakrishnan



internet
democracy
project

Data Governance Network

The Data Governance Network is developing a multi-disciplinary community of researchers tackling India's next policy frontiers: data-enabled policymaking and the digital economy. At DGN, we work to cultivate and communicate research stemming from diverse viewpoints on market regulation, information privacy and digital rights. Our hope is to generate balanced and networked perspectives on data governance – thereby helping governments make smart policy choices which advance the empowerment and protection of individuals in today's data-rich environment.

About Us

The Internet Democracy Project works towards realising feminist visions of the digital in society, by exploring and addressing power imbalances in the areas of norms, governance and infrastructure in India and beyond

Disclaimer and Terms of Use

The views and opinions expressed in this paper are those of the authors and do not necessarily represent those of the organization.



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

Design

Cactus Communications

Suggested Citation:

Radhakrishnan, R. (2020). *“I took Allah's name and stepped out”*: Bodies, Data and Embodied Experiences of Surveillance and Control during COVID-19 in India. Data Governance Network Working Paper 12.

Abstract

This paper presents a study of COVID-19 in India to illustrate how surveillance is increasing control over bodies of individuals, and how the dominant framework of data as a resource is facilitating this control. Disembodied constructions of data erase connections between data and people's bodies and make surveillance seem innocuous. As a departure from such a framework, this study adopts a feminist bodies-as-data approach to pinpoint the specific, embodied harms of surveillance. Starting from lived experiences of marginalised communities whose voices are often left out in debates on data protection, it shows that surveillance undermines not just data privacy, but more importantly, the bodily integrity, autonomy, and dignity of individuals.

Table of Contents

Introduction	04
Literature Review	05
Research Methodology	06
Structure of the paper	07
1. Unequal homes: Restricting access to data	08
2. Unequal communities: Stigmatisation	10
2.1 Gated communities	11
2.2 Community vigilantism through disinformation	12
3. Role of the state in perpetuating inequalities within homes and communities	15
3.1 The state disciplining the home	15
3.2 Interplay between the state and communities	17
i. Communities as spies of the state	17
ii. Caught between the state and communities	18
4. Regulation and criminalisation of public mobilities by the state	21
4.1 Drone patrolling	22
4.2 Mobile location tracing	23
5. Exclusion from essential services, rights and social protection	25
5.1 Mandatory digital requirements	25
i. Aadhaar	25
ii. Aarogya Setu	27
5.2 Social protection schemes	30
i. Apps for financial assistance to inter-state migrants	31
ii. Controlling financial data of the poor	33
6. Where do we go from here to protect bodies in disease surveillance?	35
6.1 Can data keep people safe during a pandemic?	35
6.2 Resistance and its limitations	37
6.3 Role of care	38
6.4 Role of mutual trust	40
Conclusion	42
References	43
Acknowledgements	58
About the author	58

Introduction

It's the class that jetsets that is actually carrying this [virus] from place to place and it's our unwillingness to self-isolate that creates community infection... We will...inevitably say, "it's a sabziwala who is doing this, it's the press wali... it is her iron that is transmitting the virus from my clothes to your clothes"... How long will it take for us to revert to these attitudes that maybe we never really got rid of? And to turn the same habits of surveillance to erect further social barriers? ... And then will some of these tools of surveillance, will some of this freely available data then become a way to narrow our social circles? ... A pandemic-sanctioned habit of distancing facilitated by easily available data--what will that make us?

- Swarna Rajagopalan, Founder and Managing Trustee, Prajnya Trust

Data has helped us make sense of the Coronavirus Disease 2019 (COVID-19) pandemic, from offering insights into numbers of confirmed cases to mortality rates, thus providing public health authorities with a common ground for action (French & Monahan, 2020). Moreover, from enabling communication to facilitating relief efforts, many groups of people have relied upon data and digital technologies to survive the pandemic. At the same time, when in the hands of more powerful members of families and communities, as well as the state, data has enabled widespread surveillance of people through contact tracing apps, drone patrolling, and tracking mobile data of people, among other measures.

Epidemiological surveillance has historically been carried out during epidemics for disease control. However, the manner in which it is carried out determines how it is experienced by people. Akhila Vasan and Vijaya Kumar from the Karnataka Janarogya Chaluvali, a people's health movement, explained:

The term surveillance is used in epidemiology very typically for disease travel... to contain an outbreak... But I think today, when you say surveillance, that's not what comes to mind, despite being someone who works in health... Now what people are trying to do is making the same epidemiological surveillance more and more efficient, more real-time...Apps are coming like that, drones are coming like that...Earlier anything would involve a personal interaction where you have a certain kind of a connect with the person but I think all that is now replaced with an app. And with the state, I think somehow there is a fear of... constantly being watched, you're looking over your shoulder to see who is tracking you.... COVID-19 is a convenient ruse for the state to introduce these apps.

This paper presents a study of COVID-19 in India to illustrate how surveillance is increasing control over bodies of individuals, and how the dominant framework of data as a resource is facilitating this control. Disembodied constructions of data erase connections between data and people's bodies and make surveillance seem innocuous. As a departure from such a framework, this study adopts a feminist bodies-as-data approach to pinpoint the specific, embodied harms of surveillance. Starting from lived experiences of marginalised communities whose voices are often left out in debates on data protection, it shows that surveillance undermines not just data privacy, but more importantly, the bodily integrity, autonomy, and dignity of individuals.

Literature Review¹

The dominant framework for conceptualising data is that of a resource, an asset (like oil), the worth of which depends upon human ability to extract its value for our use (“The world's most valuable resource”, 2017). Such constructions of data find root in the field of cybernetics as a layer of information that permeates everything and still exists independently from the medium carrying it, making it possible to transfer it from one medium to another (Hayles, 1999). This dematerialisation and disembodiment of data open it up to possibilities of human exploitation and manipulation (Couldry & Mejias, 2019).

When data is used for surveillance, the framework of data-as-resource reduces bodies to disembodied data points, erasing the social contexts and power dynamics that surveillance occurs in. It then becomes easier to make data seem like an accurate, objective truth-teller that takes precedence over material bodies (Hayles, 1999). However, Kovacs and Ranganathan (2019) argue that data does not exist outside of the social world because the bodies that generate data also do not. Highlighting that surveillance does not take into account social contexts, Lyon (2003) proposes the concept of “surveillance as social sorting” (p. 1) according to which surveillance goes beyond threatening individual freedoms towards creating and reinforcing long-term social differences.

Building upon this analysis, viewing surveillance from a feminist perspective helps us focus on power relations and attend to difference, while also bringing bodies back into the picture (Kovacs, 2017a). Foundational work by Monahan (2009) analyses the ways in which surveillant technologies have gendered outcomes but does not question its implications for the conceptualisation of data on a more fundamental level. Some scholars have argued that data is embodied within surveillance practices (Lupton, 2016; Smith, 2016), and creates value for those who seek that data even if it does not always coincide with an individual's lived, embodied identity (Ball, 2016). Haggerty and Ericson (2000) contend that instead of treating bodies as single, whole entities, contemporary data-driven surveillance practices fragment our bodies into a series of discrete disembodied information flows forming a 'surveillant assemblage'. They refer to this new datafied body as a 'data double', which constitutes an additional self, primarily serving the purpose of being useful to institutions for allowing or denying access to material bodies. While being a useful framework for understanding surveillance, alluding to a data double implies that a separation exists between the material body and the datafied body.

Going beyond emphasising embodiment of data, van der Ploeg (2003) questions the very ontological distinction between embodied persons and data about persons. Offering the example of biometrics such as iris or finger scans, she argues that when data is increasingly collected for surveillance, data can no longer be thought of as about the body but must be reconceptualised to be a part of the body under surveillance. If data constitutes who a person is, then what happens to our data, how it is used, by whom and for what purposes, become grave concerns with far-reaching consequences for our material bodies. These consequences come to light in policy design since we have different policies for protecting bodies and data from intrusion (van der Ploeg, 2012). Normative concerns around data misuse are described in terms of potential violations of data privacy which is defined as having control over one's data. Such a policy framework aims to protect personal data and not bodies that generate this data. To reconcile this difference, van der Ploeg suggests that when data emerges as an extension of our bodies, the harms of data misuse should be reconceptualised as violations of bodily integrity rather than data protection violations so that more stringent criteria may apply to them.

¹ The conceptual links across different fields of scholarship that this paper builds upon have been developed by Anja Kovacs and will be further detailed in a forthcoming working paper by her for the Data Governance Network.

Other scholars have also critiqued the hegemonic, narrow focus on privacy that subsumes broader discourse around the body, calling attention to its ethical aspects (Ajana, 2013) and the violence of writing the body into digital form (Amoore & Hall, 2009). Kovacs and Ranganathan (2019) contend that policies on data sovereignty erase bodies and selfhoods, thereby failing to protect the autonomy, freedom and dignity of citizens. Taking bodily integrity as their starting point, Kovacs and Jain (2020) apply feminist scholarship to rethink consent frameworks within data protection policies.

Beyond the issue of privacy, the use of data for surveillance complicates traditional notions of surveillance that were envisioned by Foucault (1991). Surveillance becomes ubiquitous with multiple actors involved, and decontextualised (Haggerty & Ericson, 2000). It transcends space and time, no longer requiring the physical presence of the observer (McCahill, 1998) and making bodies searchable from a distance (van der Ploeg, 2012). It is used to not only watch over us, but also to identify, track, monitor, and analyse our actions (Monahan, 2009). Because surveillance (who does it, where, on whose behalf) is often opaque or invisible to people, there is reduced control over and consent for the decisions made about them. While in earlier forms of context-specific social control, there was some space for negotiations, this space is now reduced (Norris, 2005). The use of data for surveillance also makes possible its pre-emptive (seeking to control now, so it can avoid having to repress later) and productive (making people do certain things) nature (West, 2014). In some cases, surveillance may not be the goal of a technological system, though it can have that effect (Monahan, 2009; Fisher, 2006). Other differences have also been theorised (Marx, 2002).

Much of this scholarship on data, embodiment, privacy, and surveillance has provided the theorisation that this study builds upon. This study provides greater depth to this scholarship by examining the mechanics of how this theorisation works in practice using qualitative data. It responds to the gap in literature as pointed out by Lyon (2007) to “show the connection between the real lives of ordinary people and the modes of surveillance that serve to watch, record, detail, track and classify them.”

Feminist standpoint epistemology (Harding, 1992) claims that some ways of knowing the world are inherently better than other possible ways—the starting point for knowledge about society should come from the lives of marginalised persons, as this would provide a better understanding of the world and visibilise those oppressions that are invisible to epistemologically privileged worldviews of dominant communities. By highlighting lived experiences of people at the margins who are most severely affected by the harms of surveillance, this paper bridges the gap between theory and practice from a feminist standpoint and provides a starting point for policies to be framed around the embodied nature of data.

Research Methodology

This paper adopts a qualitative research methodology. I conducted twenty-five semi-structured, in-depth telephonic or online interviews (mobility constraints imposed by the nation-wide COVID-19 lockdown made in-person interviews not possible). The interviews were conducted between April 2020 and July 2020 in English and Hindi with the following communities and stakeholders in India: trans-queer persons, sex workers, Muslims, migrant labourers, app-based gig worker unions, ASHA worker unions, persons being denied services without smartphone applications, persons experiencing drone surveillance, women's rights organisations and activists, organisations working with Adivasis and working-class communities, and public health activists.

² I'd like to thank Tanisha Ranjit from the Internet Democracy Project for sharing this piece of literature with me.

Known acquaintances and people within common feminist networks were initially contacted. From here onwards, the snowball sampling method was used to select participants for this study. A call for inputs in English and Hindi was posted on the Internet Democracy Project website and shared on various social media and messaging platforms (Radhakrishnan, 2020).

The motivation for this methodology was to understand how surveillance impacts people and communities at the margins of gender, sexuality, class, caste, and religion, among other factors, during a pandemic. Either their socio-cultural identities or the nature of their labour—and sometimes an overlap of both—made them vulnerable to surveillance. These voices are often left out of the discourse around data and surveillance within policy studies; when they are referred to, they are often spoken about without being spoken to. This paper is an attempt to challenge and change that norm so that wider expressions, experiences, and knowledge(s) of surveillance may arise.

Due to COVID-19 lockdown mobility restrictions, there were limitations in conducting ethnographic fieldwork, participant observation, and in-person interviews. Because of this, it was difficult to connect with many of those who were hit hardest by surveillance since they had limited access to phones or the Internet to establish contact. To work around this limitation, I interviewed some research participants for their expertise on or extensive grassroots work with communities whose experiences I was trying to understand, such as women's rights organisations and public health activists. I was not able to establish communication with some marginalised communities, such as persons with disabilities and farmers, which is a limitation of the sample of this study. Wherever possible, media reports and other studies have been referenced to fill these gaps.

Some names used in this paper have been changed as per the request of the research participants, and this has been indicated in footnotes for their first usage in the paper. Names and organisations that have been used as is have been mentioned after seeking explicit written or verbal consent from research participants.

In addition to conducting interviews, I attended webinars that discussed key issues pertinent to the communities whose experiences I was studying, as well as analysed academic literature, news reports, government documents, and studies done by other organisations to triangulate my findings.

Structure of the paper

In Sections 1 to 3, I unpack how surveillance, through disembodied constructions of data, shapes the lived experiences of marginalised persons within unequal spaces of the home, community, and the state, respectively. In Section 1, I analyse how surveillance is reproducing social hierarchies and vulnerabilities within the home by restricting access to technology for some family members. In Section 2, at the level of communities, I analyse how inequalities take the form of stigmatisation promoted by surveillance technologies within gated communities and through digital disinformation. In Section 3, I highlight the role of the state in perpetuating surveillance and exacerbating inequalities within homes and communities.

The state plays a key role in surveillance during COVID-19 in other ways as well, as shown in Sections 4 and 5. In Section 4, I look at how surveillance through data is used to regulate public mobilities and criminalise people during the pandemic. In Section 5, I analyse how datafication, while often aimed at improving access, creates challenges for people to access essential services, rights and social protection during the pandemic, and adds to the surveillance infrastructure of the state.

Disease surveillance has historically been a part of epidemic responses to contain their spread, and some degree of surveillance may similarly be required to control the COVID-19 pandemic. In Section 6, I reflect upon how this can be done while protecting the bodies of people. The section first fundamentally questions whether data can keep people safe during a pandemic. It then looks at the various ways in which people and communities are mobilising their agency in resisting surveillance during COVID-19, the limitations to such resistance, and the newer challenges to resistance that data-enabled surveillance throws up. To respond to these challenges going forward, the section lastly analyses the structural role of care and mutual trust in disease surveillance during COVID-19.

1. Unequal homes: Restricting access to data

During COVID-19, we have constantly been told to stay at home to stay safe (Vallee, 2020). However, feminist research on domestic violence in India has established that the home is not always a safe place (“COVID-19, Domestic Abuse and Violence”, 2020). The home is an unequal space in which bodies of the vulnerable are surveilled by more powerful family members, leading to the reproduction of inequalities, with data playing a key role. I will illustrate this through the experiences of trans-queer persons, women facing domestic violence, and commercial sex workers.

First, for persons identifying as trans or queer, the home is often not an accepting space for their preferred gender expression. At the same time, during the COVID-19 lockdown, people have been restricted to the home. Amrita Sarkar, a programme manager and helpline counsellor at SAATHII (Solidarity and Action Against The HIV Infection in India) observed: “Based on their [trans person's] preferred gender identity, they want to have certain behaviours but during COVID-19, they are being asked to behave like a 'proper boy or girl,' so they cannot express their gender identity.”

Since technologies exist within social hierarchies, the same technology that allows queer persons to connect with support structures outside the home can turn back on them when in the hands of others. Bishakha Datta, Executive Director of Point of View, an organisation that works on technology, gender and sexuality, shared that during the lockdown, a queer person got outed in their family when someone else answered their phone. Social hierarchies are thus mirrored in the use of digital technologies.

Second, the National Commission for Women (NCW) noted a rise in the number of domestic violence complaints received by email during the lockdown (Kumar, Mehta & Mehta, 2020) as women have been forced to be in proximity to abusive families for unprecedented longer periods of time. However, reports in the early days of the lockdown showed that despite this situation, helplines were not receiving more calls than usual (Bose, 2020). According to NCW, the real number of cases is likely to be higher than what is reported, because most complaints come by post since women might not be able to access the Internet (NDTV, 2020). Highlighting this concern further, Shubhangi at the Association For Advocacy and Legal Initiatives (AALI), Lucknow, a feminist legal advocacy and resource group working with domestic violence survivors, observed:

Many women don't have their own phones... [Sometimes] there is a family phone... that they have to share. The priority just shifts in terms of adolescent girls... if there is just one device that is Internet-enabled, then she is definitely not in the list of preferences for its usage... So only when it will be free will she have access.

India has one of the highest gender divides for access to communication technologies: only 59% of women in India own mobile phones, as compared to 80% of men (GSMA, 2019). This divide is much higher for some demographics, such as low-income groups and in rural India. Moreover, it is not enough to merely have access to a mobile phone; one must be able to access it meaningfully (Internet Governance Forum, 2016) in a context-appropriate manner wherein women can exercise their agency over the autonomous usage of the device.

These gendered inequalities bring into question the efficacy of WhatsApp numbers and helplines that have been introduced by the state to report violence during COVID-19 (“NCW launches WhatsApp number”, 2020). For women with disabilities, this is even more challenging (Rising Flame & Sightsavers, 2020). Datta mentioned:

Women who are facing domestic violence are finding it really hard to use phones to get any sort of help even if they knew who to go to... So even if you were to get that phone and make a phone call to... a helpline number or the police... everyone is in a small house, everyone is really hearing each other. So how would you complain?... Women are also feeling a little nervous about [using] helpline numbers because the minute you use that number, it's recorded on your phone. So if that is not your own phone, then it gets recorded on a shared phone which means... whoever has access to that number can just call it back. People are scared of leaving a trace of the number that they are calling.

Third, consider the case of some commercial sex workers who (unlike the case of women using shared phones) may own two phones or SIM cards—one for personal use and one for professional use. Studies show that commercial sex workers who have access to mobile phones increasingly depend on these devices for soliciting clients and managing long-term relationships with them (Panchanadeswaran et al., 2017). However, power hierarchies within the home have created challenges for them to keep in touch with clients during COVID-19 because sex work is highly stigmatised and the families of sex workers don't always know about the nature of their work. Datta shared:

What [sex workers] usually do when they are working is that they will take out the SIM and hide it every evening...but because these are shared spaces, they are not able to use their separate SIM for professional work, and now they are just permanently taking it out and keeping it away. So there is a sort of fear of loss of business... They cannot function because of a lack of privacy, so there is a lot of fear that ... the information that is there on the phone, somebody in the family might actually be able to see it, and know what they are doing.

In all the cases discussed here, restrictions are placed upon bodies of already vulnerable persons through restrictions upon their access to technology. In each case, the use of data and technology can potentially be liberating to access communities and possibilities outside the home. However, it is this same liberatory potential that threatens to destabilize the hierarchies that exist within the home, resulting in stricter control over access to technology to prevent such subversion.

Women are sometimes banned from using mobile phones and the Internet because the networking potential of such technologies is culturally deemed to be a corrupting or dangerous influence on them (Kovacs, 2017; Arora & Scheiber, 2017). It is believed that if women access information online, they may be 'liberated' from the traditional grasp of patriarchal control. Data is seen as an escape, a way out, for

women from their traditional boundaries. For women reporting domestic violence through a mobile phone, data is a way out of abusive households. Similarly, for sex workers contacting clients on their mobile phones, data is a pathway to labour that is considered immoral under patriarchy. For trans queer persons, data is a way to connect with 'forbidden' experiences and communities outside of heteronormative patriarchal norms. Thus, controlling a person's data is a way of controlling their bodies, movements and activities.

Feminist scholars have conceptualised such bodily control as a form of surveillance. Kovacs and Ranganathan (2017) argue that surveillance is a dominant mode for controlling people (though other forms of control also exist) in a manner that everyone is implicitly governed by some expectations of social conduct. These expectations are, in turn, determined by the identities and social locations of persons under surveillance, such as gender, caste, sexuality, religion, class, and ability. Deviations from these norms are punished, often through acts of violence, and adherence may be rewarded through 'protection' from violence.

