Development Informatics

Working Paper Series

The Development Informatics working paper series discusses the broad issues surrounding digital data, information, knowledge, information systems, and information and communication technologies in the process of socio-economic development

Paper No. 81

Capturing Gender and Class Inequities: *The CCTVisation of Delhi*

AAYUSH RATHI & AMBIKA TANDON

2019

Published in collaboration with, and with the financial support of, the University of Manchester's Sustainable Consumption Institute

Published by: ***Centre for Development Informatics***
Global Development Institute, SEED
University of Manchester, Arthur Lewis Building, Manchester, M13 9PL, UK
Email: cdi@manchester.ac.uk Web: http://www.cdi.manchester.ac.uk

View/Download from:
http://www.gdi.manchester.ac.uk/research/publications/di/

Table of Contents

Capturing Gender and Class Inequities: *The CCTVisation of Delhi*

Aayush Rathi & Ambika Tandon[1]
The Centre for Internet and Society (India)

2019

Abstract

Cityscapes across the global South, following historical trends in the North, are increasingly being littered by closed-circuit television (CCTV) cameras. In this paper, we study the wholesale implementation of CCTV in New Delhi, a city notorious for incredibly high rates of crime against women. The push for CCTV, then, became one of many approaches explored by the state in making the city safer for women.

In this paper, we deconstruct this narrative of greater surveillance equating to greater safety by using empirical evidence to understand the subjective experience of surveilling and being surveilled. By focussing on gender and utilising work from feminist thought, we find that the experience of surveillance is intersectionally mediated along the axes of class and gender. The gaze of CCTV is cast upon those already marginalised to arrive at normative encumbrances placed by private, neoliberal interests on the urban public space. The politicisation of CCTV has happened in this context, and continues unabated in the absence of any concerted policy apparatus regulating it. We frame our findings utilising an analytical data justice framework put forth by Heeks and Shekhar (2019). This comprehensively sets out a social justice agenda that situates CCTV within the socio-political contexts that are intertwined in the development and implementation of the technology itself.

[1] Authors are listed in alphabetical order.

A. Introduction

The past decade has seen monumental growth in video-based surveillance systems across cities in the global South. Governments have invested in such systems for a variety of reasons, including anti-terrorism initiatives, general safety and security, and law and order (Firmino and Duarte, 2015). Surveillance of public spaces is also directed at providing security to women from harassment and violence, as can be seen in cities such as New Delhi that are grappling with high incidence of crime against women. Accordingly, the location for this research is New Delhi.

Over the past decade, Delhi has developed a dense network of cameras. These are implemented and controlled by a complex network of both private and public actors, who share management, resources, and control over closed-circuit television (CCTV) spread throughout the city. Private actors controlling the system include property-owning individuals, commercial establishments, and Resident Welfare Associations (RWAs) and Market Welfare Associations (MWAs)[2]. Public stakeholders include the Delhi government, which is currently in the process of fulfilling its election promise of providing each electoral constituency in the city with extensive CCTV coverage, the central government, the Delhi Police, the Public Works Department, the Delhi Metro Railway Corporation and three municipal corporations.

This paper contributes to the discussion on CCTV surveillance from the perspective of data justice, which assesses the ability of a data system to provide social justice to those it impacts. We interrogate the extent to which CCTV cameras support the achievement of justice, particularly from the perspective of women using public spaces. To do so, we adopt Heeks and Shekhar's (2019) model of data justice which provides various dimensions to analyse datafication initiatives.

We also borrow concepts from feminist surveillance studies, which has been overtly political in critiquing the "heterosexual, heteronormative, and sexist male gaze" of surveillance of women and sexual minorities (Walby, 2005). In generating empirical evidence, we employ a feminist qualitative approach to question intersectional power dynamics and centre the embodiedness of data, safety, and privacy in the city. We align this with the framework of urban data justice to understand datafication as being embedded within the social contexts in which the data systems are operationalised. Existing literature on feminist surveillance has underrepresented the experiences of women in the global South, while data justice has, so far, not directly engaged with feminist thought.

One of the key research aims of the project, then, is to critically deconstruct this narrative of greater surveillance and visibility equating to greater safety by using empirical evidence to understand the subjective experience of being surveilled. This allows us to position CCTV cameras within the broader understanding of gendered access to geographical space as well as rights and justice systems. These feed into interrogating the extent to which CCTV in

[2] Resident Welfare Associations and Market Welfare Associations, as the names indicate, are elected non-governmental bodies that respectively represent the interests of residents or businesses operating out of particular residential or commercial areas.

Delhi is designed to enable accomplishment of the stated objectives of safety to women, especially those from informal settlements.

The paper is structured as follows. The first section provides a background of the existing literature that the study will draw upon or challenge, largely within the fields of urban data justice, surveillance studies, and feminist surveillance studies. After briefly discussing the methodology, the findings from the research are presented using the five dimensional analytical framework developed by Heeks and Shekhar (2019). Finally, we conclude with some further discussion, and propose recommendations and future research questions that arise out of the present study.

B. Background

B1. Feminist Surveillance Studies

A crucial aspect of this paper is to advance an understanding of how, taken-for-granted as benign, surveillance technologies such as CCTV systems end up impacting already disenfranchised bodies. The dominant rationality of neutrality and objectivity that lend support to these technological tools could be borne out of historical inequalities, or morph and challenge them. For instance, Ruha Benjamin has shown that new technologies are often thrust upon populations that have historically had to resist their imposition (Benjamin, 2016). Browne (2010, 2015) draws nuanced linkages between the historical modalities of policing slaves and contemporary technologies of surveillance such as biometrics. Questioning the supposed neutrality of these technologies allows for an exposition of the power relations that give rise to and govern the use of these technologies.

While not having been originally articulated in the context of ‘datafication’, a key theme utilised in feminist responses to surveillance borrows from feminist scholarship focusing on the intersectional, not additive, ways in which power differentials are wedded into the social relations of domination and resistance (Crenshaw, 1989). Using a critical intersectional feminist approach allows for the unravelling of “what constitutes surveillance, who is scrutinised, why and at what cost” (Dubrofsky and Magnet, 2015).

Monahan's (2009) conceptualisation of the overlapping gendered dimensions of surveillance is a useful analytical framework to draw from as well. Monahan conceptualises technology to mediate the reproduction and reinforcement of unequal power structures through: (a) body discrimination i.e. by privileging a certain type of person and rendering others as deviant, (b) context or use discrimination by reproducing already unequal social structures, and (c) discrimination by abstraction i.e. by the reduction to data points that facilitates the control from distance (*ibid.*). In other words, a feminist approach to surveillance allows for the interrogation of what the mythologies are that lend meaning to the technology in the first place.

That being said, most studies assessing CCTV along the axis of gender indicate general support for CCTV among women as a measure of providing the experience of safety and

security (Koskela, 2002; Huey, 2010). This can be found in studies such as Hasija and Nagpal's (2018), who in their survey of 250 young women in Delhi and their responses to CCTV found overwhelming support despite awareness of the risk of stalking and abuse and lack of clarity about the identity of the surveiller or objectives of surveillance.

