PRE-PRINT

Sensing In/ Security

Sensors as transnational security infrastructures

MATTERING PRESS

Mattering Press is an academic-led Open Access publisher that operates on a not-for-profit basis as a UK registered charity. It is committed to developing new publishing models that can widen the constituency of academic knowledge and provide authors with significant levels of support and feedback. All books are available to download for free or to purchase as hard copies. More at matteringpress.org.

The Press' work has been supported by: Centre for Invention and Social Process (Goldsmiths, University of London), European Association for the Study of Science and Technology, Hybrid Publishing Lab, infostreams, Institute for Social Futures (Lancaster University), OpenAIRE, Open Humanities Press, and Tetragon, as well as many other institutions and individuals that have supported individual book projects, both financially and in kind.

PRE-PRINT EDITION

Sensing In/Security investigates how sensors and sensing practices enact regimes of security and insecurity – a topic that could not be more relevant in a time of a massive pandemic, ecological crises and ruthless policing practices. Coinciding with this year's EASST/4S meeting, Mattering Press is publishing this pre-print version of the preface, the introduction and two empirical chapters. The full edited collection will be published with Mattering Press in winter 2020. Please send an email to info@matteringpress.org to pre-order your copy, or if you want to review the final volume.

IMPRESSUM

Editors Nina Klimburg-Witjes, Nikolaus Poechhacker & Geoffrey C. Bowker

Mattering Press Editors Julien McHardy & Endre Dányi
Design Julien McHardy

Reviewers Huub Dijstelbloem & Lucy Suchman

Copy Editing Steven Lovatt

Pre-print edition published by Mattering Press, Manchester.

Freely available online at matteringpress.org/books/sensing-in-security

ISBN: 978-1-912729-05-0 (pdf)
DOI: doi.org/10.28938/9781912729050

Foreword

Writing this Foreword amidst daily news reports of the COVID-19 outbreak affords a very particular context for thinking about transnational security infrastructures. Events beginning in November of 2019 have made it abundantly clear that, under circumstances of pandemic disease, surveillance and control can be life saving resources. Yet while population monitoring as a defense against exceptional threats to public health seems at once newly relevant, it is also clearly insufficient without the political will and organisational effectiveness required for the mass mobilisation of both preparation and response. It is now clear, moreover, that the effects of pandemic disclose and amplify insecurities arising from more longstanding and systemic threats to planetary health and individual well being.

Sensing technologies are, arguably, a quintessential kind of human/machine hybridity. On one hand, like other infrastructural devices, sensor technologies must be designed to operate automatically so that once installed they run continuously. Sensing technologies reflexively constitute the world as the kinds of data that they can sense. In most instances, moreover, their sensory capacities are radically different than our own; their ability to register signals undetectable by the human sensorium is central to their value. On the other hand the significance of what is sensed, and in the service of whom, is an entirely human affair.

This rich and extensive collection of studies examines sensors and sensing at the intersections of critical security studies and science and technology studies. The trope of in/security signals the fact that insecurity and security are mutually constituted, and that states of one or the other do not objectively exist in any simple sense. Deployed in the name of securitization, sensing technologies are enrolled in particular technopolitical regimes and associated designations of what constitutes a threat and to whom. Working through the generative frame of infrastructure, these studies track the conditions of possibility that enable specific, technologically-enhanced sensoria of threat detection, and the worlds that they render legible and, as importantly, illegible. Far from seamless, their extent and redundancies nonetheless ensure remarkable degrees of continuity in operation. Notable for their scalability, electronic sensoria are engaged in processes ranging from rendering micro-organisms as genetic signatures, to monitoring whole-earth planetary transformations.