Feminists have called for the understanding of domestic violence itself to be broadened to incorporate the violence triggered by the use of digital technologies (Sen, 2020). For example, for women with some degree of access to mobile phones or the Internet, this access is mediated through more powerful members of the family, and can lead to violence. Shubhangi said:

During the times of COVID, when everyone has been locked down, access to mobility is through telephones or the internet, and we have seen this emerging as a newer and larger trigger for violence within the homes where women are being subject to violence because they are 'spending too much time on the telephone.'

Technologies amplify existing conditions of social inequality since they take on values from the contexts of their use (Monahan, 2009). For trans-queer persons, this has meant being outed to the family through their mobile phone data. For survivors of domestic violence, it has meant being unable to get adequate redressal for violence through helplines. For sex workers, it has meant a loss of income by not being able to contact their clients through their phones at home. All of these are embodied, material harms. People who are facing these harms (or people working with them) describe their experiences as “fear of loss of business” or being “scared of leaving a trace” on a phone. These are embodied emotions. These intimate experiences cannot be understood through the narrow framework of data privacy or invasion of privacy, though existing data protection policies understand them in this limiting way (van der Ploeg, 2003; Ajana, 2013). Something a lot more devastating is happening to these people when their data is being controlled within the home—their very vulnerabilities are being reproduced, reaffirming and legitimising their subjugated position within existing familial hierarchies.

2. Unequal communities: Stigmatisation

According to the World Health Organization (WHO), COVID-19 is a stigmatised disease due to three main factors (“Social Stigma associated with COVID-19”, 2020): it is a new disease for which there remain many unknowns; we are often afraid of the unknown; and it is easy to associate that fear with 'others' who are 'outsiders' or on the margins of society. Stigma has material consequences—medical experts who have studied past epidemics warn that stigma and blame for a contagious disease weaken trust in

marginalised communities and make people less likely to seek treatment. Stigma is also adding to the mortality rate of India's COVID-19 cases as people with symptoms are reluctant to report them (Ghosal, Saaliq & Schmall, 2020).

This has been observed in other stigmatised health epidemics in the past. In the case of tuberculosis (TB), women suspected of having TB have been abandoned and ostracised due to its stigma, leading to a gendered delay in their diagnosis and treatment (Rao, 2015). In the case of HIV/AIDS, sex workers and trans-queer communities have been stigmatised as the predominant carriers of the virus (Dube, 2019). Similarly, in the case of COVID-19, stigma of the disease is being passed on to marginalised communities.

What is of particular relevance to this study is that the fears of this relatively new disease with many unknowns are being offset by surveillance of bodies suspected to be carrying the virus. By targeting specific marginalised communities, surveillance is used to reinforce and reproduce unequal social norms. This control is being facilitated by data through surveillance technologies as well as digital disinformation campaigns. This section explores the stigmatisation of 'others' within a patriarchal, Brahmanical, and Islamophobic society by focusing on the lived experiences of surveillance for bahujan, Muslim, transgender, and working-class communities during COVID-19.

2.1 Gated communities

Within gated communities such as Resident Welfare Associations (RWAs) in urban areas, surveillance has been put into place during COVID-19 for domestic workers, cooks, and drivers, who are mostly from marginalised castes. Bishakha Datta observed:

I was told [by my RWA]... 'you can get your cook tested'... in a context where they [cooks] are not even living in that society and you [RWA], who are living there, are not testing yourself. You're not testing other family members, or insisting that other members of the building be tested even if they go to work.... People [are] physically surveilling domestic workers, really watching their actions to see whether they are being hygienic during COVID-19... There is a way in which surveillance is working now where some people feel like they are morally superior and can pass judgment on other people.

This is despite the first domestic worker reported with COVID-19 in Mumbai having contracted the virus from her employer (Kakodkar, 2020). In India, the caste system is characterised by a birth-based graded hierarchy of endogamous castes, premised upon notions of ritual purity and pollution of bodies (Ambedkar, 2014). The cleanliness discourse around COVID-19 refers to ritual purity as opposed to physical cleanliness, and their conflation constructs the bodies of Dalits as carriers of the disease, exacerbating prejudices towards them (Kumar, 2020). While caste-based exclusion and stigma have long existed in the country, COVID-19 has further legitimised it by co-opting the language of disease as a justification for discriminating against marginalised castes. In Bihar, a Dalit man shared: "Every time I step out, people start shouting 'corona, corona'... Earlier they would walk at a distance because I am a Dalit, but now they call me the disease itself" (Sur, 2020).

Data facilitates the surveillance of marginalised bodies. A mobile phone application (henceforth, app), MyGate, collects personal details and working hours of domestic workers and displays their schedules to all the residents in an apartment block, and facilitates their entry and exit into the building's premises. According to their website, over 60 million users are 'validated' by their app every month ("MyGate", n.d.). Another security management app developed by the real-estate startup, NoBroker,

facilitates touchless entry with facial recognition at the gates of housing societies. The app recently introduced a COVID-19 tracker feature that is integrated with the central government's Aarogya Setu contact-tracing app. The app's co-founder, Akhil Gupta, said: "in case domestic help or a driver are coming from any of the containment zones near the society, residents will be alerted and can choose to deny entry to them" (Khan, 2020).

Both these apps give residents immense power over domestic workers by exerting control over their entry and exit into a housing society. Qualitative studies show that this puts workers in a precarious position: when each visit needs to be pre-approved by their employer, domestic workers may have trouble approaching them, for example, when their salaries have not been paid on time (G.P., 2020). During the pandemic, this may have had a devastating impact on domestic workers since many of them have not received monthly payments due to employers denying them entry into their homes as a result of the stigma attached to their marginalised collective identities (Raj, 2020).

During the Unlock 2.0 phase, the Municipal Corporation of Gurugram declared that "entry of house-helpers and maids [would] be allowed with restrictions such as... thermal scanning... at entry gate" (ANI, 2020). This is despite research that shows the inaccuracy of thermal cameras and the fact that human temperatures tend to vary widely (Guarglia & Quintin, 2020). The conceptualisation of data as a resource lends to it being considered accurate and objective, taking precedence over material bodies that the data is meant to represent.

Moreover, many RWAs are using CCTV cameras within residential complexes to monitor physical distancing and restrict entry to their premises (Madur, 2020). The data collected through CCTVs is accessible only to RWA officers and heads, and is used to surveil 'outsiders'. The presence of cameras outside society gates is a way to signal who belongs in a particular space and who should be kept out of it. In the context of the stigma around marginalised bodies during the pandemic, the cost of such surveillance is mostly borne by communities, such as those of domestic workers, who are already being denied entry into these spaces. With the introduction of CCTVs, the surveillance gaze is far removed from the temporal and spatial constraints that were present in face-to-face surveillance (Norris, 2005).

CCTV cameras could be desirable, even empowering, in some contexts (Ranganathan, 2017). For example, some slums in Delhi and Mumbai voluntarily installed CCTV cameras in their localities to expose false arrests of slum dwellers by the police during episodes of communal violence (Jha, 2013). What matters is the power dynamics such technologies operate within, which dictate who has control over the usage of the technology and who is controlled by it (Lyon, 2003).

Within the space of the family, we saw previously how differential power dynamics dictate the use of mobile phones within the home, disallowing their access to vulnerable members and facilitating control over their bodies. Similarly, at the level of communities, surveillance systems such as those put in place by RWAs facilitate bodily control through context or use discrimination, which is discrimination engendered by social contexts (Monahan, 2009). Data collected through surveillance systems is in the hands of more powerful communities such as RWAs and working-class communities have little say in how this data about them is collected or used. Thus the existing unequal power relations between communities are reinforced and reproduced by these technologies.

In all of the above examples, surveillance leads to the stigma of COVID-19 being legitimised and reinscribed in the bodies of persons from marginalised communities through physical, bodily restrictions on their movements. Bodies of domestic workers are controlled through their data on apps

and CCTVs. Beyond concerns of data privacy, this has material consequences, such as workers being stopped from approaching employers for payments because they are stigmatised, pushing them into poverty, especially during a health crisis.

2.2 Community vigilantism through disinformation

Image 1: Poster reads, “Warning: Do not allow Kojja, Hijras near the shops. If you talk to them or have sex with them, you will be infected with Corona Virus. Beat and drive them away or call 100 immediately. Save people from Corona Virus Hijras”.

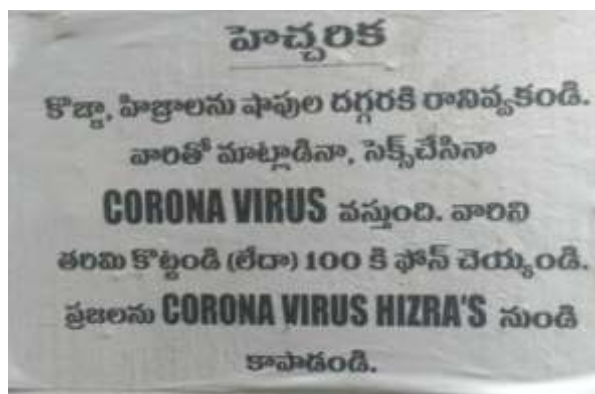


Image 1 is a poster that appeared in many places in Hyderabad, blaming transgender persons for the spread of COVID-19 (Sanghamitra, 2020). Discriminatory acts of surveillance have been put into place by cis-communities due to the stigma against trans persons. Raina Roy is the Director of the non-profit Samabhabona, and a trans woman. She spoke of Meena,³ a trans woman who works as a sex worker in West Bengal, who was recently diagnosed with COVID-19. When she wanted to go back to her family's residence after recovering at the hospital, Roy said:

Other members in her apartment protested that she cannot come and live in the flat... Her neighbours got to know that this person who was [COVID-19] positive was transgender, and they started to discriminate. They called up the police and made a barricade over there. And the neighbours told her family they will not give entry to their child when she comes back from the hospital.

Other members in her apartment protested that she cannot come and live in the flat... Her neighbours got to know that this person who was [COVID-19] positive was transgender, and they started to discriminate. They called up the police and made a barricade over there. And the neighbours told her family they will not give entry to their child when she comes back from the hospital.

Chellamma,⁴ a trans woman, shared her concerns about data exacerbating this scenario:

There is already a negative stereotype of criminality associated with trans persons... With more surveillance...with more technology coming in...increasingly you'll find trans persons becoming more vulnerable because...now it's not just about a... rumour in some remote space. It will end up being like... rounding up trans persons if...[you] don't like trans persons.

The World Health Organization has declared that “we're not just fighting an epidemic; we're fighting an infodemic. Fake news spreads faster and more easily than this virus and is just as dangerous.” (Ghebreyesus, 2020) The deluge of disinformation about COVID-19 on social media and messaging platforms has taken various forms, such as falsified facts, xenophobia, false government notifications, and threats of violence (Sengupta, 2020). In all of these cases, data is stripped of its original social context with the intention to mislead. When disinformation targets marginalised communities, it potentially shapes prejudices against them, and promotes the need for surveillance of their bodies. More importantly, this surveillance enabled through disinformation in digital spaces can have devastating consequences for them in physical spaces.

³ Name changed

⁴ Name changed

Medical experts say that the best way to prevent community transmission of COVID-19 is to maintain 'physical distancing' (World Health Organization, n.d.). In this context, social media and WhatsApp campaigns are using the altered terminology of 'social distancing' to defend caste discrimination, justifying historic practices of caste-based distancing as a cure for COVID-19 (Harikrishnan, 2020). In India, social distancing is a sociocultural phenomenon prescribing the social isolation of Dalits in the caste order (Kumar, 2020). People from upper caste communities are claiming that Brahmins discovered caste-based physical distancing as a cure to the virus thousands of years ago (Harikrishnan, 2020). Such casteist rhetoric not only legitimises stigma and discrimination against marginalised castes but also reproduces caste hierarchies by actively promoting the renewal of these practices to contain the spread of the virus. This can have life-threatening implications. In Beed, a Dalit man was assaulted by men from the upper-caste Maratha community, after a rumour was spread that his family members had tested positive for COVID-19 (Modak, 2020).

Similar links are observed between disinformation online, community surveillance, and resulting physical harm to bodies in the case of Muslims. In New Delhi in March 2020, a religious congregation was organised by the Tablighi Jamaat, an Islamic missionary movement, in the Nizamuddin Markaz Mosque; it was attended by more than 9,000 missionaries. The Indian government claims that this event caused the largest spike in COVID-19 cases in India despite the 'Indian Scientists' Response to COVID-19' group denying the claim (Ellis-Petersen & Rahman, 2020). According to data shared by Equality Labs with Time magazine, tweets with the hashtag #CoronaJihad appeared nearly 300,000 times and were potentially seen by 165 million people (Perrigo, 2020). A 37-year-old chicken peddler in Himachal Pradesh, Dilshad Mohammad, died by suicide after neighbours accused him of deliberately trying to infect them with the virus when he gave two members of the Jamaat congregation a ride to their village on his scooter. The district police superintendent blamed his suicide on stigma (Ghosal, Saaliq & Schmall, 2020).

In another case, after a video depicting residents threatening to impose a ban on Muslim vegetable vendors went viral on Facebook, buyers in North-West Delhi began seeking identity cards to ascertain whether the vendors are Muslim (Bhardwaj, 2020). Drishti Agarwal and Manju Rajput are Programme Executives of the Family Empowerment Programme of Aajeevika Bureau, an organisation that works with migrant labourers. In the context of rural Rajasthan, they said that “vegetable sellers who are Muslims are being boycotted, people are saying don't buy vegetables and other things from Muslims” (translated from Hindi). Vinay Sreenivasa, an advocate from Naavu Bharatheeyaru, recounted in the context of Bengaluru that “We've seen that Muslim volunteers who have gone to distribute food have been... asked to remove their... white cap... and prevented from distributing food in hospitals saying 'you would have spit into the food.'”

Disinformation relies upon the misrepresentation of data taken out of its original social context, either by digitally altering it (such as images and videos) or combining it with text to manipulate readers. Monahan (2009) conceptualises discrimination by abstraction as “the ways that technological systems...strip away social context, leaving a disembodied and highly abstract depiction of the world and of what matters in it”. In the process of filtering out social contexts, inequalities are exacerbated because bodies become data without representational presence outside their social contexts (Monahan, 2009).

This form of surveillance is slightly different from surveillance within gated communities analysed earlier, but it is still an important way in which bodies are controlled through data. In this case, data is not directly collected about individuals and communities to exercise control over their bodies (as we saw previously). Instead here, existing data which may not originally be about specific communities is

manipulated to target those communities. The bodies of those targeted are harmed despite this data not corresponding to their physical realities, because data exists within social contexts that are already prejudiced against them. Since the dominant conceptualisation of data is that of an objective, accurate resource, it becomes easier to consider it a truthful representation, even when it is not. When we focus on how the realities of targeted communities are shaped by such disinformation, the bodily harms of such surveillance come to light. In 2018, there were over 30 reported deaths linked to rumours circulated on WhatsApp in India (Christopher, 2020). This indicates that when disinformation promotes surveillance of marginalised communities, it leads to social stigmatisation and fatal harm to their physical bodies. In the cases of information as well as disinformation, the prejudices against those who are targeted through surveillance are reproduced and legitimised, and its harms are material and embodied, such as the inability to access gated communities and receive wages (as seen previously), or fatal physical violence (as seen here).

3. Role of the state in perpetuating inequalities within homes and communities

So far, this study has analysed surveillance that takes place in homes and communities by more powerful stakeholders present there, reproducing existing inequalities. This section now analyses the key role that the state plays in perpetuating surveillance and inequalities in these spaces.

As the previous section examined, social stigmatisation is observed at the level of communities and promotes surveillance of the bodies of people suspected of carrying the virus. Stigmatisation is also linked to state actions targeted towards marginalised communities through surveillance (Corrêa, 2020). For example, a group of migrant labourers in Bareilly were sprayed with bleach on the street (Tarafer & Sonkar, 2020), while no such dehumanising disinfection measures were enforced for airline travellers, for whom even thermal screening measures were not always put in place by the state (Sharma, 2020).

Epidemic crises are similar to other kinds of political crises since they become ways in which the state is able to legitimately intervene into the social lives of people (Agamben, 2020). For example, the Indian state has used the threat of colonial legislations such as the Epidemic Diseases Act (EDA) to implement surveillance measures (Banerjee, 2020), some illustrations of which will be explored in this section. Social theorists such as French and Monahan (2020) contend that the COVID-19 pandemic is being used to normalise state surveillance around the world by justifying it as a necessary insurance against future threats.

3.1 The state disciplining the home

During the pandemic, the names and addresses of persons in home quarantine were made public by various state governments, including Karnataka (Pandey, 2020), by invoking the EDA (Banerjee, 2020). Soon after this, Karnataka's government released the Quarantine Watch app, which required all home-quarantined persons to upload geo-tagged mobile phone selfies every hour to prove their presence at home (Urs, 2020). These selfies are then checked using a facial recognition software. A breach occurs if a person fails to upload the selfie in a timely manner. The first two breaches are met with a warning, and subsequent breaches result in an FIR being registered against the violator, who is forcibly sent to an institutional mass quarantine centre. At least 85 FIRs have been filed through the data collected from

this app so far (Shenoy, 2020). Various other apps using selfies have been released during COVID-19 for persons in home quarantine (Kappan, 2020).

With this, the state's disciplinary power of surveillance has reached the intimate space of the home, blurring the divide between what is traditionally considered private and public. Terming this phenomenon “self(ie)-governance”, Datta (2020) argues that the introduction of the selfie in the Quarantine Watch app moves facial recognition from public spaces into the home, bringing domesticity directly under the state's gaze..

What are the tangible consequences of this? Moving beyond the concern of privacy of the images collected, I analyse the app from the perspectives of gendering surveillance (Kovacs, 2017a) and embodied data (Kovacs & Ranganathan, 2019; Kovacs & Jain, 2020; van der Ploeg, 2003). Feminist studies show that one of the reasons women prefer to not approach the police to file complaints relating to cyber violence is a lack of faith in the legal system (Kovacs, Padte & Shobha, 2013). This includes discomfort and distrust associated with the state being able to view their private content such as images on their phones during the investigation of a case. Sending hourly selfies from within the private space of the home could bring up the same discomfort. For women, such access to their images could extend to slut-shaming, voyeurism and predatory actions by the state. This brings into question concerns around the protection of not just the data being shared, but the bodily integrity of the person sharing it.

Beyond the use of selfies, the state is also monitoring the locations of persons in home quarantine through apps with a feature for 'geo-fencing' which creates a virtual perimeter for a real-world geographic area—in this case, the home. For example, Punjab's COVA app (Ranjit, 2020a), Chandigarh's COVID 19 Tracker (Sehgal, 2020), and similar apps in Gurugram (Jha, 2020) among others, all use geo-fencing to track movements of persons in home quarantine. If a person leaves their quarantined area by a certain distance, an alert is generated and the police department is notified. In earlier forms of surveillance, the presence of a human was necessary to monitor a person's actions. Most people (especially women, as analysed above) may feel unsettled by the presence of police officers within their homes (Ranjit, 2020a). In the age of digital surveillance, bodies of individuals within the home are now subjects of the digital state through their data collected by home quarantine apps. The physical body is being disciplined to stay at home and follow state orders without the physical presence of the observer (McCahill, 1998)—in this case, a police officer. This is one of the ways in which our bodies are tracked, monitored and controlled through our data.

When the selfie becomes proof of self-discipline under quarantine, it triggers new power relationships between the state and citizens (Datta, 2020). As analysed in section 1, power inequalities within the home are reproduced through control over data by family members in positions of power. Women have, to some extent, been able to negotiate with this power within the home. For example, women sometimes simulated possession by goddesses to broker money for domestic expenses from god-fearing husbands. In this way, women negotiated more power within the home (Kumar, 1993). However, under the state's constitutional framework, all citizens must be treated equally, even though all of us are not considered equal by social norms (Ambedkar, 2014). The new hierarchical power relationships brokered by data throw a spanner in this principle by reducing the space available for negotiations that would otherwise be available within the home. This is very concerning in a pandemic which the state is accountable for managing.