Previous research assessing CCTV surveillance from a feminist lens has also highlighted the impact of subjectivities and power relations on the experience of video-based and other surveillance systems. For instance, Wright et al. (2014), in their study on video-based surveillance within apartment buildings in Toronto, found that women tended to identify as the objects of surveillance rather than agents conducting the surveillance, even in private settings where residents have a certain level of control over surveillant infrastructure. They further found that women were more likely to express trust in the surveillance system if their objectives aligned with that of the surveillant authority.

B2. Privacy and the Gaze through a Critical Feminist Lens

In addition to state and private surveillance, feminist scholars have also had a long engagement with the subject of privacy and its relation to the male gaze, expanding on the notion of differentiated rights. Adler-Bell (2018) argues that for marginalised communities, privacy in the form of "ungoverned" spaces has been historically inaccessible. The Fourth Amendment in the United States, for instance, defines privacy spatially - the "reasonable expectation of privacy" is largely within the private space of the home (*ibid.*). This then implies that privacy as a right is contingent on property rights rather than being a universal right; something available only to those who can afford it. This leads to a stratified access to privacy, with groups living in informal settlements and the homeless having the least access to privacy (Gellman and Adler-Bell, 2017). One of the possible consequences of differential access to the right to privacy for different groups is the enforcement of normative boundaries in public spaces.

This is also reflected in jurisprudence around privacy in the United States, where the Supreme Court has ruled that citizens should not expect privacy in public spaces, as the constitution does not prevent people from spying on each other in public (Firmino and Duarte, 2014). The conception of the right to privacy as only available in private spaces is contingent on the historical dichotomy between the two (public and private) kinds of spaces, which has been amply critiqued by feminist scholars. They critique the imposition of modesty and domestic isolation on middle and upper class women in India and other contexts as a result of the private/public divide, which has also led feminist writers to critique the notion of privacy itself (Allen, 2011). Feminists argue that framing the discourse of privacy as protectionist, including in the context of video-based surveillance, does not align with a rights-based approach that would aim to increase decisional autonomy among women (Thomasen, 2018).

In the context of India, Phadke et al. (2011) argue that the threat posed by public spaces to 'respectable' women is constructed within middle class discourse as arising from lower class or Muslim men. In a three year project on the use of urban public space in Mumbai, they find women internalised this discourse, identifying Muslim and lower class men as a source of anxiety and threat (*ibid.*). This then justifies placing the surveillant (protectionist) gaze on

middle class women and the surveillant (suspicious) gaze on lower class men - mediating access to public space for both.

Khan (2018) argues that in urban Pakistan, women are put under the surveillant gazes of men and the paternalistic state as they enter public spaces, with the attempt to provide women security by "inverting the male gaze onto itself". This is a function of state surveillance also embodying characteristics of the male gaze, such that only particular types of "good women" are guaranteed protection - those who enter public space for legitimate purposes and have a character deemed "worthy of protection" (Khan, 2018).

However, rights-based framings of privacy have also been critiqued by feminists for starting from the perspective of an individualised subject with bargaining power (Allen, 2011). Individualisation has the potential to invisibilise the web of power and social relations which mediate decision-making for women across the global South, including about their own bodies (Weinberg, 2017).

Kovacs (2017), while critiquing surveillance through the lens of gender, invokes Lyon (2003) in arguing for a shift from the individual rights-based framing of privacy to that of social justice, since surveillance is a "structural" rather than "individual" problem. This aligns well with the theorisation of data justice, the starting point for which is embedding data systems in their social context and web of power relations (Taylor, 2017).

B3. Data Justice

Where the discourse around CCTV surveillance, as with other data-driven systems, has been framed around tradeoffs between efficient security, privacy, and data protection (Dencik et al., 2016), data justice allows for factoring in the politics of data by squarely situating these data-driven systems within the social contexts in which they are embedded (Taylor, 2017).

Recognising the shifts in the social contract that datafication is bringing about, Taylor (2017) utilises a 'capabilities' approach to bridge disparate conversations around data justice to carve out three pillars on which an international data justice approach could be premised: (in)visibility, (dis)engagement with technology and anti-discrimination. Taylor (2017) argues that these integrate the key negative and positive freedoms which are required by individuals for a fair engagement with data systems globally. For instance, along with the right to privacy, this would include the right to be represented, or to move out of the "surveillance gap" - which applies to individuals or groups who are excluded from databases depriving them of critical rights ranging from citizenship to welfare benefits (Gilman and Green, 2018).

Heeks and Shekhar (2019) provide an overarching analytical framework to think through the different dimensions of data justice. As mentioned earlier, we use their model to situate our case study of CCTV systems in Delhi. They define data justice as having five dimensions, relating to data flows and results of the data system. The first dimension, that of procedural data justice, relates to the processes of data handling within the "information value chain": the flow from data through information and decisions to actions and results. It indicates the level of inclusion across different points in the value chain, upstream (relating to data and

information) and downstream (relating to decisions and actions), which in turn indicates the distribution of those contributing data and those who make decisions utilising that data. The second dimension relates to instrumental data justice, or fairness in the results of the data system. Rights-based data justice relates to the enforcement of the negative and positive rights outlined by Taylor's (2017) framework, including representation and anti-discrimination. Structural data justice pertains to the extent to which the 'structure', constituted by dominant actors and institutions, supports social justice in the functioning of data systems. Finally, distributive data justice encompasses all of the categories detailed above, and relates to broader concerns of justice and equity (or lack thereof) that underpin data systems. Put simply, it is "the concern for who gets what as a result of data systems" (Heeks and Shekhar, 2019).

B4. Neoliberal Governance and Urban Planning

Data justice - particularly the structural dimension - concerns itself with the political economy of the data system, and the extent to which it is dictated by, or challenges, power differentials. Recent work has noted the increasing privatisation of public spaces, reflected in practices of neoliberal governance and the discourse around data-driven 'smart cities' (Firmino and Duarte, 2015; Coletta et al., 2018). A critical imperative within this discourse is projecting efficiency to attract investment by global capital (Firmino and Duarte, 2015). Phadke et al. (2011) argue that this imperative inherently conflicts with the rights of marginalised groups to equally access public spaces, as they get sanitised and commercialised. They go so far as to say that private spaces of consumption then "masquerade" as public spaces, welcoming only those with the "capacity to buy" (*ibid.*).

This happens, in part, through privately funded surveillance systems that impose the normative boundaries on public spaces, set by private actors. Fyfe (2004) characterises public-private partnerships in the United Kingdom as a way of "justifying private control over public spaces". He argues that private surveillance excludes those individuals that are considered deviant by the private actors that control the surveillance system (*ibid.*). Minnaar (2012), in an empirical study on growth of CCTV in South Africa, demonstrates that such growth can be mapped onto the parallel growth of gated neighbourhood enclosures. Gated residential enclosures have also sprung up all over New Delhi, and have been illegally encroaching on public spaces through the city (Govindarajan, 2016). Video-based surveillance in semi-private spaces such as gated residential areas then distributes security unequally (Huey, 2010), and could even reinforce caste and class relations by policing workers (Alkazi, 2015).