A crucial topic for these studies is the question of who feels threatened and who feels protected by regimes of surveillance, and how apparatuses deployed in the name of securitization are at the same time generative of insecurity, in the ways that they presume and figure a threat. Contemporary security infrastructures, we are reminded, are deeply indebted to their military and colonial histories, which set the terms for who is in a position to monitor and administer whom. We learn how very different the resulting effects (and affects) are if surveillance from the air is done in the name of protecting those on the ground, or for purposes of rendering them as targets. It matters as well what the relations are between those who are positioned as vulnerable (for example, the wealthy in the so-called war on crime), and those who are figured as the threat (for example, the 'unlawful combatant' in the war on terror). We learn as well about the work of fear (whether of burglary or of extrajudicial assassination), and the promise of protection to those that the apparatus figures as deserving. As vendors search for new markets, military technologies like the Predator B drone, developed for the identification of targets for attack abroad, are reimagined as a critical security infrastructure required to safeguard citizens at home.

Media accounts of technological developments typically conflate references to actually and already existing infrastructures and more speculative projects. Crucially, these conflations are performative, contributing to widespread acceptance of the fact that 'it's only a matter of time' before that imaginary is more than a prototypical reality. Too often discussions around the proliferation of embedded sensing share with discourses of technological progress the naturalization of sociotechnical developments. In the voice of the disinterested observer, the 'advance' of technology is described as if it were a kind of *force majeure*. The increasing presence of sensors in our built environments is not the result of an autonomously unfolding process, however, but rather of concerted actions on the part of those bodies (persons, agencies, corporations, states) invested in their proliferation. However large the investment, the proliferation is not inevitable.

The authors collected here ground their engagement with security infrastructures in empirical studies, which in turn make evident the political and practical contingencies that characterise actual projects. Countering discourses of seamless integration and linear development, these studies attend to the fragmented, boundary-constructing processes and very differentially distributed effects of infrastructuring. Transnational private/public partnerships carry discourses of the 'smart city,' promoting standardization under the sign of innovation. Technological solutions searching for their problems, the imaginaries and technological devices involved travel across sites (for example, the Israeli Skystar 180 aerostatic surveillance balloon travels via College Station, Texas, to become one of a suite of surveillance technologies adopted in Santiago, Chile; US multinationals set the stage for 'smart city' projects of India and South Africa.) While technophiles defend these investments, those on the front lines of their operation frequently express skepticism regarding their efficacy. Enacted within the layered historical/political/economic realities of the target territory, standardised visions are torqued and hybridized, furthering unequal distributions of access to resources. The smart city and the biometric border are conjoined through schemes for profiling and risk assessment. We hear as well about devices for the (partial) detection of (messy), noncoherent surveillance infrastructures, themselves parasitic on the military lineages of GPS. And we are treated to the graphic-novel arabesques of visual vignettes, offered as a counter-genre for infrastructural inversions of both surveillance infrastructures and the media for their tracking and analysis.

As infrastructural studies have taught us, sensing at once requires and enacts delineations of similarity and difference, sorting and classification. Seeing is always *seeing as*. Infrastructural inversion as method underscores the importance of attending both to the labours and politics of creating accountable relations between data and worlds, and that which escapes the data sensorium. For and by whom are infrastructures themselves rendered variously visible (for example, to those who build, maintain and operate them) and invisible (to those who are their subjects/objects)? What modes of knowledge and action live in the digital sensorium's blind spots and exceed its capacities of registration? What would it mean to re-engage the sensorium in deeper awareness of its politics? As the contributors to this collection suggest, new digital infrastructures rematerialise already existing social orderings, and are re/generative of dominant cultural, historical, political, and economic relations. At the same time, the configuration of sociotechnical infrastructures of in/security is always fragmented and open to contestation. Perhaps most importantly, then, we need to recover the partiality and contingency of surveillance technologies and their associated in/securities, in order to recognize the forms of life that escape them and the different possibilities for knowing and world-making that those lifeworlds both demand and enable.

Lucy Suchman
Saltspring Island, British Colombia

Sensing In/Security
An Introduction

Nina Klimburg-Witjes
Nikolaus Poechhacker
Geoffrey C. Bowker

> *There are more automated sensors perceiving our environment and the elements that constitute it than there are living human beings*
> *Tironi 2017: 2*

Almost anything and anyone can become a sensor, gathering and transmitting data about our world. Sensors are omnipresent and increasingly important elements in constituting and controlling contemporary societies in many domains of our lives. Built into ('smart') cities, communication devices, and our clothes, attached to our bodies, to drones, satellites and cars, sensors have become our mostly invisible companions. Invested with ideals such as 'invisible computing', the 'Internet of Things', 'global transparency' or 'algorithmic governance', 'these automatic electromechanical labourers, at the fringe of our awareness, control the world around us. At times, they even control us. Yet they are now so familiar, so mundane, that we hardly notice' (Townsend 2014: xi). In/security is one of the domains that we now find equipped, imagined and measured with sensors.