While the state is responsible for controlling the pandemic, the control it is exercising through apps must be seen in the context of the absence of physical infrastructures for health such as quarantine centres and testing facilities (Datta, 2020). The state's responsibility to provide physical health infrastructure is passed on to citizens and monitored through digital infrastructures such as quarantin

e apps. The COVID-19 threat thus resembles neoliberal constructions of responsible subjects as those who manage risks without relying on the state for safety (French & Monahan, 2020). This is observed in the Indian state's vision for 'Atmanirbhar Bharat' (self-reliant India) to make India a self-reliant nation during COVID-19 ("Building Atmanirbhar Bharat", n.d.). This redirects blame for the public health crisis and its (mis)management to individuals, diverting attention away from dysfunctional state institutions such as public health services which are responsible for controlling the crisis (French & Monahan, 2020).

3.2 Interplay between the state and communities

i. Communities as spies of the state

As part of the Prime Minister's national address during the pandemic, he encouraged vigilantism and snitching on lockdown violators (Sengupta, 2020). This has had dire consequences for marginalised communities even in cases which are not directly related to disease control, as this section will highlight. For example, during the lockdown, Indians were asked by the Prime Minister to switch off all lights in their homes at 9 PM and light candles or lamps for nine minutes in a show of solidarity in the struggle against COVID-19. A Dalit family in Haryana was attacked by members of a dominant community for not following this ("Covid-19: Dalit family in Haryana attacked", 2020). Heena Ruvaid, a Kashmiri Muslim living with her sister in a predominantly Hindu locality, shared:

We heard them [our neighbours] going around the colony and telling everyone, 'battiyaan band karo' [switch off the lights]. And that was really ridiculous because it was supposed to be voluntary, why do they have to enforce it?... And then we also had to...shut our lights, because if we didn't, it would look like a boycott and that would have consequences for us. We are living alone here, we can't even call our friends for help because of the lockdown. That's where I felt that there was surveillance... They were standing outside and checking who's not turning off their lights.

In addition, many state governments have put up posters proclaiming "Do not visit. Home under quarantine" outside the houses of home-quarantined persons, and pictures of such houses are being circulated on community WhatsApp groups. These posters are causing residents stress and psychological pressure: "neighbours ask to go inside even when we step out into our balcony for a minute" (Pandey, 2020). Swarna Rajagopalan, Founder and Managing Trustee of the Prajnya Trust, lives with her mother. Though she was not COVID-19 positive, this poster was put up outside her house in her building as part of preventive home quarantine after she had travelled from outside the state. She said:

The light switch for the common corridor is on my wall. When we didn't go out to put it on, nobody did. In the evening, we'd go out to put the milk bag out and it would be pitch dark. It was almost as if my wall was infected.

Previously, this section analysed that home quarantine apps prioritise digital infrastructure over physical infrastructure to control the pandemic. This also applies to other kinds of state apps, such as contact-tracing apps which provide another source of data for community surveillance. Some of these apps make it possible for users to report on other citizens and access personal data of infected and at-risk users (Gupta, 2020). For example, the CovaApp by the Punjab government allows users to report

mass gatherings, as illustrated in image 2. The RajCovid app⁵ by the Rajasthan government has an option called “violation reports” that reveals the names and mobile numbers of COVID-19 positive patients (Government of Rajasthan, 2020). The Nashik Municipal Corporation (NMC) COVID-19 app has an option for providing information regarding people suspected to be affected by COVID-19 in one's vicinity. The Swachhata app by the Ministry of Housing and Urban Affairs (MoHUA) allows users to complain against people who are not following lockdown rules or adhering to social distancing (Malhotra, 2020). The Corona Watch app shows the locations of Corona Affected Patients and their movement history of fourteen days on a publicly accessible map (KRSRAC KGIS, 2020).

Image 2: Tweet by the Government of Punjab (2020): “Is there a mass gathering nearby you? Now you can report it through #CovaApp. Just open the app in your phone click on 'Report Mass Gathering' select your district, upload photograph, give remarks and submit it.”



In this crucial hour of
#CovidPandemic, is someone
still breaking the law ?

Is there a Mass Gathering
nearby you?

Report it right now through
CovaApp!

Download Now



As mentioned earlier, the names and addresses of persons in home quarantine were made public by the state in some cities like Hyderabad and Bangalore. This was done

under the powers granted to the government under the EDA. Many of those whose details were made public wrote to the government saying they are facing ostracisation and harassment (Swamy, 2020). Data from contact tracing apps or released publicly by the state makes it easier for communities to surveil each other with negligible personal risk. Bodies are reduced to data points on these apps, and reporting bodies is reduced to reporting their data trails. For example, a 70-year old doctor was booked by the police in Bangalore for allegedly violating home quarantine when he was taking a morning walk in a park. Other walkers had seen his quarantine stamp on an app and had alerted the police. This is despite him not being sick, and observing home quarantine only as a precautionary measure after traveling home from outside the country (Swamy, 2020).

In Kerala, state police have gone as far as deploying untrained local men as community patrol squads, which has led to multiple reported incidents of the squads turning into vigilante groups and assaulting innocent citizens with sticks and crude weapons (“Vigilantism mars community policing”, 2020). Such initiatives involving “citizen volunteers” to complement police efforts to tackle the COVID-19 pandemic have been reported in other parts of the country too (Poovanna, 2020). Instead of surveilling the virus, it is the bodies of persons who may potentially be carrying the virus that are surveilled, and always suspect. State apps, such as the ones discussed here, provide a less risky way to carry out the same kind of community surveillance in a more socially acceptable manner.

Mark Andrejevic (2005) introduced the concept of lateral surveillance as the use of surveillance tools by individuals, rather than public or private institutions, to track each other. Such practices emulate surveillance and foster the internalisation of government strategies in private spaces by treating everyone as suspect and urging the public to become spies. As the previous section analysed, data for surveillance is often accessible only to dominant communities and is used for the surveillance of marginalised communities, reproducing social hierarchies. State support for community vigilante measures amplifies these inequalities by legitimising the hierarchies.

⁵ I would like to thank Tanisha Ranjit from the Internet Democracy Project for bringing this to my attention.

ii. Caught between the state and communities

While the state promotes community surveillance, it does not support its own workers carrying out surveillance on its behalf. One of the most important arms of the state for disease surveillance during COVID-19 are Accredited Social Health Activist (ASHA) workers, who have been on the front-line of community healthcare during the pandemic. Their usual tasks include creating awareness about health among communities and mobilising communities towards utilising health services, such as encouraging family planning and helping with women's childbirth and children's immunisation.

During COVID-19, additional tasks of conducting door-to-door surveys, patrolling containment zones and creating awareness about the pandemic have been assigned to them. An ASHA worker reportedly said that “we have been doing almost double the work as compared to what we used to during pre-COVID days. We now have no time to rest” (Menezes, 2020). Over a million ASHAs in various states have not been paid for months during the pandemic, and are owed money from the state, which has pushed them into debt (Rao, 2020). In addition to this, they have not been provided with adequate safety gear by the state to carry out their jobs (“The Women Warriors Fighting COVID-19”, 2020). When more than a hundred ASHA workers held a protest against these work conditions during the lockdown, the Delhi Police filed a case against them (“FIR against 100 Asha workers for Jantar Mantar protest”, 2020). ASHA workers thus face multiple challenges of being women health workers labouring on low or unpaid wages in high-risk conditions without adequate resources.

They are also positioned uniquely between the state and communities, being state workers who are usually residents of the same village or area they work in. Yet, they have little negotiating power with both the state as well as their own communities. Worse still, they have been stigmatised within their homes and communities during COVID-19, due to which their door-to-door surveillance work is seen as that of spreading the pandemic instead of curbing it (“The Women Warriors Fighting COVID-19”, 2020).

In the midst of this precarious situation, the Punjab Government launched the Ghar Ghar Nigrani (which translates to “home-to-home surveillance”) app on 12 June 2020. The app is meant for undertaking home-to-home surveillance as a tool for early detection and testing, to prevent community spread of COVID-19 (“Capt launches 'Ghar Ghar Nigrani' app”, 2020). It was made mandatory for ASHAs to collect information about COVID-19 patients through door-to-door surveys and upload this data to the app. This includes a person's name, parents' names, mobile number, gender, age, occupation, and ailments of all persons aged above 30. Prior to its launch, these surveys were being done by manually registering collected data on printed forms, which ASHA workers say were easier for them to use.

Concerns have been raised about the data collected through the app being an infringement of privacy for people whose data is collected (“Asked to get smartphones for survey”, 2020). Broadening the framework beyond privacy, it is observed that the bodies of the data collectors (ASHA workers) are put at risk because they occupy less privileged positions than those whose data they collect. This section will unpack this by highlighting the power dynamics this data is collected within. To understand this better, let us first look at the various issues that ASHA workers are facing with the app. These issues are so severe that on 15 June 2020, during the lockdown, ASHA workers in Punjab staged a protest against the app's mandatory usage (“Asked to get smartphones for survey”, 2020).

The first issue arises from the digital gender divide. Ranjit Kaur, a union leader in Punjab for the All India ASHA Worker and Facilitators Union said:

Many ASHA workers have no net [Internet] pack and no mobiles and cannot get their net packs recharged... If ASHA worker has no mobile of her own, the government has

asked her to borrow the mobile from her husband or son to use the app. (translated from Hindi)

The second issue is the lack of digital literacy among ASHA workers. Kaur said:

If we tell ASHAs to download some app suddenly, they can't do it. They also cannot type so fast. It takes 15-20 minutes for them to feed the data for one person... Most of them can read, but feeding the data is very difficult - they are not used to it. (translated from Hindi)

Third, ASHA workers have been given no digital training by the state for using either mobile phones or the Ghar Ghar Nigrani app, as explained by Kaur:

They [government] tell us as facilitators to do the training. I have twenty one ASHAs under me... So it is difficult to do the training for all of them.... Manual entry would be easier. Suddenly out of the blue they have introduced the app. They called us facilitators, told us an app has been launched, sent us one download link, and told us we have to download it and tell the same to the ASHA workers also. (translated from Hindi)

Fourth, there are many issues with the app itself, making it difficult for even a digitally literate person who owns a mobile phone to use it effectively, as shared by Kaur:

The app download is not happening properly. If it is downloading, it is not opening, if it is opening, registration is not happening. So many error messages come... When we have issues with the app, we take screenshots and tell the PHC [Primary Health Centre] personnel. They keep saying try again. Sometimes it works, but most times it does not work. (translated from Hindi)

Fifth, ASHA workers are not being monetarily compensated for the extra work they need to put in due to the difficulties in using the app. Kaur said “We get only 4 rupee per form and it takes ASHAs 15 minutes to fill one form. She has to buy or borrow a phone, buy a net pack, and recharge her phone... she won't have any profit at the end of it” (translated from Hindi). As mentioned above, ASHA workers are already not being paid even their usual compensation for manual data entry.

In these ways, newer challenges introduced through the Ghar Ghar Nigrani app have complicated the already precarious situation of ASHA workers. The use of the app is meant to make the process of surveillance by ASHA workers more efficient during COVID-19. However, the highlighted issues show that digitisation is impacting their livelihoods in devastating ways. This may also take the extreme form of violence against them: there are multiple reports of ASHA workers facing violence within the home and from community members during door-to-door surveillance (“Coronavirus: ASHA workers endure abuse”, 2020; Mohanty, 2020; Nandakumar, 2020). Kaur shared:

If someone has a cough in the village, and ASHA enters that in the app [Ghar Ghar Nigrani], if they get called for enquiry, they blame the ASHA for putting them in that situation. ASHAs are facing violence due to it... One of our ASHAs was beaten up for it... Her husband and kid were also beaten up. Migrants from another state had come to the village. ASHA had to enter that data in the app. **They did not want her to take their data, so they beat her up.** She had to be hospitalised. (translated from Hindi; emphasis mine)

News reports also corroborate the role of data collection in violence; when asked about why community members were attacking ASHA workers, some of them responded: “they [locals] avoid sharing their contact numbers fearing that they might be detained by authorities” (“Coronavirus: ASHA workers endure abuse and assault on field”, 2020).

This illustrates that people may even resort to extreme measures such as violence to keep their data-as-bodies safe; the brunt of this is borne by the bodies of those holding lesser power in that dynamic, in this case, ASHA workers. Though ASHAs usually work in the same communities they reside in, various factors have led to a power differential heightening between them and their communities during COVID-19. Earlier, when ASHA workers visited homes, they would collect health-related information of each household by interacting mostly with the women of the house while the men would be away. However, during the lockdown, ASHA workers are having to face the threat of violence from men at home (Warrier, 2020). In some cases, they are also facing violence from migrants visiting these areas who fear that “the police will take them away, that they will be made unconscious and kill them” when ASHAs record their data (Rao, 2020). As the arms of state surveillance, ASHA workers face the brunt of public anxieties and distrust of the state's data collection while their own demands and concerns remain unheard by the state.

4. Regulation and criminalisation of public mobilities by the state

So far, this study has analysed how social inequalities have been exacerbated through the use of data for surveillance during COVID-19 in the spaces of families and communities, and in some cases, aided by the state. Sections 4 and 5 now focus upon surveillance practices directly carried out by the state during the pandemic.

State restrictions upon the mobility of persons in public spaces have been a key feature of the COVID-19 lockdown globally. There is divided opinion on whether this has been helpful. According to the Indian state, a lockdown with mobility restrictions was the best strategy for COVID-19 as the virus spreads by contact (Saha & Bindal, 2020). Critics suggest that, in India, the lockdown was a political decision, rather than an epidemiological one. They argue that since the lockdown was initially implemented when the officially reported number of cases was low, it was a political strategy to buy more time for the state to prepare for the pandemic (“CDC New Covid Guidelines”, 2020). During this time, people's livelihoods became collateral damage, especially those of the poor who could not afford to stay indoors without pay (Karpagam, 2020). A better strategy, critics suggest, would have been easing mobility restrictions and implementing large-scale testing (Vij, 2020).

This regulation of public mobilities has also been accompanied by criminalisation of the pandemic. Criminalisation is often aimed at prevention and deterrence, or punishment. During a previous health pandemic, HIV, criminalisation occurred without any evidence that a criminal justice response assists in HIV prevention (Mykhalovskiy, 2015). On the contrary, HIV advocacy has shown that criminalisation is ineffective, disproportionately impacts marginalised communities and negatively impacts public health. Despite this, there has been a rise in punitive approaches to infectious diseases (Hoppe, 2018), including COVID-19. Powers granted to the central government under the Disaster Management Act, 2005 were invoked to enforce the COVID-19 lockdown in India. The police were authorised to arrest and detain those found violating government orders. The Maharashtra police registered 1,33,730 offences

and arrested 27,446 people for violating prohibitory regulations during the lockdown (“133,730 FIRs registered”, 2020).

Historian David Arnold contends that a primary role of colonial police was the control and surveillance of Indian subjects of the British Empire (1986). In the context of healthcare, historian Tarangini Sriraman (2020) argues that the Epidemic Diseases Act was a “medical surveillance tool”, enacted to target the cart-drivers, sweepers, cleaners and sanitary workers who mostly were part of marginalised castes. Drawing upon this work, Nikita Sonavane and Ameya Bokil argue that the colonial system has continued in the post-colonial state with marginalised communities being the primary subjects of state surveillance (Bokil & Sonavane, 2020). This section analyses the role of data in regulating and criminalising mobilities in public spaces during COVID-19 as a form of control over bodies from a distance.

4.1 Drone patrolling

Surveillance during COVID-19 has largely been rooted within the criminal justice system instead of the public healthcare system (Joshi & Kak, 2020). One of the surveillance tools used by the criminal justice system in India during COVID-19 is drones. Drones have been used to monitor movements of people in various states (Barik, 2020a). These drones are equipped to capture images of persons on the ground, detect distances between humans, and send GPS coordinates of lockdown violators to the police. Police have also made arrests on the basis of drone footage (Barik, 2020b).

Bilal⁶ is a daily wage labourer residing in a predominantly Muslim locality in Jharkhand. He recalls that, during Ramzan, “people were coming out of their homes for the daily rozana, but social distancing was being maintained.” At the same time, “drones were deployed because maybe police were scared that people were coming out too much.” He added that “people were scared of drones capturing their images. Men used to move to the sides of the roads when drones were coming.” (all quotes translated from Hindi)

Salma⁷ is a resident of another predominantly Muslim locality in Jharkhand. She works as a nurse in a gynaecologist's office and is a single parent to her children. She observed:

People were not getting medicine because if they left the house, drones were coming and monitoring, and people were being scared so they'd go back inside...They [police] had kept the lanes closed and blocked so we could not leave the house. Police were guarding the barricades. People were scared of the police, and on top of that, drones were flying over our heads. (translated from Hindi)

When asked why people were scared of the drones, she mentioned that people had no evidence for what purpose they were leaving their homes to go out. In her own case, she said, “it's not written anywhere that I am going for work... that's why I was scared” (translated from Hindi). None of the people I spoke to had been informed about why drones had been deployed in their localities. “Maybe drones were deployed because the police thought that people were coming out of their houses,” was Bilal's guess (translated from Hindi). Their fear of drones was also linked to this lack of information, and the worry that the police would catch them through the images captured by the drones.

Salma recounted an incident during the lockdown when she received an urgent call for assistance with childbirth in the neighbourhood. The pregnant woman was in such a critical condition that Salma said,

⁶ Name Changed

⁷ Name Changed

“either the child would survive or the mother” (translated from Hindi). She narrated:

When I got the call, it was around 8:10 PM... We could not take out our vehicles. We could not call an ambulance. Our locality was entirely seized. We could not even step out... I was very scared. But my job requires me to go out for childbirth... **I took Allah's name and stepped out...** I went to the lane outside my house, the pregnant woman's family had come till the end of my lane to pick me up by walk, and they said 'if police come, we will respond to them, you come with us'. One man from her family moved the police barricades a little, and we bent down and went through them. **Drones were flying overhead the whole time. This happened at night, there were no street lights outside, so we hid in the dark close to the footpaths and walked quietly to their house.** (translated from Hindi; emphasis mine)

In Kerala, visuals recorded by drones were posted on the police department's official social media pages; people are trying to cover their faces and hide behind trees and rocks to evade being seen by drones (“Kerala police uses drones for surveillance, visuals become viral”, 2020). In some cases, drones have also been regulating mobilities in private spaces. For example, in Kolkata, it was reported that the police have started urging residents to not assemble on their terraces during the lockdown, after images captured by drones revealed that people were mingling on the roofs of their apartment buildings (Javed, 2020).

As mentioned earlier, one of the ways in which technology-mediated surveillance differs from earlier forms of surveillance is the ability to facilitate control of bodies from a distance without requiring human presence to monitor (McCahill, 1998; van der Ploeg, 2012). The previous section analysed how this happens through quarantine apps within the home. Drones are a manifestation of such state control in the public sphere, and in some cases, extending to private spaces such as balconies of homes as well, as seen here. Through the threat of digital images captured by drones, our physical bodies are being disciplined to stay at home, without any police official having to be physically present.

Surveillance through drones makes health workers have to hide in order to save the lives of pregnant women. It makes Muslims scared of meeting each other during religious festivals despite maintaining physical distancing. It stops people from leaving their houses to buy medicine during a health pandemic, as observed in Salma's experience with drone patrolling mentioned here. These are severe restrictions upon people's mobility in public spaces, with material consequences for their lives, enforced through criminalisation. When individuals experience fear and modify bodily movements as a direct consequence of the threat of drones capturing their digital images, then data is being used to determine bodily experiences.

4.2 Mobile location tracing

States such as Delhi (Kejriwal, 2020) and Kerala (Sebastian, 2020) have announced measures to track the movements and locations of persons in home quarantine through their mobile data. It has been reported that the police were using mobile phone data to trace people who attended or were in the vicinity of the Tablighi Jamaat event in Delhi which was introduced in section 2 (Sanyal, 2020). Various state governments also released public lists of people (including their names and mobile numbers) who were thought to have attended the religious event (Das, 2020).