Firmino and Duarte (2015) further argue that the public-private model of CCTV systems leads to "scattered networks of technologies and practices", as opposed to acting like a centralised control system as has been projected in the discourse of urban planning. These are then understood to be locally contextualised and mediated, rather than entirely top-down systems with perfect command-and-control centres. Despite such fragmentation, it has been argued that constant awareness as a risk management strategy has become an integral identifier of contemporary societies (Giddens, 1990; Beck, 1992). As video-based surveillance systems move towards greater integration, penology moves away from problem diagnosis towards risk management (*ibid.*). An "actuarial" approach to managing

criminal activity at the aggregated level of entire populations is then seen to be taking hold (McCahill, 2002).

C. Methodology

The study takes a feminist approach to qualitative methods. Drawing on Wickramasinghe's (2009) conception of feminist epistemology of knowledge in the global South, we conducted semi-structured, in-depth interviews to bring out lived experiences of surveillance among different stakeholders, with a focus on women living in informal settlements in Delhi. Other stakeholders were interviewed to surface the social relations in which the surveillance system is embedded. We interviewed six categories of stakeholders, listed in Table 1. Interviews also allowed us to glean perspectives of different stakeholders to interrogate dominant, alternative, and counter narratives around video-based surveillance and privacy, and integrate these into a theoretical framework of urban data justice.

We employed purposive sampling, aiming to gather perspectives from across key stakeholders engaged in and affected by video-based surveillance of public spaces in New Delhi. We employed the snowballing technique within purposive sampling for law enforcement and government officials, and attempted to diversify civilian respondents by class.

In addition to the interviews, some observational and anecdotal evidence was also collected during the course of the fieldwork, by observing meetings between stakeholders. Finally, we also sent in Right to Information requests to the Delhi Police inquiring about budgetary allocations to cameras and drones under programmes that aim to ensure safety for women.

Stakeholder Group	**No. of Respondents**
Women using public spaces	15
Delhi Police	11
Delhi Metro Railway Corporation/Central Industrial Security Force	4
Resident Welfare Association	7
Commercial Establishments	8
Government Officials (Ministry of Women and Child Development, Public Works Department, New Delhi Municipal Council, civil servants)	5
Total	**50**

Table 1: Stakeholders Interviewed

D. Findings

D1. Procedural Data Justice

Fragmentation and function creep

Several differing motivations and functions behind investment into video-based surveillance by the police and state emerged during the course of our research. This has implications for the manner in which data flows are structured and data handling processes are designed. While it is unclear precisely when and what the motivations were behind the initial uptake of CCTV installation in Delhi, one of our respondents from law enforcement suggested that initial installations were rolled out in the course of preparations for New Delhi hosting the 2010 Commonwealth Games.[3] This is in consonance with other efforts to commercialise the city and make it appear worthy of investment including slum demolition and the growth of surveillance systems with commercial interests (something seen in other cities in the global South (Minnaar, 2012)).

The well-publicised push for CCTV installation in Delhi commenced as a response to the country-wide protests following the multi-perpetrator rape of a young female in New Delhi in 2012. A sizeable corpus of INR 6.6 billion (c.USD 96.5 million) earmarked for this purpose - the Nirbhaya Fund - was set up by the central government in the immediate aftermath of the rape. The installation of CCTV formed a part of technological solutions that were to play a key role in making cities safer for women (Ministry of Women and Child Development, n.d.). From 2010 until February 2018, about 5,000 CCTV cameras were installed by the Delhi Police. However, as indicated by the responses to our Right to Information application to the Delhi Police, none of them have been installed under the Nirbhaya Fund. Moreover, an interview with an official of the nodal ministry for the corpus indicated that the ministry's outlook now was that CCTV systems are not to be funded out of the corpus as they were ineffective in enhancing safety - at least in the ministry's articulation of safety - and were more effective for the purposes of investigation.

What has also emerged is a fragmented yet organised matrix of CCTV systems used to surveil over public spaces and perform undefined roles, as theorised by Firmino and Duarte (2015) previously. This then leads to the utilisation of CCTV for purposes that are determined on an *ad hoc* needs basis. For instance, while CCTV systems have been installed primarily to increase safety for women in public spaces, the police unit that is specifically designed to address crimes relating to women and children had no role to play in the implementation or monitoring of such systems. In a similar vein, the implementation of CCTV cameras by the metro corporation was initially meant to aid in operational and crowd control objectives, and the utilisation of CCTV cameras for security purposes then became a by-product. Meanwhile, the objectives behind installation of a CCTV camera system by the municipal council in its jurisdiction was intended for maintenance of public order, not criminal activity as such.

[3] The respondent also suggested that most of the cameras installed back in 2010 while preparing for the Commonwealth Games are probably dysfunctional now and need to be replaced.

Another way in which contradicting purposes behind CCTV installations emerge is by observing the provisioning of signage, if any, designed to indicate ongoing surveillance. Simply put, law enforcement officials described two aims behind placing visible signage accompanying CCTV cameras, (a) crime deterrence, and (b) making those under the camera's gaze feel safer by knowing they are being watched. On the other hand, covert surveillance, i.e. CCTV installations without any indication of such installation, aims to watch without the knowledge of the person being watched, which then has detection of crime as its primary motive. The two sets of objectives come into conflict, and are often adopted on an *ad hoc* basis.

For example, in a busy marketplace in Delhi, widespread CCTV installations by the MWA in this public spot were accompanied by regular announcements on the public address system informing those in the marketplace of being under surveillance. A law enforcement official posted at the marketplace, then, also indicated that CCTV cameras were intended to deter crime and for post-facto investigation. Within the same marketplace, however, several commercial establishments that we spoke to indicated that while they had initially installed cameras as an "insurance" against crime, a key purpose that they served now was to monitor stock as well as employees - or managerial surveillance, in other words. These commercial establishments either did not have any signage or the few that did opined that the signage was a relic from when they had initially installed the cameras, and that it served "no real purpose". For the commercial establishments especially, the symbolic deterrent effect of CCTV cameras (Hempel and Töpfer, 2004), then, is significantly diluted owing to an array of reasons: irregular monitoring, informational overkill, and the inertia within law enforcement.

The selective use of signage could additionally contribute to an information asymmetry between the implementers of CCTV cameras and those being surveilled. This argument is substantiated further in the next subsection.

Access to information

We found that a number of women were unaware of the existence of cameras installed or governed by law enforcement, except in places where cameras are very visible, such as in metro stations. A few interviewees expressed discomfort with the topic of conversation due to their perception of low levels of knowledge regarding CCTV cameras, and some women who were approached even refused to interview, citing their lack of any knowledge. None of the interviewees were aware of the extent or locations of camera coverage, the identity of surveilling authorities, or the demarcation between private and public systems - even if they were aware of the general existence of CCTV cameras. This information asymmetry was explicitly endorsed by some of our respondents within the Delhi Police, as they understood the purpose of CCTV surveillance to primarily be of crime detection. This, according to them, then mandates the least level of information dispersion, as surveillance was understood to be a covert activity to be performed without the knowledge of the watched.