The contributions to this volume bring together science and technology studies (STS) and critical security studies (CSS) to examine in/security, sensors and sensing. By bringing these fields together, in this book we aim to extend longstanding STS concerns with infrastructuring to emergent modes of surveillance and securitisation enabled by sensing practices and digital infrastructures. We set out by exploring many by now classical STS issues such as monitoring, registering, representation and visualisation (Amoore 2009; Dijstelbloem and Broeders 2015; Vertesi 2014; Dumit 2003; Witjes and Olbrich 2017; Ruivenkamp and Rip 2014); issues of technological mediation and human/non-human networks (Callon and Muniesa 2005; Law 1994; Poechhacker and Nyckel 2020); infrastructures (Larkin 2013); the politics of knowledge and expertise (Ezrahi 2012; Shapin and Schaffer 2011); issues of classification and categorisation (Bowker and Star 2000; Star and Ruhleder 1996; Star 1998; Suchman 1994; Barry 2001); group formation and data politics (Edwards et al. 2011; McCosker and

Graham 2018; Ruppert 2011); as well as questions concerning the shaping of societies, states and technologies (Bijker and Law 1992; Jasanoff 2004; Felt 2015; Hecht 2009; Scott 2001; Mitchell 2011), with a particular view towards sensors as security infrastructures.

Most sensing activities operate in the background and do not require active or direct registration by those who are monitored (see Andrejevic and Burdon 2014). Sometimes, however, it is deliberately made obvious that we are being sensed or made sense of by devices. Questions about the in/visibility of sensors drive this book: how do sensors shape and how are they being shaped by the environment in which they are placed, and by the processes they (attempt to) render visible (see Frith 2019)? Sensors pick up some data and not others, depending on which data their designers consider relevant. Materially, sensors register only what they are designed to measure (Helmreich 2019). In the case of security-related sensors, sensors pick up data that their designers take to indicate a security threat. Sensor design and deployment in this way takes part in constructing and delineating the phenomena that are to be sensed and governed. Sensors actively produce data traces by enacting otherwise contingent realities. Acts of sensing reduce the multiplicity of potential ontologies to a singular reality that the specific sensing regime can register. This translation of reality excludes enactments and actors that escape the sensing regime, making sensing a political act (Law 2002; Callon 1986).

Our aim with this volume is to draw attention to the ways in which sensors are integrated into the environment and how they produce different forms of in/security through processes of exclusion and inclusion. STS and CSS alike have observed a shift of security regimes from 'evidenced-based identification and assessment of danger informed by a causal logic and reliant on empirical analysis' (Suchman, Follis, and Weber 2017: 2) towards a predictive and risk-based evaluation of potential threats (Amoore 2013). However, the notions of causal logic and empirical evidence have been problematised in STS and neighbouring fields for some time now as emergent qualities of a socio-technical arrangement. Processes of inclusion and exclusion thus produce security and insecurity alike: security as a performed and shared form of knowledge, insecurity as becoming the subject of security regimes. This distinction can then also be discussed along the lines of becoming visible for someone or becoming visible as someone. In each case, the production of sensory in/visibility creates a dialectical relation between security and insecurity.