On one of these public lists was Mir Saqib, a Muslim resident of Srinagar, Jammu and Kashmir, who said he had not attended the congregation at all. He shared:

I didn't know what had happened. There was some problem with Tablighi, that there is COVID-19 in the Nizamuddin area or something. So the government had maybe pulled data through phone networks of which Kashmiri mobile numbers were present near Nizamuddin from 13 to 15 March. I didn't go to Nizamuddin but I was in [name of place about 5km afar redacted] that time. I don't know how this happened to me. So my name had come, along with 850 other names, on the list. I did not know about it, someone told me that my name is on the list. So I was puzzled that if my name was on the list, then how did it become public? They should have called me and told me that you are on the list, are you okay? But they made it public. (translated partly from Hindi)

Saqib described in detail how he would get calls every day from various personnel in local police stations as well as the state health department after the list was publicly released. They asked him repeatedly for his name, travel history, mode of travel, and residential address. He was also asked for his passport number by the police. He continued:

I found out that they went to [official permanent address redacted]... but I don't live there right now. It was kind of like witch hunting. It was not done in a sophisticated or professional way, the way it should be done... It was very scary, nobody would come to me, talk to me, it was like all of a sudden, everything changed. So I felt like if they really cared... they should have told me... But they created such a situation of panic... where I was not able to step out. (translated partly from Hindi)

He voluntarily home-quarantined for 15 days and, at the end of this period, was asked to get tested for COVID-19. He spoke about the fears and anxieties he experienced in the few days that elapsed between his test and receiving the results:

I thought if I don't go [for testing], they might file an FIR against me or they may make it public again and that will be very bad. So I went to get the test done... The result came negative... It took some time for the results to come, and I was worried whether it would be positive. One day when I was sleeping at home, a neighbourhood friend called me up and told me that someone is searching for you. When I looked from the window, there was an office van with a few people downstairs. I thought that I was positive and they have tracked me down and they have come to take me. So it was very scary. When I came down, I found out that they were looking for somebody else. So it was a very scary experience to suddenly have... At the back of my mind I was constantly thinking that they might track me, they might find me, if I am positive they won't call me, they'll just come and take me away. (translated partly from Hindi)

How Saqib had been surveilled through the tracking of his mobile phone location data played a key role in adding to his anxieties, as he shared:

Till the results came, it was very scary whenever anyone would come knock on my door, I would wonder who it is. Because just the way they had traced my mobile number for Nizamuddin, I felt that they could trace me now also. **Someone told me to always leave my phone at home if I went somewhere, in case they trace my location through it again... I think they kept a watch on me...** they are keeping an eye on me, I felt... They can stop me from foreign travel, **they can stop me from going anywhere... if they have a database, they can find me.** (translated partly from Hindi; emphasis mine)

It is important to understand this experience through the perspective of a Kashmiri Muslim in India. Kashmir has a long and troubling history of state surveillance and repression. Following the abrogation of Section 370 of the Indian Constitution, it has been under constant surveillance (Ayyub, 2020). The Indian state suspended Internet services in the state, making it the longest ever Internet suspension in a democracy. When the state restored Internet services, it did so only partially, resuming limited services on 2G data speeds. It took me weeks to contact Saqib and have a video call on shaky 2G mobile internet. The Indian state already exerts discretionary powers to surveil its citizens through technology, and the COVID-19 public health crisis has given the state a justification to amplify such surveillance.

Crucially, when the state was keeping a watch on Saqib's location data, he experienced it as the state keeping a watch on his body (“I think they kept a watch on me”). When he further mentions that “someone told me to always leave my phone at home if I went somewhere in case they trace my location through it again,” it underscores that our bodies are interconnected to our data to such an extent that we feel the need to sever that connection (such as by leaving the phone behind) if we don't want our bodies to be tracked and controlled through our data.

Any concerns that mobile phone users may have with mobile phone tracing are addressed by reference to privacy policies which place an emphasis on personally identifiable information rather than the fact that groups of people may be categorised and characterised in particular ways (Lyon, 2003). Thus, the discourse that focuses on the personal affronts of personal data collection ignores the structural effects of mobile location tracing. In this context, the misuse of data (such as Saqib's personal data being publicly released on a surveillance list) is concerning not only because of data privacy. Data privacy, as traditionally defined, does not capture the intimate feelings of anxiety, fear, public targeting and shaming that Saqib expressed he experienced, nor does it capture the material realities of the restrictions on his mobility that were a consequence of the data misuse (“they can stop me from going anywhere”). To foreground these harms, the body must be visibilised in constructions of data.

5. Exclusion from essential services, rights and social protection

The harms of surveillance during COVID-19 analysed so far have been consequences of measures *intended* for surveillance, at least to some extent. This makes these harms more visible once the framework of embodied data is employed, as seen in previous sections. These harms also seem more explicit and dangerous, such as direct physical violence. However, there are some forms of surveillance which do not receive the same degree of attention because they are often not viewed as surveillance measures, making their harms more difficult to point out. For example, harms experienced by rural communities from the datafication of welfare delivery systems are often categorised as last-mile connectivity challenges as opposed to surveillance measures, even though they have the effect of surveillance, as will be examined here. This section analyses some ways in which marginalised communities encounter surveillance while trying to access essential services (such as healthcare and banking), rights (such as employment and travel) and social protection schemes during COVID-19, by making their harms explicit.

5.1 Mandatory digital requirements

i. Aadhaar

Aadhaar, a 12-digit unique number issued by the Unique Identification Authority of India (UIDAI), is mandatory for accessing various essential services such as the Public Distribution System (PDS) schemes for subsidies. A lot has been written about the technology-based exclusion that this causes—from issues with enrolling for Aadhaar cards to biometric failures to surveillance concerns—severely affecting marginalised communities who depend upon these services for their livelihoods (Khera, 2017).

During COVID-19, the requirement for Aadhaar has been expanded to cover many previously unlinked services. For example, in 2019, the Odisha government had already made the linking of ration cards with Aadhaar mandatory, which was reported to exclude 1.9 million people in the state from the PDS (“Aadhaar-ration card link”, 2019). During the pandemic, the Odisha government issued another order, mandating Aadhaar to access pension benefits, which is expected to impact 1.1 million pensioners (“Odisha makes Aadhaar mandatory for pension”, 2020). As a result of this, during COVID-19, many people are not receiving their rations and pensions (Dash, 2020; Dhara, 2020). An 83-year old bedridden woman who had already lost her ration card for not having Aadhaar was further denied ex gratia support of Rs 1000 with her pension for not having Aadhaar (Right to Food Campaign, Odisha, 2020).

Aadhaar is also required to access healthcare services during the health pandemic. Ahmedabad made it mandatory for people to submit their Aadhaar details to qualify for COVID-19 tests at the city's urban health centres (Kaushik, 2020). In Bangalore, a COVID-19 patient died after two hospitals denied him treatment without his Aadhaar card details (“Bengaluru hospitals demand Aadhaar details”, 2020). Raina Roy, herself a trans woman, narrated a recent case wherein a COVID-19 positive trans sex worker, Meena,⁸ needed to be hospitalised for treatment in West Bengal. Because there was no separate transgender wing in the hospital, she was admitted to the female ward. However, even if a separate ward had been present, if the trans sex worker did not have a valid identification proof that mentioned their transgender identity, this could have caused problems, as Roy shared:

People who have no identity card saying they are transgender, they might be in problem if they become COVID-19 positive... Because there are lots of issues. People are not open in their family and neighbors, so they always have this [fear] that if I make my voter card as transgender [or preferred gender] then what will be the problems within the family... The government is not sensitive about people who are still hidden, who only open their identity within the [trans] community. So in that case, they will count it as either male or female. So this problem will arise if someone like this gets positive. The government is trying to create some [provisions] for trans persons, but for that the identity card will be a big issue... If your voter card and Aadhaar card is the identity, then it's problematic practically for the trans community.

Chellamma,⁹ also a trans woman, says that “the principle way in which surveillance is happening during COVID-19 is through trying to document trans persons by saying that you will not get your entitlements if you do not have certain documents”. Such identification documents are a means for the state to “get to know us and to then control and manage trans people's bodies,” she adds. While this has been true since before the pandemic, it has devastating consequences at a time when access to health services is crucial

⁸ Name Changed

⁹ Name Changed

Through biometrics used for Aadhaar authentication, the physical body itself is becoming a “machine-readable body” (van der Ploeg, 2003). This has translated human identity to a new form of digital identity (Aas, 2006). The consequences of not being able to authenticate this identity has led to life-and-death situations for people when they are denied rations, pensions, and timely hospitalisation, as seen in the examples here. While most of the focus on Aadhaar has been around data protection, this narrow focus will not help to prevent such bodily harms from occurring or to provide recourse when they do (Kovacs, 2018).

Moreover, this biometric body is considered to be a “source of truth” which is privileged over the corporeal body (Aas, 2006), irrespective of whether this represents a person's physical reality (Ball, 2016). For example, when people are denied access to essential services because they do not have valid digital identification, it highlights that without linking our bodies and personal information with our biometric data, we cannot 'prove' whose body this really is (Kovacs, 2020), even if our bodies are physically present to access these services.

Not only do digital identities take precedence over corporeal identities, they also slot people into inflexible categories determined by biometric data, hampering our autonomy to make decisions about our lives. For example, when Aadhaar was made mandatory for accessing rehabilitation schemes for manual scavengers, Bezwada Wilson, the head of Safai Karmachari Aandolan (SKA) that represents manual scavengers, had argued as an intervener in the Aadhaar legal challenge:

Any marginalized community, any manual scavenging or vulnerable community wants to destroy its existing identity; that is our whole struggle... Even if I come out of this and get liberation also, but in your Aadhaar, my occupation, where I come from, everything will be there. (Deshmane, 2017)

Thus, there occurs a reification of categories through a fixed digital identity (Bhatia, 2019), highlighting that digital identities remain affixed to people, becoming “like a person's shadow: hard to fight, impossible to shake” (van der Ploeg, 2012). People become mere data points and are slotted into categories which are used to make decisions about them that they often have no control over, but face devastating consequences of. Since the mandatory requirement of Aadhaar to access essential services ends up excluding the poor from welfare systems, this becomes a surveillance concern where bodies of the poor are socially controlled through their digital identities. During a health pandemic, such exclusion from accessing essential services due to a lack of valid digital identification is leading to the deaths of people who are in need of medical care, as seen here.

ii. Aarogya Setu

Aarogya Setu (which translates to 'bridge for liberation from disease') is a COVID-19 contact tracing app based on user self-assessment. It was jointly developed by National Informatics Centre and volunteers from the private sector (Agarwal, 2020) and was released in April 2020. Aarogya Setu works through self-declaration of health symptoms on the app combined with location data from Bluetooth and GPS. With this data collected from all mobile devices that have this app installed in a given area, the app claims to determine the risk of a person being near someone who is COVID-19-infected and the risk of potentially being in a COVID-19 hotspot.

Privacy concerns have been raised about data sharing on the app since its privacy policy does not lay out the purposes for which data is being collected (Jain & Ranjit, 2020). Other concerns such as

proportionality, legality and necessity of data collection, along with lack of oversight and accountability measures have also been raised (Internet Freedom Foundation, n.d.). Due to all of these issues, it has been criticised for being a surveillance system (Sen, 2020).

The app was also temporarily made mandatory by state as well as industry stakeholders for accessing various essential services such as the Indian railways, private airlines, and metro travel, as well as for central government and industry employees (Ranjit, 2020b). As an example of the app being required to access state healthcare services, Sandeep Narwani, a resident of Delhi, shared:

I went to get myself a COVID test at a Delhi government testing center. I was waiting in line, and when my turn came, they asked me... if I had downloaded the Aarogya Setu app. They said it's mandatory. I said my phone does not have any memory in it right now. They said, 'delete some apps on your phone and make space for it,' in a very condescending tone. I was not sure whether to just focus on my health, download the app, and get the test done or to fight back... I told the doctor that the need to have the app is not there in the government rulebook. She said 'without that, I cannot upload your data as per ICMR [Indian Council of Medical Research] guidelines.'

I found no mention of the app being required in the publicly available ICRM advisory (Indian Council of Medical Research, 2020), indicating that requiring the app for COVID-19 testing may not be strictly legal.

In early May, guidelines issued by the state made the app mandatory for office employees of the private sector, with the heads of companies to be held responsible if employees violated the order (“Aarogya Setu app compulsory”, 2020). Bhupen¹⁰ is an employee of an Indian company that released guidelines mandating the download of Aarogya Setu for those who wished to visit the company premises during the lockdown. He said:

I had to go to get a new laptop from the office. For us to do that... we have to show the [Aarogya Setu] app is installed, and then go through questions on the app and ensure they are answered. Someone is standing and checking at the office for this. Just having the app installed is not good enough for them. Then after answering the questions on the app, we'd be given access to the office... I had not answered these questions. I was hoping to get past by just showing that I had installed the app. But they ensured that I was responding to the questions. After coming out of the office, I uninstalled it immediately... I have not gone back to the office since then. I am working from home.... As someone who believes in data privacy, I was really unnerved by the experience considering the privacy concerns with the app.

Since the nature of Bhupen's job permitted him to do so, he could uninstall the app after he left his office and continue working from home. However, for workers from marginalised class locations whose jobs cannot be done from home, this can have more serious implications for their livelihoods. For example, the app has been made mandatory by transport and food delivery companies such as Uber, Ola, Swiggy, and Zomato for their transport workers (Chakravarti, 2020). Shaik Salauddin, the national General Secretary of the Indian Federation Of App-Based Transport Workers (IFAT), shared:

If I don't have trust on this app, then the choice to download or not download should be mine, not my company's no? ... Where did you get the right to do this from? This is not your constitutional right to mandate people to download it... **How do you have the**

¹⁰Name Changed

right to stop someone's livelihood and daily bread-and-butter because they did not download it? (translated from Hindi) (emphasis mine)

When the app is linked to accessing employment for some workers, marginalised communities are the first to lose out. Highlighting the class-divide in the app's usage, Salauddin further shared:

Only third-category of daily wage laborers, BPL [Below Poverty Line] persons have the app... Why are the rich not using it? Do they not know the app? Do they not trust it? Are they worried their data is getting stolen? Are they scared the app will record when they sit, stand, move?... The person who has to book an Uber does not have the app. Why is that so? If it is compulsory for the drivers, then even for people booking the app, it should be compulsory...If I am the CEO of Uber, why can't I incorporate the Aarogya Setu app into the Uber app? Because my data will get stolen. Your data should not get stolen, but if the driver's data gets stolen, that is okay? (translated from Hindi)

Nagesh Kumar, state vice-president of IFAT, highlighted its long-term potential harms for transport workers:

The companies having access to the health data of the employee through this app could also effectively screen which individuals should be terminated from their positions or reduce their rides/deliveries if they report on the app of any ailment or discomfort. This would ensure that the companies don't have to shell out any relief or insurance aid in case the worker is suffering from any ailment or has contracted the virus while working for them. ("Workers flag privacy concerns over use of Aarogya Setu app", 2020)

This shows that when data is collected about individuals on a large scale, it can be used to profile or socially sort them into risk categories (Lyon, 2003). This is also what lends such data collection to being a form of mass surveillance. Through our self-reported health data on the app and the assimilation of such collected data from other mobile devices, our bodies are being categorised as 'diseased' or 'healthy' and 'low risk' or 'high risk' on the app. This categorisation may seem legitimate during a health pandemic. However, when these assessments are made without heed to their social contexts, they have concrete consequences for the immediate futures of individuals, including their exclusion from essential services, jobs or insurance, and ability to continue livelihoods.

Moreover, it is important to note here that this categorisation based on collected data may not necessarily reflect reality. In other words, the digital realities constructed through the app are unlikely to correspond to the state of our physical bodies for various reasons.

First, as has been discussed here, many people either do not own smartphones or do not have the app installed on their phones for concerns around data privacy. Since the app calculates a person's risk of infection based on their proximity to others who have reported to be COVID-19 positive on the app, this is effective only when a critical mass of people one comes in contact with also have the app.

Second, as mentioned earlier, one of the factors for the app to indicate the likelihood of a person being infected is the self-reporting of symptoms. Since self-reporting precedes actual medical testing (which is a more accurate metric to determine whether one is infected), self-reported symptoms are themselves not entirely reliable given the asymptomatic nature of the disease in many cases. For self-reported symptoms to be accurate and verified medically, there needs to be large-scale testing for the virus. However, India has an abysmally low testing rate (Bhardwaj, 2020).

Third, as Salauddin questioned, “In today's world... why will anyone declare their symptoms on the app honestly? Nobody will... So what is this app proving? Nothing.” (translated from Hindi). The stigma attached to the COVID-19 virus (as discussed earlier in this study) is one of the reasons why people may hesitate to self-report accurately on the app. This also makes it possible to game the system to an extent and represent a form of digital reality that does not correspond to one's physical reality.

Fourth, there may be occurrences of false positives or negatives on the app (Jain & Ranjit, 2020). For example, since the app works on Bluetooth which travels through walls, it may indicate that people on two different floors have been in contact, even if they haven't (Clarence, 2020). A woman with no COVID-19 symptoms was forcibly quarantined in Mumbai after an alert was generated by the Aarogya Setu app that she had installed on her phone, despite not having uploaded her medical history on the app (“Woman with no medical history, symptoms quarantined by BMC”, 2020). Other such cases of false positives have also been reported (Sapkale, 2020).

For all of the above reasons, the digital reality constructed by the app may not correspond with an individual's physical reality. However, the data on the app is what ultimately matters to evaluate whether someone poses a health risk to others and vice versa. For example, if one's neighbour is COVID-19 positive but this data is not reflected on the app due to any of the reasons analysed above, then that health risk is not detected and flagged. Once bodies have been translated into digital representations and categorised into risk categories through their data as seen here, the attributed identities become affixed to a person (van der Ploeg, 2012), irrespective of whether the person actually fits into the assigned category or not. By mandating the app, this digital reality has far-reaching consequences for a person's physical reality, such as exclusion from accessing essential services (such as healthcare) and rights (such as travel and employment). By collecting data about people's health symptoms and locations on a large scale without effectively helping with contact tracing, Aarogya Setu adds to the state's surveillance infrastructure while being marketed as a justified requirement during the pandemic.

5.2 Social protection schemes

“Who could have thought that the money this government sends will reach the beneficiaries directly? Especially when everything was shut down. The JAM [Jan Dhan-Aadhaar-Mobile] trinity had this effect.”

- Prime Minister Narendra Modi, national address May 12, 2020
(translated from Hindi)

“I have received not even one rupee from the government through any scheme.”

- Satya, migrant laborer from Jharkhand (translated from Hindi)

An important way to ensure that health pandemics do not turn into socio-economic crises is through social protection, which ensures that the livelihoods of the poor and marginalised remain protected. During COVID-19, the state implemented various social protection schemes for the poor, relying upon technology-mediated methods such as direct benefit transfers (DBTs) (Direct Benefit Transfer, n.d.) and the JAM (Jan Dhan-Aadhaar-Mobile) Trinity (Digital India, n.d.). Despite this, according to a survey across 23 states, 23% of the respondents had to borrow money to manage their household, and 8% had to sell a valuable possession (“During lockdown, rural India faced insurmountable sufferings”, 2020). Another survey among low-income households across 15 states showed that only 19% of people were satisfied with how much government entitlements helped them navigate the crisis (Data Dashboard, n.d.).

By exploring various layers of technology-mediated exclusions, this section argues that instead of helping people during a crisis, technology-mediated social protection schemes, when designed without understanding socio-economic contexts, add to the infrastructure of state surveillance during the pandemic.

i. Apps for financial assistance to inter-state migrants

Among the worst impacted by the COVID-19 lockdown have been migrant labourers stranded in the states they work in, away from their families. With transport services shut down, troubling images of migrants walking thousands of miles by foot on roads, carrying their belongings and children, have been reported (“Migrants continue to walk”, 2020). In the midst of this, some states introduced relief schemes to provide financial assistance to migrants who were stranded outside their home states.

Among 15 surveyed states, only 53% of low-income households knew which government schemes they were eligible for during the crisis, with awareness in West Bengal being as low as 21% (Data Dashboard, n.d.). For example, the state of Jharkhand promised Rs 1,000 to each migrant who is stranded outside the state during the pandemic, under the Chief Minister's Special Assistance Scheme. A migrant, Satya, said:

Nobody has told us anything. We don't know about any of these government schemes... We are just waiting for almost a month now, but we have not seen any money... When we were living in the school [quarantine facility after returning from a different state] for 15 days, one man came to the school - I don't know his name - he said we should get 1000 rupees. I don't know what to do to get that money. But nothing has come yet. (translated from Hindi)

Availing of this scheme also requires the installation of the Jharkhand Corona Sahayata App on your smartphone, an Internet connection, and a Pradhan Mantri Jan Dhan Yojana (PMJDY) account registered in Jharkhand (Government of Jharkhand, n.d.). PMJDY is a financial inclusion program of the Government of India to expand access to financial services to all Indian citizens. Each mobile device can be used to register only one migrant, and this is verified through a geo-tagged selfie that the migrant is required to upload to the app. The state of Bihar has a similar scheme for Rs 1,000 with the same registration requirements (Bihar Government, n.d.).