In most cases, however, this did not erode trust in the system, as the general awareness of cameras operated by law enforcement made women feel safer, especially in isolated areas. This is in contrast to Koskela's (2002) interviewees, whose trust in the system was

significantly eroded by lack of knowledge regarding the identity and location of the surveillers. This could partly be attributed to the perceived lack of capacity and approachability of, and therefore trust in, the Delhi Police. Women across locations and classes, with a few exceptions, expressed the inadequacy of the Delhi Police in responding to crimes against women. By and large, women who expressed distrust in the police also expressed increased trust in technological systems, perceiving them as unbiased and dispassionate observers.

To regulate or not to regulate

Delhi's CCTV project has stemmed from a drive towards crime control that is governed through coalitions between locally situated police, retailers, private citizenry and hyper-local governing institutions. What is emergent then is "scattered networks" (Firmino and Duarte, 2015). This has significant repercussions for the manner in which data is handled and the kinds of voices that become dominant in decision-making processes. Over the last 2 years, there have been calls from voices, albeit solitary, within the state machinery to have standard operating procedures in place that govern the installation of CCTV cameras (Barman, 2018). In the absence of any governing legislation speaking to the installation of CCTV cameras specifically, or data protection broadly, untethered power is being granted to both state and non-state actors without any accountability mechanism in place.

It was in this backdrop that a draft version of the "Delhi Rules for Regulation of CCTV Camera Systems in NCT [*National Capital Territory*] of Delhi, 2018" (CCTV Rules hereafter) were released. While the CCTV Rules still do not have the force of law, members of one RWA that we interviewed stated that the CCTV Rules make the CCTV installations legal and are being utilised to support further installation drives. The CCTV Rules seek to regulate the installation and use of CCTV cameras in public spaces in Delhi. The CCTV Rules do have some useful stipulations, such as somewhat limiting the purposes for which the information recorded is used, mandating signage indicating ongoing surveillance, and also on the utilisation of open technical standards. However, they fall short on several counts. For one, they treat the information recorded as belonging to the owner of the system with the right to access the information provided only to "authorised persons". It is unclear who such authorised persons are. Further, they pay performative obeisance to incorporating privacy protections when they state that "the camera shall be located at such place so that it shall not collect information which invades the privacy of an individual" (Government of Delhi, 2018). These stipulations read together encode an understanding of privacy as a condition that individuals occupying public spaces do not have a claim to. It is evident that a primary objective here is of according significantly enhanced law enforcement control to, knowledge of, and access to all CCTV installations "collecting information from a public space" (*ibid.*).

D2. Instrumental Data Justice

Security for whom?

The Delhi Police had installed 5,000 cameras across the city as of February 2018. A majority of its network comes from a public-private model of collaboration, called the 'Nigehbaan' scheme. This allows the Delhi Police to access another 175,000 cameras across the city. This

network includes cameras installed by private individuals or groups, including individual residents, businesses, wealthier RWAs and MWAs. An overwhelming majority of CCTV cameras in Delhi are thus implemented and controlled by private stakeholders. As has been pointed out in other cities across the global North and South, the privatisation of security in public spaces inevitably results in unequal access to security for different groups (Huey, 2010). This also brings into question data ownership, as it is very likely that the individuals being recorded would not even have ready access to the footage, or any procedures in place in order to do so.

Access to public space itself becomes unequal, as privately funded security systems privilege the interests of the landed class or those with commercial capital and discriminate against lower caste and class groups entering those spaces (Alkazi, 2015). The interests of those who own surveillance systems often come into conflict with interests of those without access to resources and capital to perform surveillance - posing challenges to rights to access and ownership of data and data systems. This surveillance system can then be seen as a concrete reproduction of the 'suspicious gaze', extending here to all workers entering gated residential areas and other privately surveilled public spaces (Phadke et al., 2011).

Such conflicts emerged during a meeting we observed between residents of a gated residential area with local police officials in the south of New Delhi. Residents raised several questions demanding the implementation of CCTV, which they were told has been taken care of by the RWA. Law enforcement and residents then discussed security issues in the area, largely seen as arising from the entry of workers such as private security personnel, cab drivers and domestic workers within the gated community. Both residents and law enforcement discursively positioned workers as potential criminals to be controlled through surveillance systems. It is in such a context that CCTV systems are being introduced into the gated area, including those being funded by the Delhi government. The privatisation of data and data systems then inevitably creates the conditions for distributive injustice, as data is extracted from lower class workers and benefits accrue to upper or middle class employers.

Simultaneously, we found that poorer sections of the urban landscape, such as slum camps - even those that are legally recognised by the state - were found to be existing in the surveillance gap (Gilman and Green, 2018). With no CCTV installations provided either by law enforcement or the state, these areas were curiously outside of the growing ubiquitousness of CCTV-based surveillance systems. This was consistent with the non-recognition of their requirement for basic amenities such as water drainage and pothole-free lanes. Contrast this with the experience of affluent gated communities where not only is there a web of privately installed CCTV cameras, but also funding and infrastructural support by the state for further installations. This leads to the structural invisibilisation of vulnerable groups with very little political voice.

Akin to how surveillance is utilised to reproduce power dynamics, the surveillance gap can be similarly utilised as a tool to exert social control (*ibid.*). While the "gap" is not something that is *de facto* intended to be bridged, our respondents expressed a strong preference for the installation of at least some CCTV cameras at the entry and exit points as a crime-deterrent tool in the absence of a responsive and approachable law enforcement mechanism. This lends further credence to the feminist understanding of privacy as having a

deeply contextual meaning, instead of implying the complete rejection of surveillance systems.

Conflicting expectations and objectives

This section deals with conflicting expectations within women respondents and law enforcement, which indicate different results of surveillance for different groups.
There emerged several fault lines, along the lines of caste, region, and class, within women respondents using public spaces. A small subset of women respondents, largely those who identified as middle class, advocated for CCTV cameras covering residential areas in which they lived. They expressed the need to monitor entry and exit points into gated residential spaces, and to regulate the movement of outsiders into what were perceived as private zones. These outsiders mostly constituted other marginalised groups, including working class men, male migrant workers from other states or neighbouring countries, and sex workers. This corroborates Phadke et al.'s (2011) conception of the dominant narrative of working class men being constructed as one of the primary threats to middle class women as they use public spaces, justifying the use of surveillance mechanisms to police both groups. Further, as corroborated by Wright et al. (2014), groups such as sex workers and beggars are at greater risk of persecution as they regularly perform solicitation on the street which either (a) heightens visibility in public spaces or (b) is criminalised when performed in public.

Fault lines between the objectives of civilian women respondents and surveilling authorities also emerged in several cases. Most women respondents argued that CCTV fulfilled either or both of two purposes – prevention and investigation. However, all our interviews with law enforcement indicated that there is little to no crime prevention, including sexual harassment and violence, that they have experienced or expect to experience in the future - at least while systems continue to be fragmented. In addition, women respondents also expected constant real-time monitoring in places where cameras had been installed, which is not the case across state and privately controlled systems. The perceived trade off being made by respondents between security and privacy in urban public spaces is then made in the context of limited information dispersion. This then leads to expectations of constant surveillance from a system that is excessively fragmented.

Fault lines were also found in specific use cases. We found that tracking missing persons is a regular function of the Delhi Metro surveillance system, which includes women or men who have run away from home. Maintaining the autonomy of the "missing persons" then lies at the discretion of the officers handling their case – as one respondent told us, they don't do anything "unethical" and therefore turn back husbands who are stalking their wives, but do help with cases of runaway persons whose parents report them as missing. That these fault lines appear along the axis of gender very frequently can also be found in other cases - such as in Orissa, when a camera that was installed to protect women against violence had to be removed after protests from women who did not want to be watched while bathing (PTI, 2012). These cases illustrate that the objectives and zones of protection determined by those in authority and those of the beneficiaries do not always overlap.

The conflicts then bring out contradictions in surveillance systems that are aimed at both control and care, demanding the balancing of the right to privacy against physical security (Taylor, 2017). Wright et al. (2014) describe this conflict as the extent to which "visibility threatens or provides safety". Reading the concept of the male gaze along with Monahan's (2009) understanding of context/use discrimination is relevant here. Read together, they speak to the masculinised and distanced monitoring of the feminine body and feminised spaces. As Monahan (*ibid.*) argues, "when social contexts are already marked by sexist relations, then surveillance (and other) technologies tend to amplify those tensions and inequalities". The case of the surveillant gaze and the voyeuristic gaze are, in this case, overlapping to disadvantage either particular groups across contexts (couples getting intimate), or all women in a particular zone of surveillance (on the beaches of Puri). The latter can be addressed through the principle of engagement with technology (*ibid.*) within the principles of data justice, which enables *selective* use of technology, and could then be mobilised to reject surveillance in certain public zones.

D3. Rights-Based Data Justice

Privacy and the surveillant male gaze

We found women respondents prioritising the right to be represented in video-based surveillance systems over their right to privacy, displaying very high levels of support for CCTV systems. This then implies that the CCTV system in the city provides rights-based data justice, in the trade-off between security and privacy. As in Hasija and Nagpal's (2018) study, women overwhelmingly chose the right to be represented in the surveillance systems with the perceived benefit of security. Unlike Hasija and Nagpal's study however, we did not find evidence of women feeling at risk of stalking or violations of privacy. We further found that respondents who supported video-based surveillance also felt that current levels of coverage in the city were low, advocating for further coverage of isolated or lonely roads in particular.

Respondents across the various stakeholders we interviewed indicated their understanding of privacy as confined to private spaces, which were amorphously defined. Individual police officials define the private zone based on their subjective understandings of privacy. One of our respondents from the Delhi Police, for instance, conceptualised private zones as any area inside one's home that is not visible from the street. It then appears that being constantly monitored and recorded is inevitable for those who do not have access to private property, limiting rights to disengage with technology. It was striking that it was only in the context in which privacy in public spaces was brought up by a law enforcement official in our interviews was when referring to areas that house senior government officials and those with political power, described as "VIPs". A senior Delhi Police official revealed that the provision of safety to VIPs could even be through the temporary installation of cameras on routes being used by such persons, which are then removed to protect the privacy of permanent residents in these areas which typically house a host of high-level politicians and government officials. The right to disengage from surveillance systems, a critical data right (Taylor, 2017), was only accessible to publicly elected officials and government officials at the very top of the hierarchy.

Women using public spaces affirmed the dominant discourse of privacy and public spaces being in completely separate domains, with privacy only to be sought and protected in the spatial understanding of the private domain. The lack of a conception of privacy in public spaces reiterates the gradations in access to the right to privacy outlined by feminists, through its contingency on a strict dichotomy between private and public spaces (Allen, 2011; Adler-Bell, 2018). The publicness of a space then justified, and even demanded, the presence of the surveillant gaze of law enforcement. The gaze is then aimed at sanitising public spaces of potentially dangerous elements, who could cause disruption to public order (Walby, 2005).

When asked whether they considered the leaking of footage of couples getting intimate in metro trains as a harm of CCTV-based surveillance, most women civilian respondents, with the exception of two, did not perceive this to be a privacy violation and blamed the couples for getting intimate in a public space. In a similar vein, Phadke et al. (2011) finds in her study that the discourse of privacy has been used to persecute couples for acts such as holding hands in public spaces, through the discourse of obscenity. Obscenity then overwhelms the privacy violation in the public imagination, with several respondents arguing that being intimate in a public space such as a metro, which has families and children, is against cultural norms of propriety in public spaces. This also points to the notion that expectations of privacy are hyperlocal and specific to the norms of a particular space.

Video surveillance in this case is used to enforce cultural behavioural norms by punishing deviance with not only the violation of privacy, but the removal of the expectation of privacy at all. This manifestation of privacy is very similar to Allen's (2011) notion of unpopular privacy - as an argument against autonomy.

Contrary to this, two women raised distinct objections to the leaking of footage of couples on the metro. One argued that such incidents are "disgusting" and "amount to the misuse of the public", particularly because the official monitoring the footage is "watching porn and gaining entertainment...they make a video of it and upload". The respondent raises a specific concern about the voyeuristic gaze of the surveillant authority, which brings disproportionate attention on women in public - including particular categories of vulnerability such as "breastfeeding women".

The second argument against data leaks, made by a respondent who described herself as being a recent entrant into public spaces without male companionship, supported increased protections against leakage "especially because people don't have knowledge of these things, and are very often not educated or aware". Lack of awareness could stem from poor access to information, barriers such as signs indicating the presence of cameras being in an unfamiliar language, or general unfamiliarity with public spaces due to barriers to access. It can be seen that categories such as women with unequal access to public space, undereducated groups, and migrants then simultaneously face higher risks of privacy violation (Adler-Bell, 2018) and/or have fewer resources or awareness to deal with such violation. This could then pose a threat to rights-based data justice as certain groups are overrepresented in the leaked data, and procedural data justice, as those groups are left out of the value-chain of information flows.

Criminalisation and the panoptic gaze

In our interviews with Delhi Police in Central Delhi, the part of the city with the maximum concentration of government offices and other state agencies, and also therefore of public demonstrations, we found protest gatherings to be one of the key sites of surveillance. Officials from control rooms that perform the surveillance revealed that some of the fish-eye cameras have been recently acquired and are only deployed in key locations - which includes the locations where political protests and public demonstrations are organised. The heightened surveillance at sites of public demonstrations are in a context where protesters can be detained or arrested for performing demonstrations as it constitutes a breach of public order, among other concerns (Delhi Police, 2019). Targeted surveillance at sites that have been demarcated for public demonstrations by law enforcement are an additional measure of control, in addition to prior permissions from law enforcement to stage such demonstrations. Taken together with instances of illegal detention, heightened surveillance adds to a context of constraints placed upon the right to freedom of assembly in the city.

This can be seen as an instance of a larger shift in how risk assessment and criminalisation is increasingly being thought of by law enforcement, with the imagination of heightened surveillance technology. Respondents involved in the implementation of CCTV systems expressed intentions to integrate other technologies in the 'ideal' security solution. Technologies such as facial recognition and video analytics were frequently suggested. One proposed implementation of facial recognition was of metro users at station entry and exit points. Among other functions, this could be used to expedite entry and exit from metro stations of certain categories of individuals such as government employees. The data of these individuals would be stored in a database against which the facial recognition software would cross-check the legitimacy of those seeking to enter or exit through this system. Another proposed implementation was for images of 'suspects' at metro stations to be searched in real-time against a database that already had stored images. Such 'searchability' in CCTV footage is also being desired nationally (NCRB, n.d.).