Reshma is a Programme Coordinator at the Association for Advocacy and Legal Initiatives (AALI) in Jharkhand, working with migrants to secure rations for them during COVID-19. She mentioned that the requirement to have an individual phone is a hurdle to access this scheme since in most cases, phones are shared in poorer families. It has also been reported that many migrants have been unable to register for this scheme as they do not have an internet-enabled mobile phone (Mishra, 2020). Even for those who have access to phones, the situation is grim. I explain this by laying out three cases of inter-state migrants who did not receive the money from this scheme due to failures on the app.

First, as mentioned earlier, the migrant's bank account has to be registered in the home state to be eligible for the scheme. A migrant labourer, Satya,¹¹ who had returned to Jharkhand (where he lived) from Gujarat (where he was employed before the lockdown) was unaware of this requirement. Being an inter-state migrant, he had worked in Gujarat for many years, so expectedly, his bank account was registered in Gujarat. He had tried registering for the scheme by entering his Gujarat bank account

¹¹ Name changed

details into the Jharkhand Corona Sahayata App. He was repeatedly shown an error with the registration, but due to limited digital literacy, he was unable to understand why the registration was failing. Reshma explained the available redressal mechanism:

After you submit the bank account number on the app, the user receives a receipt of registration... If there is an issue with the money not coming to the bank account, after showing this receipt to the block Labour department, the person can find out the status of their application. (translated from Hindi).

Satya told me that he checked with the bank to follow up on the status of his money: “It has been twenty, twenty five days since I have opened the bank account in Jharkhand. The money that we are supposed to get if we come from outside the state, I have not received a rupee of that“ (translated from Hindi). The bank itself had not received this money from the government since his registration for the scheme had failed on the app. The scheme was valid only for inter-state migrants, and having made the journey back home, Satya was no longer eligible for the scheme. He was also not able to raise a complaint because of the failed registration on the app due to which he had not received a registration receipt, without which he could not claim any redress. Reshma further shared:

People have no information about this process. Banks that have a target of opening a certain number of accounts are getting new accounts opened for migrants. But whether the money will come into that new account is an entirely different matter. If the registration process itself is failing on the app, then having a new bank account is not going to help in getting the money.... You have to first successfully apply for the scheme. (translated from Hindi)

Second, during a public event, Navmee from the Stranded Workers Action Network stated: “for the Jharkhand Sahayta app, there were GPS issues. A labour group stranded in Bihar was shown to be in Jharkhand, and thus was considered ineligible [to receive money].” (Jan Sarokar/People's Agenda '19, 2020).

Third, a report mentions that a migrant's selfie was not accepted on the app despite trying 8-9 times because his beard had grown and he did not have a beard in the picture on his Aadhaar card (Stranded Workers Action Network, 2020). Due to this, he did not receive the money from the state and had to use his savings to travel back home.

In all of these cases, the app requires migrants to provide a digital proof of their physical realities. This could be in the form of a selfie, bank account number, GPS location, or Aadhaar number. When the physical realities of migrants don't match these digital identifiers, as seen here, it is considered a 'data error' or an 'authentication failure' on the app. In other words, a person's physical presence is not 'authentic' enough for the app unless it is corroborated with a digital identity.

But the harms of this are not experienced merely as 'data harms' by those who fail to receive their financial entitlements due to the error. When people's bodies are datafied, these data points are used to make decisions about them (such as whether they are eligible to receive money), with people having no control over these decisions (Kovacs, 2018). When the data makes wrong decisions, these 'data errors' can have life-threatening consequences for the poor. In this case, a failure to register on the app could lead to them not receiving the money under the state scheme. As a result of this, migrants have to pay out of pocket to travel back to their homes. Satya said:

There was so much expense to travel from Gujarat to Jharkhand, what to say? It cost me around 4000 rupees in total for the trip. I had taken out a loan to get money for my ticket to come here. Now I am not getting any work to do here. I am just sitting at home right now. Nobody else in my family is employed. (translated from Hindi)

ii. Controlling financial data of the poor

Knowledge is power, and knowledge about one's banking information is crucial to make financial decisions, especially during a pandemic. However, there are various technological issues with accessing such information about money from social protection schemes. Many of these issues predate the pandemic but have been exacerbated by it. This section describes the challenges that people are facing with accessing this information and its implications upon their lives.

First, many state schemes require Pradhan Mantri Jan Dhan Yojana (PMJDY) accounts to access cash transfers from the state during COVID-19 (Pradhan Mantri Jan-Dhan Yojana, n.d.). However, according to a recent study, less than half of poor adult women have a PMJDY account, and many women are unaware of the details of their accounts (Pande, Schaner, Moore & Stacy, 2020). Drishti Agarwal and Manju Rajput from the Aajeevika Bureau said that women often have multiple PMJDY accounts under various state schemes, with each account linked to a different scheme. As a result of this, “women are confused about which accounts give access for what, and which accounts the COVID-19 money is coming to” (translated from Hindi).

This issue has persisted for a long time in part due to the pressure that banks faced to open accounts for people in large numbers to meet the targets of the PMJDY when it was initiated. This resulted in duplicate accounts and issues with mapping Aadhaar numbers with these newly opened bank accounts (Dhorajiwala & Wagner, 2019). Many PMJDY accounts became either dormant as customers were not able to access them (“Almost every fifth Jan Dhan account 'inoperative’”, 2020) or were blocked (Dhorajiwala, Dreze & Wagner, 2019) because account holders could not complete biometric authentication for Aadhaar numbers linked to their accounts.

Second, an SMS update is sent to the registered mobile number when money from DBTs is credited to a bank holder's account; however, there are some issues with this. Referring to the gendered digital divide, Agarwal and Rajput shared:

Since women are mostly illiterate, they can't read these messages... Even if they can read, the phone is usually the man's, and if the man is not in town, she will not know if the message has come to his number or not. (translated from Hindi)

For women with disabilities, there is high dependence upon able-bodied family members to access money that is transferred directly to the bank accounts of the women (Rising Flame & Sightsavers, 2020). For Dalits and Adivasis, control of the bank account is usually with an upper caste literate landlord or the ration shopkeeper (Sur, 2020). In villages, Agarwal and Rajput added: “An OTP is sent to the mobile number after registration. In panchayats which don't have mobile connectivity, the OTP does not come” (translated from Hindi).

In some cases, bank account holders are not receiving SMS updates on their mobile numbers due to erroneous mapping between mobile numbers and Aadhaar numbers. While it is not mandatory for Aadhaar to be directly linked to mobile numbers, it is mandatory for bank accounts to be linked to Aadhaar numbers under Digital India, and it is through this process that mobile numbers get indirectly

mapped to Aadhaar through an individual's bank account. In some cases, this mapping is done erroneously (Narayanan & Dhorajiwala, 2019), and in other cases, the mapping does not happen at all. Since people are entirely dependent on these digital modes of payments and information during COVID-19, “the message not coming on the phone is a big loss for people... they don't know how much money is there in their accounts,” as observed by Agarwal and Rajput (translated from Hindi).

Third, there are issues with 'bank correspondents (Kulkarni, 2020)' who provide essential services such as cash withdrawals through Point-Of-Sale [POS] devices (swipe machines) enabled with biometric verification to locals in their homes. Agarwal and Rajput said that POS machines do not provide details of the current account balance and transaction history. They said: “bank persons always say, 'why should these people know all this, what will they do finding out their transaction history?'" All the people we spoke to said this was essential information for them, that they wanted to know.” This highlights not only the technical drawbacks of POS devices, but more importantly, patronising attitudes of banking correspondents towards the rural poor.

Fourth, banks and banking services are inaccessible during COVID-19 due to banks being very far away from remote areas (Times of India, 2020), being overcrowded with long queues (Dreze, 2020), and lack of access to ATMs in rural areas, making it difficult to withdraw money in these places. Agarwal and Rajput said: “In the bank, from the past 2-3 months, diary entries [bank statements] have been closed. The excuse they give is that coronavirus is there, so there is a fear of being infected. In remote areas, these services are all shut right now.” (translated from Hindi). Due to this, people are unable to get information about their accounts.

Digitisation was aimed at improving public access, removing the offline hurdles associated with it, and building people-centric systems. However, digital systems have not only failed at improving access but have created further complexities for people in accessing information and services, as seen here. This is especially problematic in the midst of a pandemic during which no non-technological alternatives have been made available to people for receiving money and financial stability has become a matter of life and death. Even if well-intended as a form of social protection, digitisation measures such as linking various pieces of information about citizens like mobile numbers, bank account details, social identity markers and location history enable state surveillance. This most significantly harms the marginalised who are the most dependent on it.

Monahan (2009) analyses surveillance to be not just about social control through technology, but more broadly a system of identification, monitoring, tracking, and data analysis. Systems which may not originally be intended for the purpose of surveillance may also have the effect of surveillance by imposing some degree of social control through data (Fisher, 2006). For example, Electronic benefit transfer systems for American welfare recipients are a method for the state to surveil poor, racialized women, by labelling them to be people in need of paternalistic supervision (Monahan, 2010). While welfare reforms through digital measures in the US were introduced to prevent fraud, they track purchases made by the poor with devastating consequences for their budgeting strategies (Eubanks, 2012). In India, welfare delivery through digitisation has been critiqued in the context of Aadhaar (Ramanathan, 2019). Such literature on the subject has crucially focused on the discrimination faced by people through surveillance while accessing social protection.

This study further analyses that the challenges highlighted in this section arise fundamentally because the state views data as a resource to be made available to people to empower financial and banking services. While doing so, it does not consider that data exists within social contexts. Knowledge is indeed power, but what happens when this knowledge is not available to those whose realities it is based upon?

It is crucial for the poor to have access to their own financial information such as account balance, transaction history, and notifications of money being credited to their bank accounts. This is especially true during a health pandemic when ill-informed budgeting strategies that are dependent upon such information can push people into poverty. This financial information about individuals is available to the state and banking institutions, but not to the individuals themselves because of the social contexts that this information exists within, as seen here. By making technology a requirement to access financial services under Digital India, people lose control over their own financial data and consequently over their ability to make informed financial decisions about their lives. By controlling people's financial data, the state and financial institutions are thus able to control people's livelihoods.

6. Where do we go from here to protect bodies in disease surveillance?

So far, this study has discussed various harms arising from surveillance practices enabled through data. As analysed in this study, these harms are not limited to control over people's data, but also extend to control over their bodies. At the same time, as introduced earlier, public health experts consider some forms of disease surveillance to be necessary to manage the pandemic. With an embodied understanding, what would such surveillance look like? This section now discusses how we can ensure the protection of people's bodies in disease surveillance. Section 6.1 first fundamentally questions the need for data to be used for large-scale disease surveillance. After establishing that data in itself cannot keep people safe during a pandemic, Section 6.2 next analyses the various forms of resistance that are being observed to oppose the use of data for surveillance. It also examines some structural limitations to such resistance which calls for more thinking around what is needed to bring about structural change. Sections 6.3 and 6.4 respond to this by charting out a way forward that incorporates care and mutual trust in disease surveillance during COVID-19.

6.1 Can data keep people safe during a pandemic?

In July, 15,000 people were caught on CCTV footage and fined by the police for not wearing face masks in the city of Hyderabad (Bansal, 2020). When CCTV cameras spotted individuals without masks, the images of these individuals were broadcast to patrolling police officers who attempted to track down the offender. Madhya Pradesh police have also been using CCTV footage for such surveillance (Fernandes, 2020). Sonavane and Bokil opined that this is not a new experience for some targeted communities. In the city of Khandwa, Madhya Pradesh, even before the pandemic, Bokil had witnessed:

One of the tools that the police had employed to check the slaughter of cattle in a Muslim dominated area was CCTV cameras. They had installed them in that area to keep a watch on whether any cattle is being brought in or taken out... Surveillance through CCTV was just one part of the environment the police had created. They had also punished the people who were involved in these incidents by demolishing their houses. So the police have been involved in every part of their lives. That was underscored by that 'eye' that was there all the time.

They gave an example of the pardhis, a de-notified tribe (DNT), to illustrate this:

Police stations have registers of 'habitual offenders', which is a loosely defined category of people who have a criminal record in their jurisdiction. Before a festival or any election, there will be hoards of people who will be taken to the police station and there will be these elaborate forms that include questions like “what are the acids that you own”, “who were your friends when you were in jail”, “what is the number of your bike”... And there is no legal basis to any of these actions. For the Pardhis, which is a DNT community, surveillance measures will also include... if there is a wedding in the family, they're required to go to the local police station and submit an application along with a copy of the wedding invite and guest list; otherwise the police will end up at the wedding and arrest someone. Things like this are a constant part of their lives.

Scholars have written about the historical basis for the persecution and surveillance of DNTs (Radhakrishna, 2001; D'Souza, 1999). Since colonial rule, Indian police have maintained subjective databases of individuals who need to be surveilled because the police believe that they are likely to commit crimes (Satish, 2011). For such tribes that “have always been subjected to surveillance tactics of different kinds” (as Sonavane and Bokil observe), the 'new normal' of COVID-19 has, in fact, always been the way of life. Some communities have always been surveilled more than others. With data increasingly forming the basis for surveillance, without correcting for these historic cultural biases, some communities will continue to be targeted disproportionately (Internet Governance Forum, 2019). Sonavane and Bokil further opined:

Policing measures are not as much about safety, as they were about keeping an eye on people... to surveil them... A lot of people don't think these are safety measures... Even if it is being sold to them as a measure of safety, I don't think that is something they are going to buy into because they've already been living in this ecosystem where they have been subjected to surveillance of different kinds... Technology may be a new factor, but it's always happened.

This is similarly observed for app-based transport workers which include delivery partners of food delivery companies and drivers of cab service companies. As seen in Section 5, these workers are being mandated to download the Aarogya Setu contact tracing app, which is meant to be a safety measure according to the companies mandating it. Shaik Salauddin, the national General Secretary of the Indian Federation Of App-Based Transport Workers (IFAT), shared:

Delivery boys are risking their lives doing their jobs.... If the company or government has any care for the driver's safety, then why don't you provide gloves and masks to the people? How many drivers did you give N95 masks to? How many drivers did you give protection sheets for the car? Why is there no option to complain for the driver if he is not given these protections? ... The person who has to book an Uber does not have the app.... If I am a driver, and someone gets into my cab, how will the driver know if the person is positive or negative? ... What is this app proving? Nothing. (translated from Hindi)

This indicates that, even if surveillance through technology was meant to be a safety measure, it is not aimed at keeping workers safe, but rather those who avail their services. In the above example, the driver's safety is of lesser concern to the state and industry than the safety of consumers. This highlights a class angle to surveillance. This is also echoed in experiences of ASHA workers who, while doing door-to-door surveillance during COVID-19 through the Ghar Ghar Nigrani app, have not been given adequate safety gear such as PPEs, masks, gloves, and sanitisers to keep themselves safe (Rao & Tewari,

2020). Worse still, they have faced violence from communities while carrying out their data collection tasks (as seen in section 3). Salauddin further added:

If you get an order on Swiggy today as a delivery boy... you can't cancel the order because you will not know the order is from a Red Zone until you reach the area. You will not know at the time the order is placed and accepted. So the app has failed no? ... Does Aarogya Setu tell you to not go ahead in that zone? No. It just intimates you about it no? It can't stop you, no? ... What is the big new thing Aarogya Setu is telling you? Everyone already knows what the Red Zones are. Barricades will be there, it will be there in the news. I don't want that from the app. My expectation from a useful app will be one that stops me from going to the Red Zone area for my safety. Why can't you build that? (translated from Hindi)

This underscores that although data may be helpful in providing insights on safety during a pandemic, as an end in itself, data cannot keep people safe. Mandatory measures such as the downloading of apps for workers are data collection practices more than safety-enhancing practices. Not only does surveillance fail at keeping people safe, it can also lead to violence in some cases.

6.2 Resistance and its limitations

If the use of data for surveillance does not necessarily keep people safe, then it is expected that some degree of resistance to surveillance would be observed during COVID-19. Sandeep Narwani, a lawyer who was asked to download the Aarogya Setu app at a government testing center in Delhi to get a COVID-19 test, said:

I was not sure whether to focus on my health, download the app, and get the test done or to fight back. I came out and called a friend. He said that the test can be done anywhere, don't download it. I went back inside and asked the person why it is mandatory. I told him I am not installing it, and to give me in writing that I need to download it because I am not going to download this app. He was quite startled. I told him, "I am a lawyer myself. And tomorrow I will take you to court about it". Then they said, "no no please come inside". And then they did my test.

These actions that individuals perform in their daily lives often do not get accounted for within existing understandings of resistance which are generally extolled to be organised (Mahanta & Bharadwaj, 2019). This ignores the realities of persons who may employ individual forms of resistance for the attainment of immediate personal gains (Martin, Van Brakel, & Bernhard, 2009). Such negotiations with surveillance by invoking hierarchy through veiled threats offer understandings of individual resistance during COVID-19.

However, there are structural limitations to individual forms of resistance. For example, Heena Ruvaidd is a Kashmiri Muslim living with her sister in a predominantly Hindu locality where "everyone knows who we are because we are two women living alone, single, Muslim, Kashmiri." During the lockdown, an event was announced by the Prime Minister on March 22 for five minutes worth of applause for healthcare professionals. Ruvaidd shared:ed:

We opened our balcony and curtains so that we also gave the impression that we are part of it, we didn't want to look like we were boycotting it.... I was peeling onions and I continued to do that so that if anyone sees why we are not participating, I have an

excuse that I'm peeling onions... My friends, whoever is Hindu... said that we boycotted this event... This defiance and transgression, these are prerogatives of the majority, of the dominant social class and we just can't afford to do that.

Narwani is privileged along the axes of gender and religion, which made resistance a possibility for him. However, Ruvaid and her sister occupy more stigmatised religious identities, and are therefore disprivileged in ways that have come to take prominence during the pandemic (as discussed in section 2). Their marginalised contexts make it not only difficult to resist oppressive systems, but also coerce them to comply with surveillance on an individual level.

Organised forms of resistance may be able to overcome some of the risks of individual resistance to an extent. The Indian Federation Of App-Based Transport Workers (IFAT) have opposed the mandatory download of the Aarogya Setu app for workers in companies such as Uber, Zomato, and Swiggy (Indian Federation of App Based Transport Workers, 2020). Section 3 also mentioned an organised protest by the All India ASHA Worker and Facilitators Union in Punjab against the mandatory usage of the Ghar Ghar Nigrani app. One of the demands made by domestic workers' unions in Karnataka for RWAs has been to limit the data collected from domestic workers and to ensure the protection of collected data (Menon, 2020). Reversing the surveillant gaze, the Sarva Shramik Sanghatana, which has a membership of 19,000 domestic workers in Mumbai, has demanded that if domestic workers need to produce COVID-19-negative certificates to resume work, then so should their employers within the residential societies (Ganapatye & Rao, 2020). The Migrant Workers Solidarity Network has documented migrant workers' resistance across India during the COVID-19 lockdown in an interactive map which spans over 150 protests involving over 100,000 migrant workers ("Migrant Workers Solidarity Network", n.d.). All of these are powerful subversions of the dominant narrative of marginalised communities being dependents seeking the help of the state. They reaffirm the status of marginalised communities as rightful citizens and political subjects capable of challenging their oppressive conditions (Menon, 2020).

Organised resistance also faces some social limitations. Accessibility of data is one such limiting factor. India ranks third in terms of the number of digital signatures received for top COVID-19-related online petitions (Mishra, 2020). Raina Roy, Director of Samabhabona and a trans woman, observed, "Nowadays protests are not happening... Some online protests are happening, but except few privileged people, there is no protest happening... That is not possible for all Indians, for the trans community, it is actually not applicable." This highlights that without access to Internet-enabled devices, it is difficult to resist when many forms of organised resistance have moved online due to COVID-19 mobility restrictions.

Through the reproduction of power relations, surveillance becomes structural and a matter of social justice, not just personal privacy (Lyon, 2003). This means that effective responses to surveillance would also need to be structural. Organised resistance may be one such response. However, as data surveillance becomes increasingly ubiquitous, enacted through multiple agents in tandem (Haggerty & Ericson, 2000), resistance will require newer strategies. This may be due to at least two possible asymmetry problems arising from the use of data for surveilling bodies. First, data exacerbates power asymmetries because individuals have little control over how their bodies are monitored and controlled by those in power. Second, data exacerbates knowledge asymmetries as individuals rarely have enough information about how they are being monitored and by whom. These two asymmetries can make resistance much harder, since we cannot meaningfully resist something that we do not fully understand, know about and are not in a position to influence (Galič, Timan, & Koops 2017). With the use of data for surveillance, there is also reduced space available for negotiations with the categories that we are slotted into, which was more easily available in earlier forms of social control (Norris, 2005). Especially during

the COVID-19 crisis, practices of surveillance have, in many cases, been supposedly designed to serve useful purposes such as safety. It becomes harder to resist practices that are packaged as benevolent schemes.

6.3 Role of care

Menaka Rao, an independent healthcare journalist, said:

For the prevention and control of any disease, some form of surveillance is required. Older ways of doing surveillance manually are probably better than using technology. If the patient starts feeling threatened or stigmatised, then they will not reveal their symptoms. It has to be done with a lot of care.

Offering the example of the TB DOTS (Direct Observed Therapy) programme ("The five elements of DOTS", n.d.), Akhila Vasan and Vijaya Kumar mentioned: "The DOTS Program requires that a patient go to the local anganwadi [rural child care centre], or the ASHA worker will come to their house and give medicine, and that person has to consume the medicine in the presence of either the ASHA worker or the anganwadi worker." This monitoring is a form of manual surveillance, carried out through the healthcare system by trained healthcare workers, ensuring that people's needs are understood and cared for. Similarly, Rao highlighted care protocols that were laid down for HIV/AIDS such as not revealing the names of patients and providing them with counselling. In contrast, as this study has examined, during COVID-19, personal data of people suspected to have COVID-19 has been released publicly by the state on government lists and apps, and people have been criminalised for violations of state orders. Nikita Sonavane and Ameya Bokil shared:

We don't think that [care is] something that can happen through the policing system at all because...policing implies that there is a certain amount of violence that is ingrained in that function... the way that policing in India is structured [is] a system that is systematically used to target marginalised communities... I don't know in which form it would look like something that could imbibe the virtue of care.... I think it's a problem of not penalising people.... not showing them the threat of criminal law when it comes to dealing with problems.

The framework of data as a resource for human use or exploitation plays an important role in turning the management of the pandemic into management of datafied bodies. This framework also creates an over-reliance on technological tools and the data from these tools for managing the health pandemic. In order to begin laying down care practices for surveillance, we must therefore first center bodies in our understanding of surveillance.

According to feminist care ethics, surveillance can imbibe care. While themes of 'surveillance as control' have dominated the field of surveillance studies, leading to the default assumption that surveillance is negative, an emphasis on 'surveillance as care' may open up new possibilities (Abu-Laban, 2015). For marginalised communities, surveillance can play an important role in care since awareness about being paid attention to can have positive and affirming impacts (McIntosh, Punch, Dorrer & Emond, 2010). However, with the use of data in a manner that is opaque or invisible to the surveilled and carried out in disempowering ways, this potential for care is entirely missed out. When Heena Ruvaid and her sister, both Kashmiri Muslims, were being targeted in their predominantly Hindu locality through a rumour, Ruvaid approached the Joint Secretary of their residential society. She said:

I told him [joint secretary]... 'we are two girls staying here alone, and you guys are office bearers... we here actually fear that we may be lynched... and you are responsible for this so tell me what are you going to do about this?' He said, 'no no, don't worry'.... So [name redacted] gave me his number and said, 'if there is ever any problem you just give me a call and I will be there'. ... Once he gave me his number, I felt much more confident and reassured.

Care and control should not however be seen as contradictory approaches to surveillance. By attending to power hierarchies and vulnerabilities (which have been pointed out throughout this study) within feminist ethics of care, scholars acknowledge that care can sometimes be oppressive and create dependence, thus blurring into forms of control (Abu-Laban, 2015). Surveillance can therefore be understood as a dynamic process that involves both the logic of care and the logic of control (Lyon in Walsh 2010; Mol, 2008). Various ethnographic studies have also pointed to control and care overlapping in practices of surveillance, making them difficult to distinguish these categories in practice, thus showing that all care involves surveillance on some level (Essén, 2008; Gad & Lauritsen, 2009; Milligan et al., 2010). What would this look like in practice for COVID-19 surveillance? Sonavane and Bokil said:

If we were to... incentivise people coming forward [to report symptoms], that would help. That would allow people to consent to some kind of system that tracks people's movements. For example, if you know somebody who has COVID-19 and has travelled to a bunch of places in the time that it wasn't tested, the state could ask you to come forward, assure you that there will be no criminal prosecutions, ask you that, "these are the places that this person was at that point, if you were there, there's a likelihood that you might have also been infected", and to come forward. I think that kind of system would work better than a system where there is the threat of you having criminal charges filed against you if you were to come forward.

6.4 Role of mutual trust

"The only means to fight the plague is honesty."

- Albert Camus, *The Plague* (1947)

"We don't trust that the government is honest. We cannot entrust the government to do anything in our best interests. Finally, it comes down to that."

- Akhila Vasan, Karnataka Janarogya Chaluvali

Mutual trust is an essential prerequisite for state surveillance to be effective in controlling the spread of the pandemic without harms to people being surveilled. The state must trust individuals to share information with its functionaries, and individuals must in turn be able to trust the state with that information. First, what does the rise of data-based surveillance say about the state's trust in individuals and communities? Swarna Rajagopalan, Founder and Managing Trustee of the Prajnya Trust, opined:

Surveillance is predicated on the absence of trust, isn't it? If... tomorrow, heaven forbid, I develop COVID-19 symptoms, you trust that I will show up and tell you that, look, these are all the people I have been in contact with. Then you won't need to find out where I am. The contact tracing might only be [useful] if I don't know where the delivery boy has been. You might still need to do some of it [contact tracing], but it might need to be less. The point of departure for any kind of surveillance is the absence of trust... There is something wrong with a democracy when the government doesn't trust you but you must trust the government.

Second, are individuals and communities in a position to trust the state? Heena Ruvaid, a Kashmiri Muslim, said:

The virus does not discriminate, but the government discriminates. You feel betrayed... What if the authorities... put me in a quarantine facility? It did come to my mind whether I would come back intact or not. How do I know they won't inject me with soap poison or they wouldn't bug me? ... How do I know that I won't be in fact killed in the quarantine facility? Because the government can easily say that she died of COVID-19... It is all very scary. I don't know how someone from a majority community will feel about it but as someone from a minority community... I would rather die in my room than in a quarantine facility... I don't trust my government.

Ruvaid describes her distrust of the state as someone who is facing state surveillance. On the other hand, consider ASHA workers who carry out state surveillance due to which they have been facing violence from their communities, as section 3 analysed. In this context, Menaka Rao, an independent health journalist, expressed: "There is a lack of trust in the government and the public system that is prominently being expressed, and ASHAs have to face the brunt of distrust of the system at the village level". This further highlights that, when trust in institutions is eroded, the space of institutional authority gets readily filled by fear and xenophobia (Andrejevic, 2013).

Regarding Aarogya Setu, Shaik Salauddin, the national General Secretary of the Indian Federation Of App-Based Transport Workers (IFAT), said that "we don't trust the app" (translated from Hindi). When the state considers individuals to be mere data points to be managed as resources, people find it difficult to trust the state to make decisions in their best interest. However, even if people lose faith in the state, it does not protect them from state violence if the state believes that they have contributed to the spread of COVID-19 (French & Monahan, 2020), as this study has examined in section 3.

Under such circumstances, how can trust be built? Sonavane and Bokil opined:

It's easier to build that relationship of trust with the state... [when it] is rooted in the ethos of social welfare... And that is something that Kerala has done and I think for the rest of us, we are trying to build these mechanisms while responding to a crisis... I think any sort of setup where they have been able to respond to this effectively is because a significant amount of investment has been made into these structures outside of responding to situations.

In the early days of the pandemic, the Indian state of Kerala was relatively more successful in India in combating the COVID-19 pandemic through what has now come to be known as the 'Kerala model', which has received praise from international bodies ("Responding to COVID-19", 2020). Underlying many of the strategies for Kerala's success is mutual trust. The Kerala government's response during the pandemic built public trust because of which people were more willing to observe home quarantine during the lockdown (Faleiro, 2020). One of the ways this was achieved was through community engagement. For example, with the help of members of the self-help group, 'Kudumbashree,' community kitchens were set up to provide cooked meals to the poor with support from local government bodies (National Disaster Management Authority & Coalition for Disaster Resilient Infrastructure, 2020). For other parts of the country to observe similar outcomes, there needs to be a long-term investment in building trust in public health and state institutions, which cannot be replaced by the use of data.

Conclusion

This study has presented grassroots perspectives of control through data-enabled surveillance during COVID-19, and analysed that this is experienced as control over bodies by marginalised communities. In this context, the study has also recommended ways forward.

The first harm of surveillance this study illustrated is the reproduction and legitimisation of inequalities within homes, communities, and the state-citizen relationship. Within the home, the bodies of vulnerable family members (such as women) are controlled by more powerful members by restricting their access to mobile phones and the Internet through surveillance. This impacts their ability to report domestic violence or earn livelihoods, legitimising their subjugated position within the home. At the level of communities, the stigma of COVID-19 has been associated with marginalised communities and has promoted the surveillance of their bodies through data. This happens through information collected by apps about stigmatised communities (such as domestic workers) or through digital disinformation about stigmatised communities (such as Muslims). In each case, surveillance reproduces prejudices about these communities, and its harms are material and embodied, such as the inability to access gated communities and receive wages or fatal physical violence. The state also plays a role in exacerbating inequalities within homes and communities. Home quarantine and geofencing apps extend the state's surveillant gaze into the intimate space of the home, brokering new non-negotiable power relationships between the state and citizens through their data. Many state apps also encourage communities to report on each other for violating state orders, turning them into socially legitimate spies of the state.

Second, physical restrictions on mobility in public spaces are enforced through surveillance using data and carried out through criminalisation by the state. The physical bodies of people are disciplined to stay at home through the threat of drones capturing images of lockdown violators without the need for an official to be physically present. Moreover, when the mobile locations of people are tracked by the state in an effort to track the spread of the virus, people feel the need to physically sever the connection with their phones so as to not have their bodies and movements controlled by the state.

Third, various measures for facilitating access to essential services and rights that may not be intended as surveillance have the effect of surveillance by imposing some degree of social control through data. Mandatory digital requirements and identity proofs such as Aadhaar and Aarogya Setu collect data about individuals and profile them into categories that often don't reflect their physical reality. But their digital identities are given precedence over their corporeal identities, furthering their exclusion from state services and rights such as healthcare, employment, and travel. Further, while financial information about their own lives can potentially empower people, the structural constraints introduced by technology-mediated social protection schemes cause this information to be inaccessible to them while remaining accessible only to the state and financial institutions that collect this data. This could lead to people not receiving their welfare money or making ill-informed budgeting strategies, pushing people into poverty during a health crisis.

In dominant discourse, such harms of surveillance are understood in a restricted way as data protection or privacy harms. This flows from constructions of data as a resource that is independent from our bodies, and available for exploitation by humans, erasing the connections between data and bodies. Feminist scholarship has pointed out that through this erasure, contexts and power relations that surveillance occurs within are invisibilised, making surveillance seem innocuous and harder to challenge. Placing this study within that framework by viewing data as embodied, this study has highlighted the specific harms of surveillance during COVID-19 within homes, communities, and by the

state. The embodied understanding of these harms is different in each case, but what remains common is that putting bodies back into the picture makes the harms visible. In all of the cases studied here, surveillance undermines not just data privacy, but the bodily integrity, autonomy, and dignity of individuals. By disregarding this embodiment, we would not be doing justice to the experiences of marginalised communities.

Public health experts say that some form of disease surveillance may be required to control the pandemic. What would such a form of surveillance look like, and how can it be carried out while ensuring that the bodies of people are protected? This study establishes that while data can provide insights on safety during a pandemic, it cannot itself keep people safe. In light of this, various forms of individual as well as organised resistance have been carried out during COVID-19. However, there are structural limitations to resistance when surveillance takes unprecedented digitally mediated forms that were not possible before. It is necessary, on a structural level, to incorporate feminist ethics of care and build mutual trust between the state and communities so that the harms of these newer forms of surveillance are mitigated. For this to happen, surveillance of the disease should not be conflated with surveillance of bodies, and the management of the pandemic should not be reduced to management of disembodied data. Policies responding to COVID-19 that aim to protect personal data and data privacy must be broadened to respond to the embodied harms pointed out in this study to ensure that individuals retain control over not just their data, but also their datafied bodies.

Reference

133,730 FIRs registered, 27,446 arrested for violating Covid-19 lockdown in Maharashtra. (2020, June 22). Hindustan Times. <https://www.hindustantimes.com/india-news/133-730-firs-registered-27-446-arrested-for-violating-covid-19-lockdown-in-maharashtra/story-a1ZsdBTH5wIHGZdbo7sNLK.html>.

Aadhaar-ration card link till September 15 in Odisha. (2019, September 1). The New Indian Express. <http://www.newindianexpress.com/states/odisha/2019/sep/01/aadhaar-ration-card-link-till-september-15-in-odisha-2027393.html>

Aarogya Setu app compulsory for air, train travel and more: Full list. (2020, May 18). *Indian Express*. <https://indianexpress.com/article/technology/tech-news-technology/aarogya-setu-app-mandatory-air-train-travel-more-list-6413841/>

Aas, Katja Franko. (2006). 'The body does not lie': Identity, risk and trust in technoculture. *Crime Media Culture*, 2(2). <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1006.5965&rep=rep1&type=pdf>

Abu-Laban, Yasmeen (2015). Gendering surveillance studies: The empirical and normative promise of feminist methodology. *Surveillance & Society*, 13(1), 44-56.

Agamben, Giorgio. (2020, February 26). *The Invention of an Epidemic*. Quodlibet. <https://www.quodlibet.it/giorgio-agamben-l-invenzione-di-un-epidemia>

Agarwal, Aditi. (2020, May 27). Who made Aarogya Setu? A list. *Medianama*. <https://www.medianama.com/2020/05/223-aarogya-setu-contributors/>.

Almost every fifth Jan Dhan account 'inoperative'. (2020, February 6). *Business Line*.
<https://www.thehindubusinessline.com/money-and-banking/almost-every-fifth-jan-dhan-account-inoperative/article30754738.ece>.

Ambedkar, Bhimrao Ramji. (2014). *Annihilation of caste: The annotated critical edition*. Verso Books.

Amoore, Louise, & Hall, Alexandra. (2009). Taking people apart: Digitised dissection and the body at the border. *Environment and Planning D: Society and Space*, 27(3), 444-464.

Andrejevic, Mark. (2004). The work of watching one another: Lateral surveillance, risk, and governance. *Surveillance & Society*, 2(4).

Andrejevic, Mark. (2013). *Infoglut: How Too Much Information is Changing the Way We Think and Know*. New York: Routledge.

ANI [@ANI]. (2020, July 1). *Haryana: Municipal Corporation of Gurugram issues guidelines for resident welfare associations, to be followed till 31st July during #Unlock2*[Tweet]. Twitter.
<https://twitter.com/ANI/status/1278132058922106880>.

Arnold, David. (1986). *Police power and colonial rule, Madras, 1859-1947*. Oxford University Press, USA.

Arora, Payal, & Scheiber, Laura. (2017). Slumdog romance: Facebook love and digital privacy at the margins. *Media, Culture & Society* 39:408-422.

Asked to get smartphones for survey, ASHA workers in Ludhiana stage protest. (2020, June 15). *The Hindustan Times*. <https://www.hindustantimes.com/cities/asked-to-get-smartphones-for-survey-asha-workers-in-ludhiana-stage-protest/story-9g42Kmu9NavEPK9zbzdA7L.html>

Ayyub, Rana. (2019, October 23). India's crackdown in Kashmir has paralyzed and silenced entire communities. *Washington Post*. <https://www.washingtonpost.com/opinions/2019/10/23/indias-crackdown-kashmir-has-paralyzed-silenced-entire-communities/>.

Ball, K., Di Domenico, M., & Nunan, D. (2016). Big data surveillance and the body-subject. *Body & Society*, 22(2), 58-81.

Banerjee, Dwaipayan (2020, June 30). Use of laws such as the Epidemic Diseases Act allows the Modi government to extend its authoritarian powers. <https://caravanmagazine.in/perspectives/colonial-character-of-the-modi-governments-actions-during-the-pandemic>

Bansal, Varsha. (2020, August 21). *Life in India's digital dystopia*. Coda.
<https://www.codastory.com/authoritarian-tech/indias-most-surveilled-city/>

Barik, Soumyarendra. (2020a, July 25). A complete guide to drones in India. *Medianama*.
<https://www.medianama.com/2020/07/223-drone-guide-india/>.

Barik, Soumyarendra. (2020b, April 10). In Kerala and Telangana, police turn to drones to enforce COVID 19 lockdown. *Medianama*. <https://www.medianama.com/2020/04/223-kerala-telangana-drones-coronavirus/>

Bengaluru hospitals demand Aadhaar details, patient dies. (2020, August 18). *The New Indian Express*.
<https://www.newindianexpress.com/cities/bengaluru/2020/aug/18/bengaluru-hospitals-demand-aadhaar-details-patient-dies-2184858.html>.

Bhardwaj, Amit. (2020, April 8). How fake news, rumours are driving call for ban on Muslim vendors in NW Delhi. *Asiaville News*. <https://www.asiavillenews.com/article/how-fake-news-rumours-are-driving-call-for-ban-on-muslim-vendors-in-nw-delhi-shastri-nagar-38855>

Bhardwaj, Kritika. (2020, June 5). *Digital Surveillance Systems to Combat COVID-19 May Do More Harm Than Good*. EPW Engage. <https://www.epw.in/engage/article/digital-surveillance-systems-combat-covid-9-harm>

Bhatia, Gautam. (2019). *The transformative constitution: A radical biography in nine acts*. Harper Collins.

Bihar Government. (n.d.). *Bihar Migrant Labor Exit Assistance*. [http://aapda.bih.nic.in/\(S\(afdwpspo1peohjgrfe435btd\)\)/Default.aspx](http://aapda.bih.nic.in/(S(afdwpspo1peohjgrfe435btd))/Default.aspx).

Bokil, Ameya, & Sonavane, Nikita. (2020, April 11). Why Relying on Criminal Law Should Not Be the Answer to a Pandemic. *The Wire*. <https://thewire.in/law/criminal-law-coronavirus-pandemic>.

Bose, Adrija. (2020, April 6). India's Domestic Abuse Survivors are in Lockdown with their Monsters, But Helplines Are Not Ringing. *New18*. <https://www.news18.com/news/buzz/indias-domestic-abuse-survivors-are-in-lockdown-with-their-monsters-but-the-helplines-are-not-ringing-2563955.html>.

Btithij, Ajana (2013). *Governing through Biometrics: The Biopolitics of Identity*. *Palgrave Macmillan*.

Building Atmanirbhar Bharat and Overcoming COVID-19. (n.d.). <https://www.india.gov.in/spotlight/building-atmanirbhar-bharat-overcoming-covid-19>.

Capt launches 'Ghar Ghar Nigrani' app for Covid surveillance (2020, June 13). *The Hindustan Times*. <https://www.hindustantimes.com/chandigarh/capt-launches-ghar-ghar-nigrani-app-for-covid-surveillance/story-Z2iID0go6AmMTOO1Q175HJ.html>

CDC new Covid guidelines: Was lockdown necessary or did epidemiologists get it wrong? (2020, May 22). *The Print*. <https://theprint.in/talk-point/cdc-new-covid-guidelines-was-lockdown-necessary-or-did-epidemiologists-get-it-wrong/427317/>

Chakravarti, Ankita. (2020, April 23). Zomato, Urban Company make Aarogya Setu app mandatory for staff, delivery-partners. *India Today*. <https://www.indiatoday.in/technology/news/story/zomato-urban-company-make-aarogya-setu-app-mandatory-for-staff-delivery-partners-1670032-2020-04-23>.