What these imaginations bring forth is the objective of CCTV-based systems to provide more than the raw data observed, and move towards the actuarial approach to crime management (McCahill, 2002). If implemented, these will have a profound impact on how CCTV systems are utilised, given that the data justice implications of these newer technologies such as facial recognition and artificial intelligence are only just starting to be understood by civil society. CCTV in and of itself, then, is also seen as a weak surveillance tool, whose integration with computer-based systems with sophisticated data processing power is crucial to then exercise more intensive surveillance (Lyon, 2001).

D4. Structural Data Justice

"At least then they will believe us"

Most participants from lower socioeconomic backgrounds had direct or secondary experiences of the Delhi Police as unresponsive to their needs or even violent. Poor women expressed very low levels of trust, with statements such as "the police is not meant for poor people, it is only meant for the rich". Several instances of such unresponsiveness were

detailed through interviews, including cases where the police took a response time of several days, delayed investigations, or even refused to investigate. One group of participants, selling goods close to a busy thoroughfare in Central Delhi, spoke about routinely facing violence from the police, and regularly getting taken to police stations for thefts that they did not commit. They believed themselves to be easy scapegoats during police investigations, due to their constant physical presence in public areas. Poor women felt a fear of unresponsiveness or violence in their interactions with law enforcement, in addition to their fear of harassment or violence from men in public spaces. They partly ascribed their persecution by law enforcement to their constant presence in public spaces, as they operated in public every day to earn their livelihoods.

Due to the historical experience of suspicion that the police displayed towards them, they felt that cameras in public spaces would allow them to provide incontrovertible evidence of either cases where they were complainants, or prove their innocence in cases where they have been falsely accused. One group of women also expressed that it might help them to carry investigations through, as the police personnel usually take four to five days to respond to complaints by which time witnesses may no longer be available. In all of these instances, the presence of a camera could provide or improve access to justice and legal recourse for citizens and communities who currently feel excluded from such systems.

However, several participants challenged this reading of the camera, and reiterated that it is merely an object embedded in the social context, rather than a free floating tool to be used for the benefit of the aggrieved. They were thus sceptical of the extent to which CCTV could enhance access to justice, without responsive officers carrying out investigations on the basis of that footage. This indicates that increased access to legal redressal through video surveillance is contingent on rights-based justice within broader social structures - it is critical for citizens to have access to legal systems and data flows for this potential to materialise.

Turning the gaze inwards

Several respondents from among law enforcement and government officials spoke about initiatives to provide CCTV coverage to public offices, such as police stations, civil servants' offices, and Public Works Department's offices. This is following a Supreme Court order in 2014 to install CCTV across police stations in the city, and has been explicitly identified as a move to prevent violence against women in police stations (Express News Service, 2019).

Three objectives emerged behind the coverage of police stations and other government offices in our interviews with law enforcement and government officials. One, providing officials protection from false complaints. In particular, police officials spoke about protecting themselves against false allegations of violence, while government officials spoke about false allegations of committing atrocities against Scheduled Castes and Tribes, or of sexual harassment in case of male officers. Two, increasing accountability to the public, by treating government offices as public spaces to be monitored and held accountable to citizens. Three, managerial surveillance, with monitoring of their own stations as well as through centralised monitoring of several stations in one control room. Each of these objectives could potentially contribute towards making policing systems and government

functioning more transparent and accountable to citizens, as their actions are made visible to the public and to each other. This requires greater emphasis on procedural aspects of data flows, with the inclusion of police officials upstream, and the inclusion of citizens downstream in the information value chain.

The configuration of the infrastructure of the monitoring system determines its contribution towards enabling accountability and transparency and ultimately, structural justice in the results of surveillance systems. In police stations, screens could either be placed in public areas such as reception rooms and/or in the offices of senior officials. We found some stations where screens were monitored and controlled only by senior officials, which could exacerbate power inequalities. During a field visit, for instance, we found that public demonstrators were told by beat officers that they would have to appear harsh in their behaviour since they were under surveillance from another station. On the other hand, a senior bureaucrat said that she uses CCTV cameras to ensure that each officer across departments is treating visitors properly. CCTV could then act as a tool to alleviate power inequalities between citizens and government and law enforcement, by making each stakeholder visible to the other. This is not the case in monitoring systems that prioritise upstream data flows (from citizens to state) over downstream ones (from state to citizens), posing barriers to data-just systems (Heeks and Shekhar, 2019).

E. Discussion and Conclusions

The design of contemporary urban spaces has been dominated by increasing concerns around securitisation. Achieving and maintaining these imaginations requires the reinforcing of implicit hierarchies, and by extension, exclusions, in public space. One way in which these have manifested is through geo-spatial segregations that are privately controlled. Indeed, the idea of the public itself has been constructed to value some social groups over others, with access to public space being made differentially available. That the urban public space itself is the medium as well as the outcome of social practices is abundantly clear. Exclusion and intolerance, and their conflation with safety and security, get negotiated and co-produced with others occupying the public space.

CCTV systems have proliferated remarkably in Delhi in the last few years, and continue to grow at remarkable levels even as this paper is being published. While there is a care motif at play here, it also showcases how disciplining functions co-evolve (see Lyon, 1994). Our findings indicate that the panoptic gaze is not a homogenous power exercised only by the surveiller, but is multifarious and intermingling. For example, one finding in this research is that the gaze of the panopticon is turned on itself, as both public servants and the public are both now within the gaze.

The disciplining power of the gaze also manifests in the internalisation of modesty ideals by women themselves, as women respondents in our street interviews indicated having internalised the absence of rights such as privacy that may be reasonably afforded in public spaces. The equating of increasing CCTV with increasing women's safety then indicates a contradiction in the shifting of the gender ideologies in public spaces, with women now required to be making themselves hypervisible in exchange for security guarantees from the

masculinised state. Visibility, then, is made to be a prerequisite to security. Moreover, women respondents in the study invariably identified as objects of surveillance rather than subjects, consistent with research on CCTV surveillance elsewhere (Wright et al., 2014). This is reflected in the lack of female representation among those planning and executing surveillance systems, even among those designed specifically to combat violence against women.

E1. Conclusions

The theoretical focus of work on CCTV systems has focussed on it at a post-installation stage, on its operation. Such a view leads to the dehumanising of video-based surveillance whereas the material realities unsurprisingly indicate the centrality of human engagement at every stage of implementation and operation. Re-centring the 'human element' allows for work around data justice to understand technological developments in light of larger, historical forms of structural and institutional oppression. We utilise this framework, particularly the model of data justice developed by Heeks and Shekhar (2019), to study the implementation of CCTV systems in New Delhi and the social context in which those systems are embedded. Further, explicitly attending to questions around gender, while incorporating methodological and epistemic innovations put forth in feminist thought, allows for the exposition of a social justice agenda. In doing so, we were able to centre the power relationships that underpin surveillance.