Christopher, Nilesh. (2020, February 18). We've Just Seen the First Use of Deepfakes in an Indian Election Campaign. *Vice*. https://www.vice.com/en_in/article/jgedjb/the-first-use-of-deepfakes-in-indian-election-by-bjp.

Clarance, Andrew. (2020, May 14). Aarogya Setu: Why India's Covid-19 contact tracing app is controversial. *BBC News*. <https://www.bbc.com/news/world-asia-india-52659520>.

Coronavirus: ASHA workers endure abuse and assault on field. (2020, April 22). *Deccan Herald*. <https://www.deccanherald.com/national/west/coronavirus-asha-workers-endure-abuse-and-assault-on-field-828525.html>

Corrêa, Sonia. (2020). *Biopolitics & The COVID-19 Pandemic: Feminist Perspectives*. *DAWN Talks on COVID-19*. https://dawnnet.org/wp-content/uploads/2020/06/DAWNTalksOnCOVID_19_SoniaCorrea.pdf

Couldry, Nick, & Mejias, Ulises A. (2019). Data colonialism: Rethinking big data's relation to the contemporary subject. *Television & New Media*, 20(4), 336-349.

COVID-19, Domestic Abuse and Violence: Where Do Indian Women Stand? (2020, April 17). *EPW Engage*. <https://www.epw.in/engage/article/covid-19-domestic-abuse-and-violence-where-do>.

Covid-19: Dalit family in Haryana attacked for allegedly not following PM's call to turn off lights. (2020, April 9). *Scroll*. [_https://scroll.in/latest/958665/covid-19-dalit-family-in-haryana-allegedly-attacked-for-not-following-pms-call-to-turn-off-lights](https://scroll.in/latest/958665/covid-19-dalit-family-in-haryana-allegedly-attacked-for-not-following-pms-call-to-turn-off-lights)

Das, Gaurav. (2020, March 31). As Assam Gets First COVID-19 Patient, 'Nizamuddin List' Violates Privacy of Many. *The Wire*. <https://thewire.in/rights/assam-coronavirus-nizamuddin-list>.

Dash, Sweta. (2020, August 29). Aadhaar-induced exclusion from the PDS is making poor go hungry in Odisha; universalise PDS, demand activists. *Gaon Connection*. <https://en.gaonconnection.com/aadhaar-induced-exclusion-from-the-pds-is-making-poor-go-hungry-in-odisha-universalise-pds-demand-activists/>

Data Dashboard. (n.d.). Impacts of COVID-19. <https://impactsocovid.in/data-dashboard>.

Datta, Ayona. (2020). Self (ie)-governance: Technologies of intimate surveillance in India under COVID19. *Dialogues in Human Geography*, 2043820620929797.

Davis, Angela Y. (2011). *Are prisons obsolete?*. Seven Stories Press.

Deshmane, Akshay. (2017, April 28). The Dalit identity dilemma. *Frontline*. <https://frontline.thehindu.com/cover-story/the-dalit-identity-dilemma/article9629313.ece>.

Dhara, Tushar. (2020, August 21). Cancelled ration cards deprived Telangana's poor of food rations amid lockdown. *Caravan*. <https://caravanmagazine.in/government/cancelled-ration-cards-deprived-telanganas-poor-of-food-rations-amid-lockdown>

Dhorajiwala, Sakina, & Wagner, Niklas. (2019, August 23). *Consent to nothing: Aadhaar-based payment systems in welfare*. Ideas for India. <https://www.ideasforindia.in/topics/governance/consent-to-nothing-aadhaar-based-payment-systems-in-welfare.html>.

Dhorajiwala, Sakina, Dreze, Jean, & Wagner, Niklas. (2019, March 27). A bridge to nowhere. *The Hindu*. <https://www.thehindu.com/opinion/lead/a-bridge-to-nowhere/article26646131.ece>.
Digital India. (n.d.). <https://digitalindia.gov.in/ebook/dot/page6.php>

Direct Benefit Transfer. (n.d.) <https://dbtbharat.gov.in/>

Diwaker, Ravi Kumar. (2020, March 25). COVID-19 impact: Apartment owners ban outsiders' entry. *Economic Times*. <https://realty.economictimes.indiatimes.com/news/residential/covid-19-impact-apartment-owners-ban-outsiders-entry/74806069>.

Dreze, Jean. (2020, April 21). Cash to the poor is good – but will they be able to access it safely from banks? *Scroll.in*. <https://scroll.in/article/959730/cash-to-the-poor-is-good-but-will-they-be-able-to-access-it-safely-from-banks>

Dube, Siddharth. (2019). *An Indefinite Sentence: A Personal History of Outlawed Love and Sex*. Atria Books.

During lockdown, rural India faced insurmountable sufferings; 74% satisfied with government. (2020, August 14). Gaon Connection. <https://en.gaonconnection.com/gaon-connection-survey-rural-india-faced-insurmountable-sufferings-during-covid-19-lockdown-74-of-respondents-satisfied-with-modi-government/>.

D' Souza, Dilip. (1999, December). De-Notified Tribes: Still 'Criminal?' Economic and Political Weekly, (34)51, 3576-78.

Ellis-Petersen, Hannah, & Rahman, Shaikh Azizur. (2020). Coronavirus conspiracy theories targeting Muslims spread in India. The Guardian. <https://www.theguardian.com/world/2020/apr/13/coronavirus-conspiracy-theories-targeting-muslims-spread-in-india>

Essén, Anna (2008) The Two Facets of Electronic Care Surveillance: An Exploration of the Views of Older People Who Live with Monitoring Devices. *Social Science & Medicine* 67 (1): 128–36.

Eubanks, Virginia. (2012). *Digital Dead End: Fighting for Social Justice in the Information Age*. Cambridge, MA and London: MIT Press.

Faleiro, Sonia (2020). What the world can learn from Kerala about how to fight covid-19. MIT Technology Review. <https://www.technologyreview.com/2020/04/13/999313/kerala-fight-covid-19-india-coronavirus/>

Fernandes, Brigitte. (2020, June 22). Indore's Khajrana Police Station All Set To Combat COVID-19 With Latest Equipment, Republic World. <https://www.republicworld.com/india-news/general-news/indores-khajrana-police-station-all-set-to-combat-covid-19.html>

FIR against 100 Asha workers for Jantar Mantar protest. (2020, August 11). Hindustan Times. <https://www.hindustantimes.com/cities/fir-against-100-asha-workers-for-jantar-mantar-protest/story-q2obOCJAwddgNEt0QeM7LL.html>

Fisher, Jill A. (2006). Indoor positioning and digital management: Emerging surveillance regimes in hospitals. *Surveillance and Security* (pp. 89-100). Routledge.

Foucault, Michel. (1991). *Discipline and punish: the birth of the prison*. Penguin.

French, Martin, & Monahan, Torin. (2020). Dis-ease Surveillance: How Might Surveillance Studies Address COVID-19?. *Surveillance & Society*, 18(1), 1-11.

G.P., Parijatha. (2020, April 8). Domestic Work In The Platform Economy: Reflections On Awareness Of Worker's Rights. GenderIT.org. <https://www.genderit.org/articles/domestic-work-platform-economy-reflections-awareness-workers-rights>

Gad, Christopher, and Peter Lauritsen (2009). Situated Surveillance: An Ethnographic Study of Fisheries Inspection in Denmark. *Surveillance & Society* 7(1): 49.

Galič, Maša, Timan, Tjerk, & Koops, Bert-Jaap. (2017). Bentham, Deleuze and beyond: An overview of surveillance theories from the panopticon to participation. *Philosophy & Technology*, 30(1), 9-37.

Ganapatye, Shruti, & Rao, Shashank (2020, June 13). Want your maid back? Give proof you're Covid-free. <https://mumbaimirror.indiatimes.com/mumbai/cover-story/want-your-maid-back-give-proof-youre-covid-free/articleshow/76349894.cms>

Ghebreyesus, Tedros Adhanom. (2020, February 15). *Munich Security Conference*. World Health Organization. <https://www.who.int/dg/speeches/detail/munich-security-conference>.

Ghosal, Aniruddha, Saaliq, Sheikh &, Schmall, Emily. (2020, April 25). Indian Muslims face stigma, blame for surge in infections. *AP News*. <https://apnews.com/article/ad2e96f4caa55b817c3d8656bdb2fcbd>.

Government of Jharkhand. (n.d.). *COVID-19 Help*. <http://covid19help.jharkhand.gov.in/>.

Government of Punjab [@PunjabGovtIndia]. (2020, May 30). *Is there a mass gathering nearby you? Now you can report it through #CovaApp*[Tweet]. Twitter. <https://twitter.com/PunjabGovtIndia/status/1266651829422583816>.

Government of Rajasthan. (2020). *RajCovidInfo Mobile App* [PDF] (p. 9). https://jhunjhunu.rajasthan.gov.in/content/dam/doitassets/Jhunjhunu/Corona/RajCovaInfo%20Mobile%20App_10Apr20.pdf.

GSMA. (2019) The mobile gender gap report. *GSMA*. <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/GSMA-The-Mobile-Gender-Gap-Report-2019.pdf>

Guariglia, Matthew & Quintin, Cooper. (2020, April 7). Thermal Imaging Cameras are Still Dangerous Dagnet Surveillance Cameras. *Electronic Frontier Foundation*. <https://www.eff.org/deeplinks/2020/04/thermal-imaging-cameras-are-still-dangerous-dagnet-surveillance-cameras>.

Gupta, Apar. (2020, March 30). *Quarantine lists breach individual privacy! Social solidarity in times of Covid-19 #SaveOurPrivacy*. Internet Freedom Foundation. <https://internetfreedom.in/quarantine-list/>.

Haggerty, Kevin D., & Ericson, Richard V. (2000). The surveillant assemblage. *The British journal of sociology*, 51(4), 605-622.

Harding, Sandra. (1992). Rethinking standpoint epistemology: What is "strong objectivity?". *The Centennial Review*, 36(3), 437-470.

Harikrishnan. (2020, March 30). Coronavirus, social distancing, and the return of caste apologists. *News Laundry*. <https://www.newslaundry.com/2020/03/30/coronavirus-social-distancing-and-the-return-of-caste-apologists>

Hayles, Katherine N. (1999). *How We Became Posthuman: Virtual Bodies in Cybernetics, Literature, and Informatics*. Chicago: University of Chicago Press.

Hoppe, Trevor. (2018). *Punishing Disease: HIV and the Criminalization of Sickness*. Oakland: University of California Press.

Indian Council of Medical Research. (2020, March 17). *Strategy of COVID19 testing in India*. <https://www.mohfw.gov.in/pdf/LabTestingAdvisory.pdf>

Indian Federation of App Based Transport Workers [@Connect_IFAT] (2020, June 4). *A press note of Indian Federation of App-based Transport workers about @SetuAarogya App and Gig workers*. [Tweet]. Twitter. https://twitter.com/Connect_IFAT/status/1268257861844430848

Internet Freedom Foundation. (n.d.) *Multi-domain orgs and individuals raise concerns about Aarogya Setu #SaveOurPrivacy*. <https://internetfreedom.in/aarogya-setu-multi-domain-joint-statement/>

Internet Governance Forum, United Nations-DESA. (2016). *Overcoming Barriers to Enable Women's Meaningful Internet Access*. https://www.intgovforum.org/multilingual/filedepot_download/5004/1318

Internet Governance Forum. (2019, November 28). *IGF 2019 Day 3 - Estrel Saal B - Dynamic Coalition on Gender and Internet Governance* [Video]. Youtube. <https://www.youtube.com/watch?v=DdBuWy4WtvE>

Jain, Tripti, & Ranjit, Tanisha. (2020, May 6). An Exclusion Tale: Aarogya Setu's March From Optional to Mandatory. *The Quint*. <https://www.thequint.com/voices/opinion/aarogya-setu-app-from-voluntary-to-mandatory-and-mass-exclusion>

Jain, Tripti, & Ranjit, Tanisha. (2020, May 6). An Exclusion Tale: Aarogya Setu's March From Optional to Mandatory. *The Quint*. <https://www.thequint.com/voices/opinion/aarogya-setu-app-from-voluntary-to-mandatory-and-mass-exclusion>.

Jan Sarokar/People's Agenda '19. (2020, August 18). *Janta Parliament: Session on Technology and Surveillance* [Video]. Youtube. <https://www.youtube.com/watch?v=1bszYmUyY0M>

Javed, Zeeshan. (2020, April 27). Kolkata: Terrace gatherings in busy localities on cop radar. *Times of India*. <https://timesofindia.indiatimes.com/city/kolkata/terrace-gatherings-in-busy-localities-on-cop-radar/articleshow/75396498.cms>.

Jha, Bagish. (2020). Not enough boots on ground, police to 'geofence' home isolation patients. *Times of India*. <https://timesofindia.indiatimes.com/city/gurgaon/not-enough-boots-on-ground-police-to-geofence-home-isolation-patients/articleshow/76434707.cms>

Jha, Nishita. (2013, November 6). Someone's Watching You, But Who? *Tehelka*. <http://old.tehelka.com/someones-watching-you-but-who/>.

Joshi, Divij, & Kak, Amba. (2020, April 19). India's digital response to COVID-19 risks inefficacy, exclusion and discrimination. *Caravan*. <https://caravanmagazine.in/health/india-digital-response-covid-19-risks-inefficacy-exclusion-discrimination>

Kakodkar, Priyanka. (2020, March 20). Covid-19 in Mumbai: Maids under scanner, but high-flying employers may pose a bigger risk. *Times of India*. <https://timesofindia.indiatimes.com/city/mumbai/covid-19-in-mumbai-maids-under-scanner-but-high-flying-employers-may-pose-a-bigger-risk/articleshow/74725500.cms>

Kalra, Siddhant. (2020, June 19). Banning domestic workers, forcing quarantine: Can your apartment RWA make these 'special' COVID rules? *Citizen Matters*. <https://bengaluru.citizenmatters.in/bengaluru-apartment-association-rwa-covid-rules-legality-ward-committees-urban-governance-46442>

Kappan, Rasheed. (2020, April 11). New app scans countless pics, alerts of quarantine violations. *Deccan Herald*. <https://www.deccanherald.com/state/top-karnataka-stories/new-app-scans-countless-pics-alerts-of-quarantine-violations-824253.html>

Karpagam, Sylvia. (2020, April 11). A Lockdown Is a Solution. In India, a Lockdown Is Also Its Own Crisis. *The Wire*. <https://thewire.in/rights/coronavirus-lockdown-authoritarianism-physical-distancing-rights-elite>

Kaushik, Himanshu. (2020, August 19). Ahmedabad civic body makes Aadhaar, OTP mandatory for Covid 19 testing. *Times of India*. <https://timesofindia.indiatimes.com/city/ahmedabad/ahmedabad-civic-body-makes-aadhaar-otp-mandatory-for-covid-19-testing/articleshow/77624956.cms#>

Kerala police uses drones for surveillance, visuals become viral. (2020, April 12). *On Manorama*. <https://www.onmanorama.com/lifestyle/news/2020/04/12/kerala-police-drones-surveillance-visuals-viral.html>

Kerjiwal, Arvind [@ArvindKerjiwal]. (2020, April 1). *Police will track the phones of those who were directed home quarantine to see if they complied or not. Action will be taken against those who violated.*[Tweet]. Twitter.

Khan, Sobia. (2020, August 12). NoBrokerHood enhances security features to help residents fight Covid 19. *Economic Times*. <https://economictimes.indiatimes.com/small-biz/startups/newsbuzz/nobrokerhood-enhances-security-features-to-help-residents-fight-covid-19/articleshow/77504258.cms>

Khera, Reetika. (2017). Impact of Aadhaar in welfare programmes. *SSRN 3045235*.

Kovacs, Anja, Padte, Richa, & Shobha, S.V. (2013). 'Don't Let it Stand!' An Exploratory Study of Women and Verbal Online Abuse in India.

Kovacs, Anja. (2017). 'Chupke, Chupke': Going Behind the Mobile Phone Bans in North India. https://genderingsurveillance.internetdemocracy.in/phone_ban/

Kovacs, Anja. (2017a, February). *Reading Surveillance through a Gendered Lens: Some Theory*. *Gendering Surveillance*. <https://genderingsurveillance.internetdemocracy.in/theory/>.

Kovacs, Anja. (2018, January 12). Playing the Aadhaar card. *India Today*. <https://www.indiatoday.in/magazine/cover-story/story/20180122-aadhaar-card-privacy-uidai-11313772018-01-12>

Kovacs, Anja. (2020, May 28). *When our bodies become data, where does that leave us?* *Deep Dives*. <https://deepdives.in/when-our-bodies-become-data-where-does-that-leave-us-906674f6a969>

Kovacs, Anja, & Ranganathan, Nayantara. (2019). Data sovereignty, of whom? Limits and suitability of sovereignty frameworks for data in India. *Data Governance Network*.

Kovacs, Anja, & Jain, Tripti. (2020) *Informed Consent - Said Who? A Feminist Perspective on Principles of Consent in the Age of Embodied Data*.

KRSRAC KGIS. (2020). *Corona Watch (Version 1.07)*. [Mobile application software]. https://play.google.com/store/apps/details?id=com.ksrsac.drawshapefile&hl=en_IN.

Kulkarni, Rupal. (2020, April 30). Covid lockdown: In rural India, banking correspondents bring cash, emotional support to the doorstep. *Scroll.in*. <https://scroll.in/article/960599/covid-lockdown-in-rural-india-banking-correspondents-bring-cash-emotional-support-to-the-doorstep>

Kumar, Awanish. (2020). Reading Ambedkar in the Time of COVID-19. *Economic and Political Weekly*, 55(16), 34.

Kumar, Arjun, Mehta, Balwant Singh & Mehta, Simi. (2020, April 17). *The link between lockdown, COVID 19, and domestic violence*. *International Development Review*. <https://idronline.org/the-link-between-lockdown-covid-19-and-domestic-violence/>

Kumar, Radha (1993): *The History of Doing: An Account of Women's Rights and Feminism in India*, *New Delhi: Zubaan*, p 128.

Lupton, Deborah. (2016). *The quantified self*. John Wiley & Sons.

Lyon, David. (Ed.). (2003). *Surveillance as social sorting: Privacy, risk, and digital discrimination*. Psychology Press.

Lyon, David. (2007). *Surveillance Studies: An Overview*. Cambridge, UK: Polity.

Madur. (2020, June 17). *COVID Guidelines For Resident Welfare Associations*. Karnataka.com. <https://www.karnataka.com/govt/covid-guidelines-for-resident-welfare-associations/>

Mahanta, Upasana, & Bharadwaj, Gargi. (2019). Does feminist historiography have an emancipatory potential? *EPW Engage*. <https://www.epw.in/engage/article/does-feminist-historiography-have-emancipatory-potential>

Malhotra, Vanshika. (2020, April 10). Swachhata-MoHUA app: Use this app to complain about Coronavirus lockdown violation, get food on Android, iOS. *India TV News*. <https://www.indiatvnews.com/technology/apps-mohua-swachhata-app-report-coronavirus-lockdown-violation-how-to-download-android-ios-how-to-use-606340>

Martin, Aaron K., Van Brakel, Rosamunde. E., & Bernhard, Daniel. J. (2009). Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework. *Surveillance & Society*, 6(3), 213-232.

Marx, Gary T. (2002). What's New About the "New Surveillance"? Classifying for Change and Continuity. *Surveillance & Society*, 1(1), 9-29.

McCahill, Michael. (1998) Beyond Foucault: Towards a Contemporary Theory of Surveillance. In Norris, Clive, Moran, Jade, & Armstrong, Gary (eds) *Surveillance, Closed Circuit Television, and Social Control*, Aldershot: Ashgate.