Within the dimension of procedural data justice, or justice in handling data systems, we interrogated the motivations and interests of those who control CCTV systems in Delhi. We found objectives devised by civilians, the state, and law enforcement to be mutable, and at times contradictory. The provision of signage, or lack thereof, was found to be indicative of different theories of change behind CCTV installation. Responses addressing the uses of CCTV were usually wide ranging: pre-emptive behavioural change, and/or post-facto evidence of crime, and/or performative security. The objective for the state, at times, was to protect commercial interests, also at odds with the propagated public narrative that makes CCTV crucial in enhancing women's safety in public spaces. This could arise from the lack of representation of marginalised interests at the procedural stage of the system, with implementation being largely controlled by private actors, law enforcement, or the state.

Results of the system, or instrumental data justice, were found to be critically dependent on the harms or benefits of visibility to the state. Thus, while most middle class women supported CCTV systems for enhancing their safety, most women from informal settlements found it useful to prove their innocence in cases of false accusations or when officials refused to believe their complaints. Women performing activities in public spaces that heightened visibility while also inviting public censure or disrupting public order, such as sex workers, were found to be accruing the harms of the voyeuristic and controlling gaze of the state and others using public spaces.

Within the dimension of rights-based data justice, a key right that we focus on is that of privacy within public spaces. Our findings indicate a deeply contextual articulation of privacy. Inherent in the articulation is an internalisation of a strict separation between what constitutes a public or private space with privacy only to be expected in the latter. This,

along with belief in the efficacy of CCTV in aiding greater security and safety, also provides the fuel for the articulation of greater CCTV coverage by the supposed beneficiaries of CCTV installation. However, contradictions emerge as this trade-off between privacy and security is made in an information-scarce environment, often intentionally designed as such by surveillers. The other key right we assessed was the right to be represented, which was unfulfilled for Informal settlements as they were found to be in the 'surveillance gap' despite wanting CCTV systems to deal with unresponsive law enforcement officials.

Finally, structural data justice, or the extent to which powerful institutions and individuals support the interests of equality and justice within data systems. We found that regardless of objectives and expectations of different stakeholders, the actual usage of CCTV systems is hyperlocal and determined by power relations, social norms, and institutional structures in the particular space in which it operates. This is also applicable to CCTV cameras that are placed upon law enforcement and government officials, which aim at turning the gaze of the state onto itself but can only succeed in doing so if upstream and downstream data flows are given equal attention.

E2. Recommendations

Given the multiplicity of actors that are engaged in the unrolling of Delhi's CCTVisation, as well as the breadth of intended beneficiaries, several conflicts emerge in how these systems are designed, who they are designed for, and what benefits and harms subsequently emerge. Such conflicts can be addressed through wide public consultations with different stakeholders, including non-governmental and civil society organisations working on women's rights, gender, urban planning, and the right to privacy, in addition to RWAs and MWAs (Goswami, 2018).

A recommendation that holds true for all datafication programmes in India that are at various stages of implementation is for the crafting of policy that ensures robust transparency and accountability measures are institutionalised. This is especially critical in the absence of any comprehensive data protection law. At the same time, there is a dire need for processes that mandate mechanisms of appraisal regarding the utility and subsequent appraisal of these datafication initiatives. This is glaring in the present case of CCTV, where it is effectively the mythology of the technology that is garnering the political support for increased demarcation of public funds towards the CCTV project.

The lack of any concerted approach towards the roll out of the CCTV programme has also led to potentially debilitating consequences owing to the *ad hoc* determination of use-cases by departments within government and law enforcement tasked with the mandate to implement CCTV. The case of the police unit that has been carved out to address crimes relating to women and children having no engagement with CCTV is telling. This is especially curious given the equating of more CCTV with enhanced women's safety, as well as a scenario where uptake of CCTV is being ensured in every police station in the city. Whether any internal processes govern this inter-departmental work allocation vis-a-vis CCTV is unclear, and in any case, opaque.

Future research agenda

An immediate research agenda is to better understand the implications of the 'newer' technologies creating big data systems such as facial recognition software and artificial intelligence applications for which use-cases are being cultivated in datafication programmes being spearheaded by the state. The political economy around these moves is as yet understudied, and urgent work is required to pre-empt some of the distinct ways in which the governance of society and the data justice potential of systems could be impacted. As these make their way into the delivery of welfare systems in the global South, what datafication programmes entail for contemporary understandings of the social contract, participation in a democratic society and for citizenship itself are more overarching questions that require urgent addressing.

Any data justice project explicitly occupies the realm of governance, making it a worthwhile bridge to inform any such project through disciplines that do not occupy the space. While this case study was one such attempt at *doing* feminist surveillance studies, a data justice project could, in some sense, bring together any disciplines more occupied with critical approaches such as urban studies, critical data studies and surveillance studies.

References

Adler-Bell, S. (2018). Privacy for whom? *The New Inquiry*, 21 Feb. https://thenewinquiry.com/privacy-for-whom/

Alkazi, A. (2015). *Gated Communities in Gurgaon: Caste and Class on the Urban Frontier*. Senior Projects Paper 114. Annandale-On-Hudson, NY: Bard College. https://digitalcommons.bard.edu/cgi/viewcontent.cgi?article=1249&context=senproj_s2015

Allen, A. L. (2011). *Unpopular Privacy: What Must We Hide?* Oxford: Oxford University Press.

Barman, S. (2018). State of surveillance: Who controls the data collected from CCTVs in the capital? *Indian Express*, 21 May. https://indianexpress.com/article/cities/delhi/state-of-surveillance-delhi-cctv-aap-anil-baijal-5184751/

Beck, U. (1992). *Risk Society: Towards a New Modernity* (first ed.). London: Sage Publications.

Benjamin, R. (2016). Informed refusal: Towards a justice-based bioethics. *Science, Technology, & Human Values,* 41(6), 967-990. doi:10.1177/0162243916656059

Browne, S. (2010). Digital epidermalization: Race, identity and biometrics. *Critical Sociology,* 36(1), 131-150. doi:10.1177/0896920509347144

Browne, S. (2015). *Dark Matters: On the Surveillance of Blackness*. Durham, NC: Duke University Press.

Coletta, C., Evans, L., Heaphy, L., & Kitchin, R. (2018). *Creating Smart Cities*. Abingdon, UK: Routledge.

Crenshaw, K. (1991). Mapping the margins: Intersectionality, identity politics, and violence against women of color. *Stanford Law Review*, 43(6), 1241-1299. doi:10.2307/1229039

Delhi Police. (2019). *Order No. 1872-1996/SO-ACP/Pt.Street/NDD*. Sub-Division of Parliament Street, Delhi: Delhi Police.

Dencik, L., Hintz, A., & Cable, J. (2016). Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data & Society*, 3(2), 1-12. doi:10.1177/2053951716679678

Dubrofsky, R. E., & Magnet, S. A. (eds.). (2015). *Feminist Surveillance Studies*. Durham, NC: Duke University Press.

Express News Service. (2019). 145 out of 192 police stations got CCTV cover. *The New Indian Express*, 10 Jan. http://www.newindianexpress.com/cities/delhi/2019/jan/10/145-police-stations-got-cctv-cover-1923216.html

Firmino, R., & Duarte, F. (2015). Private video monitoring of public spaces: The construction of new invisible territories. *Urban Studies*, 53(4), 741-754. doi:10.1177/0042098014567064

Fyfe, N. (2004). Zero tolerance, maximum surveillance? Deviance, difference and crime control in the late modern city. In L. Lees (ed.), *The Emancipatory City? Paradoxes and Possibilities* (pp. 40-56). London: Sage.

Gellman, B., & Adler-Bell, S. (2017). The disparate impact of surveillance, *The Century Foundation*, 21 Dec https://tcf.org/content/report/disparate-impact-surveillance/

Giddens, A. (1990). *The Consequences of Modernity*. Cambridge, UK: Polity Press.

Gilman, M. E., & Green, R. (2018). The surveillance gap: The harms of extreme privacy and data marginalization. *NYU Review of Law and Social Change*, 42(253).

Goswami, S. (2018). 1.4 lakh CCTV cameras in Delhi's markets, residential areas by October. *Hindustan Times*, 8 Feb. https://www.hindustantimes.com/delhi-news/1-4lakh-cctv-

cameras-in-delhi-s-markets-residential-areas-by-october/story-IXqbi0PoXuyu1YFVJJU4LN.html

Government of Delhi. (2018). *Delhi Rules for Regulation of CCTV Systems in NCT of Delhi*. Delhi: Government of Delhi. http://dceast.delhigovt.nic.in/wps/wcm/connect/b4db69004622dcdbb778b7c8da9eb17e/CCTV.pdf?MOD=AJPERES&lmod=1855201116&CACHEID=b4db69004622dcdbb778b7c8da9eb17e

Govindarajan, V. (2016). Should Delhi's (illegally) gated enclaves be thrown open to reduce traffic congestion? *Scroll.in*, 30 Jun. https://web.archive.org/web/20190708123735/https://scroll.in/article/809558/should-delhis-illegal-gated-enclaves-be-thrown-open-to-reduce-traffic-congestion

Hasija, S., & Nagpal, S. (2018). CCTV surveillance in public spaces of Delhi: Exploring the perspectives of youth visiting malls and Delhi Metro. *IOSR Journal of Humanities and Social Science*, 23(12), 2nd ser.

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

Hempel, L., & Töpfer, E. (2004). *Final Report: CCTV in Europe,* Working Paper no. 15. Berlin: Centre for Technology and Society, Technical University of Berlin. http://www.urbaneye.net/results/ue_wp15.pdf

Huey, L. (2010). False security or greater social inclusion? Exploring perceptions of CCTV use in public and private spaces accessed by the homeless. *The British Journal of Sociology,* 61(1), 63-82. doi:10.1111/j.1468-4446.2009.01302.x

Khan, S. (2018). *Punjab Government's Safe Cities Project, (Safer City) or Over Policing?* Lahore: Digital Rights Foundation. https://privacyinternational.org/news-analysis/2228/punjab-governments-safe-cities-project-safer-city-or-over-policing

Koskela, H. (2002). Video surveillance, gender, and the safety of public urban space: "Peeping Tom" goes high tech? *Urban Geography*, 23(3), 257-278. doi:10.2747/0272-3638.23.3.257

Kovacs, A. (2017). Reading surveillance through a gendered lens: Some theory. *Gender Surveillance*, February. https://genderingsurveillance.internetdemocracy.in/theory/

Lyon, D. (1994). *The Electronic Eye: The Rise of Surveillance Society*. Cambridge: Polity Press.

Lyon, D. (2001). *Surveillance Society. Monitoring Everyday Life*. Buckingham: Open University Press.

Lyon, D. (ed.). (2003). Introduction. In *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*. Abingdon, UK: Routledge.

McCahill, M. (2002). *The Surveillance Web: The Rise of Visual Surveillance in an English City*. Cullompton, UK: Willan Publishing.

Ministry of Women and Child Development. (n.d.). *Framework for Nirbhaya Fund*. New Delhi: Ministry of Women and Child Development. https://wcd.nic.in/sites/default/files/Approved%20framework%20for%20Nirbhaya%20Fund_0.pdf

Minnaar, A. (2012). Private security companies, neighbourhood watches and the use of CCTV surveillance in residential neighbourhoods: The case of Pretoria-East. *Acta Criminologica: South African Journal of Criminology*, Special Edition 1, 103-116.

Monahan, T. (2008). Dreams of control at a distance: Gender, surveillance, and social control. *Cultural Studies <-> Critical Methodologies*, 9(2), 286-305. doi:10.1177/1532708608321481

National Crime Records Bureau (NCRB). (n.d.). *Request for Proposal to Procure National Automated Facial Recognition System (AFRS)*. New Delhi: Ministry of Home Affairs. http://ncrb.gov.in/TENDERS/AFRS/RFP_NAFRS.pdf

Phadke, S., Khan, S., & Ranade, S. (2011). *Why Loiter?: Women and Risk on Mumbai Streets*. New Delhi: Penguin Books.

Press Trust of India (PTI). (2012). CCTV cameras removed from Puri beach after protests by women. *The New Indian Express*, 7 Dec. http://www.newindianexpress.com/states/odisha/2012/dec/07/cctv-cameras-removed-from-puri-beach-after-protests-by-women-431766.html

Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society*, 4(2), 1-14. doi:10.1177/2053951717736335

Thomasen, K. (2017). Beyond airspace safety: A feminist perspective on drone privacy regulation. *SSRN Electronic Journal*. doi:10.2139/ssrn.3143655

Walby, K. (2005). How closed-circuit television surveillance organizes the social: An institutional ethnography. *Canadian Journal of Sociology*, 30(2), 189-214. doi:10.2307/4146130

Weinberg, L. (2017). Rethinking privacy: A feminist approach to privacy rights after Snowden. *Westminster Papers in Culture and Communication*, 12(3), 5-20.

Wickramasinghe, M. (2014). *Feminist Research Methodology: Making Meanings of Meaning-Making.* New Delhi: Zubaan.

Wright, J., Glasbeek, A., & Meulen, E. V. (2014). Securing the home: Gender, CCTV and the hybridized space of apartment buildings. *Theoretical Criminology*, 19(1), 95-111. doi:10.1177/1362480614544210

Acknowledgements

The “Urban Data, Inequality and Justice in the Global South” case studies form part of a Senior Research Fellowship funded by the University of Manchester’s Sustainable Consumption Institute with additional financial support from Canada’s International Development Research Centre (IDRC). This case study was also partially funded by the “Big Data for Development Network”, established and supported by IDRC. More information about the network and work produced by it can be found here: http://bd4d.net/. The authors express their gratitude to Richard Heeks and Linnet Taylor for being extremely generous with their time in providing prompt and insightful feedback.

About the Authors

Aayush Rathi is a researcher at the Centre for Internet and Society, India. A lawyer by training, he produces interdisciplinary research at CIS working at the intersections of feminist theory, surveillance studies and labour.

Ambika Tandon is a researcher at the Centre for Internet and Society, India. She works at the intersection of gender and technology through interdisciplinary research on areas such as surveillance, reproductive health, and labour. Before CIS, she was pursuing a Master’s in Media, Communications and Development from the London School of Economics and Political Science.