McIntosh, Ian, Samantha Punch, Nika Dorrer and Ruth Emond. 2010. 'You Don't Have to be Watched to Make Your Toast': Surveillance and Food Practices within Residential Care for Young People. *Surveillance & Society* 7(3/4): 290-303

Menezes, Naveen. (2020, July 8). *Bangalore Mirror*. <https://bangaloremirror.indiatimes.com/bangalore/others/all-work-no-pay-forget-promised-salary-hike-asha-workers-havent-even-got-what-is-rightfully-due-to-them/articleshow/76844445.cms>

Menon, Geeta (2020, June 15). Domestic workers to protest loss of jobs, wages during lockdown. *Citizen Matters, Bengaluru*. <https://bengaluru.citizenmatters.in/bengaluru-domestic-workers-job-loss-no-wages-covid-19-lockdown-dwru-46617>

Menon, Nivedita (2020, May 20). MIGRANT WORKERS' RESISTANCE MAP: Migrant Workers Solidarity Network. *Kafila*. <https://kafila.online/2020/05/20/migrant-workers-resistance-map-migrant-workers-solidarity-network/>

Migrants continue to walk thousands of miles to reach home. (2020, May 17). *Indian Express*. <https://indianexpress.com/photos/india-news/migrant-labourers-coronavirus-covid-19-india-lockdown-6410843/>

Migrant Workers Solidarity Network (n.d.). <https://www.mwsn.in/>

Milligan, Christine, Maggie Mort, and Celia Roberts (2010). Cracks in the Door? Technology and the Shifting Topology of Care. In *New Technologies and Emerging Spaces of Care*. Michael Schillmeier and Miquel Domènech eds., pp 19-38. *Farnham: Ashgate*.

Ministry of Electronics and Information Technology, Government of India. (2018). *National e-Governance Plan*. <https://meity.gov.in/divisions/national-e-governance-plan>

Ministry of Home Affairs. (2020). *National Migrant Information System*. <https://pib.gov.in/PressReleasePage.aspx?PRID=1624540>

Mishra, Harshita (2020, April 28). COVID-19 and activism's digital makeover. *The Hindu*. <https://www.thehindu.com/news/national/covid-19-and-activisms-digital-makeover/article31454884.ece>

Mishra, Manish Chandra. (2020, May 28). Bihar's Rs 1,000 Relief Not Reaching Broke & Hungry Migrants. *IndiaSpend*. <https://www.indiaspend.com/bihars-rs-1000-relief-not-reaching-broke-hungry-migrants/>.

Modak, Sadaf. (2020, April 11). One held for beating up Dalit man, spreading virus rumours. *Indian Express*. <https://indianexpress.com/article/cities/mumbai/coronavirus-one-held-for-beating-up-dalit-man-spreading-virus-rumours-6357207/>.

Mohanty, Debarata. (2020, April 24). Asha worker attacked for collecting data on Covid-19 patients in Odisha. *Hindustan Times*. <https://www.hindustantimes.com/india-news/asha-worker-attacked-for-collecting-data-on-covid-19-ve-patients-in-odisha/story-AZxHd8YHM1zGLnPkBdMUMN.html>.

Mol, Annemarie (2008). *The logic of care: Health and the problem of patient choice*. Routledge.

Monahan, Torin. (2009). Dreams of Control at a Distance: Gender, Surveillance and Social Control. *Cultural Studies ↔ Critical Methodologies*, 9(2): 286-305.

Monahan, Torin. (2010). *Surveillance in the Time of Insecurity*. New Brunswick, NJ and London: Rutgers University Press.

MyGate. (n.d.). *Home*. MyGate. <https://mygate.com/>

Mykhalovskiy, Eric. 2015. The Public Health Implications of HIV Criminalization: Past, Current, and Future Research Directions. *Critical Public Health* 25 (4): 373–385

Nandakumar, Prathima. (2020, April 2). Bengaluru: Locals attack ASHA workers on COVID-19 screening duty. *The Week*. <https://www.theweek.in/news/india/2020/04/02/bengaluru-locals-attack-asha-workers-covid-19-duty.html>.

Narayanan, Rajendran, & Dhorajiwala, Sakina. (2019, December 9). *The Namesake: Human Costs of Digital Identities*. EPW Engage.

National Disaster Management Authority & Coalition for Disaster Resilient Infrastructure. (2020). *Response to COVID-19 Kerala*. <https://ndma.gov.in/images/covid/response-to-covid19-by-kerala.pdf>

NCW launches WhatsApp number to report domestic violence during COVID-19 lockdown (2020). *The Economic Times*. <https://economictimes.indiatimes.com/news/politics-and-nation/ncw-launches-whatsapp-number-to-report-domestic-violence-during-covid-19-lockdown/articleshow/75082848.cms?from=mdr>

NDTV. *Domestic Violence Cases Have Risen Since COVID-19 Lockdown: Women's Panel* [Video file]. (2020, April 3). <https://www.ndtv.com/video/news/news/domestic-violence-cases-have-risen-since-covid-19-lockdown-women-s-panel-544604?pfrom=home-videos>.

Norris, Clive. (2005). From personal to digital: CCTV, the panopticon, and the technological mediation of suspicion and social control. In *Surveillance as social sorting* (pp. 263-295). *Routledge*.

Odisha makes Aadhaar mandatory for pension, 11 lakh pensioners could lose benefits. (2020, August 12). *National Herald*. <https://www.nationalheraldindia.com/india/odisha-makes-aadhar-mandatory-for-pension-11-lakh-pensioners-could-lose-benefits>

Panchanadeswaran, S., Unnithan, A. M., Chacko, S., Brazda, M., & Kuruppu, S. (2017). What's technology got to do with it? Exploring the impact of mobile phones on female sex workers' lives and livelihood in India. *Gender, Technology and Development*, 21(1-2), 152-167.

Pande, Rohini, Schaner, Simone, Moore, Charity Troyer, & Stacy, Elena. (2020, April 17). A Majority of India's Poor Women May Miss COVID-19 PMJDY Cash Transfers. *Yale*

Economic Growth Center, Yale Macmillan Center and USC Dornsife Center for Economic and Social Research. <https://egc.yale.edu/sites/default/files/COVID%20Brief.pdf>

Pandey, Vikas. (2020, April 8). Coronavirus: India home quarantine families face discrimination. BBC India. <https://www.bbc.com/news/world-asia-india-52201706>

Perrigo, Billy. (2020, April 3). It Was Already Dangerous to Be Muslim in India. Then Came the Coronavirus. *Time*. <https://time.com/5815264/coronavirus-india-islamophobia-coronajihad/>.

Poovanna, Sharan. (2020, July 15). Covid-19: Bengaluru police invite citizens to help in community engagement. *Livemint*. <https://www.livemint.com/news/india/covid-19-bengaluru-police-invite-citizens-to-help-in-community-engagement-11594803235737.html>

Pradhan Mantri Jan-Dhan Yojana (n.d.). <https://www.pmjdy.gov.in/scheme>

Radhakrishna, Meena. (2001). *Dishonoured by History: "Criminal Tribes" and British Colonial Policy*. Orient Blackswan.

Radhakrishnan, Radhika. (2020). Call for inputs: Surveillance and marginalised communities during COVID19. *Internet Democracy Project*. <https://internetdemocracy.in/2020/05/call-for-inputs-surveillance-and-marginalised-communities-during-covid19/>

Raghuram, Parvati. (2001). Caste and Gender in the Organisation of Paid Domestic Work in India. *Work, Employment & Society*, 15(3), 607–617. doi:10.1017/s0950017001000381

Raj, Arpita. (2020, May 15). 'We Can't Work From Home': B'luru Domestic Workers Want to be Paid. *The Quint*. <https://www.thequint.com/coronavirus/they-said-we-spread-coronavirus-bengaluru-domestic-workers-want-minimum-wage>.

Ramanathan, Usha (2019). *Aadhaar—From Welfare to Profit. Dissent on Aadhaar: Big Data Meets Big Brother*, ed. Reetika Khera. Hyderabad: Orient Blackswan, 178.

Ranganathan, Nayantara. (2017, February). Caution! Women at Work: Surveillance in Garments Factories. Gendering Surveillance. <https://genderingsurveillance.internetdemocracy.in/cctv/>.

Ranjit, Tanisha. (2020a). At stake is our bodily integrity. Retrieved 28 September 2020, from <https://www.genderit.org/resources/stake-our-bodily-integrity>

Ranjit, Tanisha (2020b). When and where is Aarogya Setu mandatory? We're keeping track. The Internet Democracy Project. <https://internetdemocracy.in/2020/05/aarogya-setu-tracker/>

Rao, Bhanupriya (2020, June 10). Article 14. <https://www.article-14.com/post/promised-mostly-never-paid-rs-1-000-covid-wage-to-million-health-workers>

Rao, Bhanupriya & Tewari, Saumya. (2020, June 9). Distress Among Health Workers In Covid-19 Fight. Article14. <https://www.article-14.com/post/anger-distress-among-india-s-frontline-workers-in-fight-against-covid-19>

Rao, Bhaskar [@deepolice12]. (2020, June 14). There is no State policy for Apartment Dwellers demand for such documents but I am proud of Bangalore RWAS who [Tweet]. Twitter. <https://twitter.com/deepolice12/status/1272049158694727681>.

Rao, Menaka. (2015, September 23). The Gendered Delay in the Diagnosis and Treatment of Tuberculosis Patients in India. Caravan. <https://caravanmagazine.in/vantage/gendered-delay-diagnosing-tuberculosis-patients>.

Rao, Menaka (2020, April 7). 'We will die doing our duty': How ASHAs are battling coronavirus without safety gear or training. *News Laundry*. <https://www.newslaundry.com/2020/04/07/we-will-die-doing-our-duty-how-ashas-are-battling-coronavirus-without-safety-gear-or-training>

Responding to COVID-19 - Learnings from Kerala. (2020). *World Health Organization*. <https://www.who.int/india/news/feature-stories/detail/responding-to-covid-19---learnings-from-kerala>

Right to Food Campaign, Odisha [@OrissaRtf]. (2020, August 16). A 83 year old bed ridden woman who already lost her ration card for not having #Aadhaar now is being denied of ex Gratia support of Rs 1000 with #pension for not having Aadhaar[Tweet]. Twitter. <https://mobile.twitter.com/OrissaRtf/status/1295041446261608449>

Rising Flame & Sightsavers. (2020). Neglected and Forgotten: Women with disabilities during the COVID 19 crisis in India. www.risingflame.org

Saha, S.K., & Bindal, Akshita. (2020, April 30). *Why Lockdown Is The Best Strategy For India To Fight COVID-19?* NITI Aayog. <https://niti.gov.in/why-lockdown-best-strategy-india-fight-covid-19>.

Sanghamitra, Meera [@meeracomposes]. (2020, March 29). #Transphobic Posters at Ameerpet Metro Station reads: "Warning: Do not allow Kojja, Hijras near the shops. If you talk to them [Tweet]. Twitter. <https://twitter.com/meeracomposes/status/1244074045882003456>.

Sanyal, Anindita (2020, April 5). Police Using Cellphone Data To Trace People Linked To Delhi Mosque Event. *NDTV*. <https://www.ndtv.com/delhi-news/delhi-police-using-cellphone-data-to-trace-people-linked-to-islamic-sect-meet-2206388>

Sapkale, Yogesh. (2020, June 29). *Beware! Aarogya Setu App is Marking People Corona Positive Due to Wrong Mobile Number Inputs*. MoneyLife. <https://www.moneylife.in/article/beware-aarogya-setu-app-is-marking-people-corona-positive-due-to-wrong-mobile-number-inputs/60757.html>

Satish, Mrinal. (2011). "Bad Characters, History Sheeters, Budding Goondas and Rowdies": Police Surveillance Files and Intelligence Databases in India. *National Law School of India Review*, 23(1), 33-160. <https://www.jstor.org/stable/44283744>.

Sebastian, Meryl. (2020, March 26). Coronavirus: Kerala Police Is Using This Tech To Monitor People In Quarantine. *Huffington Post India*. https://www.huffingtonpost.in/entry/kerala-police-quarantine-surveillance_in_5e7c801ac5b6cb9dc19ae2d9.

Sehgal, Manjeet. (2020). App to track Covid-19 home quarantined patients' movement in Chandigarh. *India Today*. <https://www.indiatoday.in/mail-today/story/app-to-track-covid-19-home-quarantined-patients-movement-in-chandigarh-1666292-2020-04-13>

Sen, Kalyani Menon. (2020, April 25). From Aadhaar to Aarogya Setu: How surveillance technology is devaluing India's democratic rights. *Scroll.in*. <https://scroll.in/article/960137/from-aadhaar-to-aarogya-setu-how-surveillance-technology-is-devaluing-indias-democratic-rights>

Sen, Rukmini. (2020, June 23). Stay Home, Stay Safe: Interrogating Violence in the Domestic Sphere. *EPW Engage*. <https://www.epw.in/engage/article/stay-home-stay-safe-interrogating-violence>

Sengupta, S. (2020). How To Stir Confusion Amidst a Pandemic: COVID-19 and Misinformation on WhatsApp. *EPW Engage*. Sengupta, Shuddhabrata. (2020, April 15). Coronavirus Lockdown: The Seven and a Half Things that Modi Said and Did Not Say. *The Wire*. <https://thewire.in/politics/coronavirus-lockdown-the-seven-and-a-half-things-that-modi-said-and-did-not-say>

Sharma, Betwa. (2020, March 28). Flight Attendant Quarantined By Govt, Harassed By RWA: COVID-19 Brings Out Middle-Class India's Worst Impulses. *HuffPost India*. https://www.huffingtonpost.in/entry/quarantined-govt-coronavirus-india_in_5e7da410c5b661492264fd39.

Sharma, Milan. (2020, March 21). Coronavirus in India: No thermal screening at most domestic airports yet. *India Today*. <https://www.indiatoday.in/india/story/no-thermal-screening-at-most-domestic-airports-yet-1658059-2020-03-21>

Shenoy, Jaideep. (2020, August 11). Covid-19: Dakshina Kannada tops Karnataka in use of 'Quarantine Watch'. *Times of India*. <https://timesofindia.indiatimes.com/city/mangaluru/covid-19-daksina-kannada-tops-karnataka-in-use-of-quarantine-watch/articleshow/77485907.cms>.

Smith, Gavin J. (2016). Surveillance, data and embodiment: On the work of being watched. *Body & Society*, 22(2), 108-139.

Social Stigma associated with COVID-19. (2020). *World Health Organization*. <https://www.who.int/docs/default-source/coronaviruse/covid19-stigma-guide.pdf>

Sriraman, Tarangini. (2020, March 22). Plague passport to detention — Epidemic Act was a medical surveillance tool in British India. *The Print*. <https://theprint.in/opinion/plague-passport-to-detention-epidemic-act-was-a-medical-surveillance-tool-in-british-india/385121/>

Stranded Workers Action Network (2020). *To leave or not to leave*. <http://strandedworkers.in/mdocuments/library/>

Sur, Priyali. (2020, April 16). Under India's caste system, Dalits are considered untouchable. The coronavirus is intensifying that slur. *CNN*. <https://edition.cnn.com/2020/04/15/asia/india-coronavirus-lower-castes-hnk-intl/index.html>

Swamy, Rohini. (2020, March 26). This is how Karnataka govt will keep track of nearly 15,000 people under home quarantine. *The Print*. <https://theprint.in/india/governance/this-is-how-karnataka-govt-will-keep-track-of-nearly-15000-people-under-home-quarantine/388870/>

Tarafder, Agnidipto & Sonkar, Siddharth. (2020, April 5). Dignity and Disinfectant in the Time of a Pandemic. *The Wire*. <https://thewire.in/government/bareilly-bleach-disinfectant-migrant-workers>

Teltumbde, Anand. (2018, August 4). The New Normal in Modi's 'New India'. *Economic and Political Weekly*, 53(31). <https://www.epw.in/journal/2018/31/margin-speak/new-normal-modis-%E2%80%98new-india%E2%80%99.html>

The five elements of DOTS. (n.d.). *World Health Organization*. <https://www.who.int/tb/dots/whatisdots/en/index2.html>

The Women Warriors Fighting COVID-19 At The Frontline: ASHA Workers Left Without Hope. (2020, May 21). *Amnesty International India*. <https://amnesty.org.in/the-women-warriors-fighting-covid-19-at-the-frontline-asha-workers-left-without-hope/>

The world's most valuable resource is no longer oil, but data. (2017). *The Economist*. <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>

Times of India. *UP: Woman walks 30 km to withdraw Rs 500, no Jan Dhan account, returns empty handed* [Video]. (2020, May 4) <https://timesofindia.indiatimes.com/videos/city/lucknow/up-woman-walks-30-km-to-withdraw-rs-500-no-jan-dhan-account-returns-empty-handed/videoshow/75525865.cms>.

Urs, Anil. (2020, March 31). Karnataka develops app to track home quarantined persons, *Business Line*. <https://www.thehindubusinessline.com/info-tech/karnataka-develops-app-to-track-home-quarantined-persons/article31214354.ece>

Vallee, Mickey. (2020). Doing nothing does something: Embodiment and data in the COVID-19 pandemic.

Van der Ploeg, Irma. (2003). Biometrics and the body as information: Normative issues of the socio technical coding of the body. *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination. Londres e Nova Iorque, Routledge, 57-73.*

Van der Ploeg, Irma (2012). The body as data in the age of information. *Kirstie Ball, Kevin & David Lyon (Eds.), Routledge Handbook of Surveillance Studies, 176-183.*

Vigilantism mars community policing. (2020, May 27). *The Hindu*. <https://www.thehindu.com/news/cities/Kochi/vigilantism-mars-community-policing/article31682455.ece>

Vij, Shivam. (2020, March 25). Modi's poorly planned lockdown won't save us from coronavirus, but will kill economy. *The Print*. <https://theprint.in/opinion/modis-poorly-planned-lockdown-wont-save-us-from-coronavirus-but-will-kill-economy/388056/>

Walsh, James P. (2010) From Border Control to Border Care: The Political and Ethical Potential of Surveillance. *Surveillance & Society* 8(2): 113–30.

Warrier, Aswanti. (2020, May 21). The Women Warriors Fighting COVID-19 At The Frontline: ASHA Workers Left Without Hope. *Amnesty International India*. Vigilantism mars community policing. (2020, May 27). *The Hindu*. <https://www.thehindu.com/news/cities/Kochi/vigilantism-mars-community-policing/article31682455.ece>

West, Lewis (2014). Jasbir Puar: Regimes of Surveillance. *Cosmologics Magazine*, 4 December, <http://cosmologicsmagazine.com/jasbir-puar-regimes-of-surveillance>

Woman with no medical history, symptoms quarantined by BMC. (2020, April 19). *Indian Express*. <https://indianexpress.com/article/cities/mumbai/woman-with-no-medical-history-symptoms-quarantined-by-bmc-6368834/>

Workers flag privacy concerns over use of Aarogya Setu app. (2020, August 10). *Times of India*. <https://timesofindia.indiatimes.com/city/hyderabad/workers-flag-privacy-concerns-over-use-of-aarogya-setu-app/articleshow/77453068.cms>

World Health Organization. (n.d.). *COVID-19: Physical Distancing*. <https://www.who.int/westernpacific/emergencies/covid-19/information/physical-distancing#:~:text=Physical%20distancing%20helps%20limit%20the,text%20to%20complete%20the%20message.>

Acknowledgements

I'd like to thank Dr. Anja Kovacs for helping me every step of the way for this study, from conceptualising it together till the last stage of writing. Thanks also to the Data Governance Network (DGN) for supporting this research. I'm grateful to Dr. Chayanika Shah and a blind reviewer assigned by DGN for their very valuable feedback on an earlier version of this paper. I'm also thankful to Devashree Somani for copy edits, and to Tanisha Ranjit, Tripti Jain, Shraddha Mahilkar, and Gautam Bhatia for their helpful comments. Lastly, but most significantly, this study would not have been possible without the conversations with all research participants who trusted me with their experiences. I hope the findings of this study contribute in some meaningful way to improving their lives.

About the Author

Radhika Radhakrishnan is a feminist researcher working at the Internet Democracy Project on the Bodies and Data Governance project. She has a Master's degree in Women's Studies from the Tata Institute of Social Sciences, Mumbai, and a Bachelor's degree in Computer Science Engineering from M.S. Ramaiah Institute of Technology, Bangalore. She previously worked with the Centre for Internet and Society (CIS) as a Programme Officer, with the Internet Governance Forum (IGF) of United Nations-DESA as a Consultant on Gender, and with the Women's Rights Programme of the Association for Progressive Communications (APC). She writes, speaks, and hosts podcasts on gender, sexuality, technology, and politics, and tweets at @so_radhikal.

 datagovernance.org  dgn@idfcinstitute.org

 [@datagovnetwork](https://twitter.com/datagovnetwork)  [/datagovnetwork](https://facebook.com/datagovnetwork)  [/datagovnetwork](https://youtube.com/datagovnetwork)