A short sensory journey

To illustrate the abundance of sensors built into our everyday practices and experiences, let us take you on a brief journey through sensing infrastructures, each enacting and interacting with the surrounding environment in its own way. First, switch on your smartphone's augmented Global Positioning System (GPS). You are no longer alone, and you will no longer get lost, as you are now sensed by apps like Google Maps using a flock of satellites circling the Earth in a series of orbits designed to optimise coverage at any given moment. Each satellite contains an atomic clock, constantly emitting electromagnetic signals carrying an almanac of information about the position each satellite is supposed to be in. Your device uses these pieces of information to triangulate your position, thereby embedding you in a military-commercial geopolitical infrastructure of ground antennae and data centres with its own (post)colonial legacy (see Oldenziel 2011). While satellites might help you on your way, they also continuously observe, measure and monitor the Earth, sending images of nearby and distant sites. In terms of security, they are situated at the intersection of technologies of militarised intelligence and those of human rights, as both are used to reify security threats posed by adversarial countries or groups. For instance, commercial satellite imagery is increasingly used by non-state actors like human rights activists and think tanks as a tool to hold perpetrators accountable for human rights violations and mass atrocities. At the same time, government agencies are still powerful in determining what is visible and to whom (see Wang et al. 2013; Witjes and Olbrich 2017). Although seen by many as omnipresent surveillance technology from above (Parks 2005; Herrscher 2014; Shim 2016; Hong 2013), the satellite gaze can be hampered by cloud cover as well as by limited windows of observation due to geocentric orbits (Zirker 2013). However, within multi-modal sensing networks, if one sensor is hindered in its function, another is likely to take over.

We have now reached the coast, where wave buoys provide local measures that satellites – although they use scanning radar altimeters, scatterometers and synthetic aperture radar – cannot (Helmreich 2019: 5). The buoy, as Helmreich suggests, could 'be read as a symptom of how ocean politics have been enabled by national, military and corporate infrastructures of measure, with buoys looking like harmless bystanders even as they concretise real relations of territorial domination in ocean space' (2019: 5). Following anthropology underwater, we encounter multiple subaquatic sensor networks. Collaboratively, they monitor physical or environmental conditions such as pressure, sound, temperature and so on, and transmit data to the underwater node. The data are transmitted to a surface buoy via a wired link, and eventually received at an onshore or surface sink via radio communication, thus enabling computation to become environmental (Gabrys 2016) and the environment to become computational (Helmreich 2019). This computation environment can be utilised in many scenarios, from environmental monitoring and deep-sea exploration to flood and tsunami alerts, from navigation and communication to underwater warfare (see Starosielski 2015; Oreskes 2003; Mort 2002).

From here, we travel to the airport, a site where sensors and security-related sensory networks condense, sensing our bodies, belongings and biometrics in multiple ways. At the check-in counter, we are asked to show our passports with now mandatory biometric fingerprint data, detected by a tiny scanner that governs both the mobility and enclosure of bodies (Amoore 2016), turning surveillance into a form of 'social sorting' (Lyon 2003a, 2003b; Leese 2016; Cunningham and Heyman 2004). At the smart border, we will have to hand over our phones to the border guard. Now, we are likely to go through the procedure of body scanning – which, shortly after its introduction, was re-labelled 'security scanning', thus distracting our attention from the vulnerability of human bodies rendered visible with the promise of increased security (Bellanova and Fuster 2013). These security devices 'illuminate the body with short-wavelength radio waves […] and form an image from the reflected radio waves […] to create a two-dimensional image of the body' (European Commission 2010: 8) that differentiates between metallic and non-metallic objects.

This journey has illustrated some of the many instances where sensing devices are employed in the name of security: from satellites to underwater networks, biometric scanners and radars. As with so many sensing technologies that were first developed for the military (see also the chapter on 'Drones as political machines' by Ciara Bracken-Roche, this volume), what is being sensed and how we are subjected to different sensing regimes is ambivalent, to say the least, as are the meaning and the consequences; seeing (like) a drone means something different if you are in a suburban house in the USA or a village in Pakistan (see Gusterson 2017).

No matter where we go, stories about sensors as actors in techno-societies are complicated, multiple and political. Not surprisingly, then, sensors have come to the foreground in contemporary academic and policy debates about the relations between data, security and politics. Some authors have even postulated that we live in a 'sensor society that is constituted by the devices we use to work, communicate and play with, and which double as probes capturing the daily lives of people, things, environments, and their interactions' (Schermer 2008, cited in Andrejevic and Burdon 2014: 6). In STS research, sensors are not new objects: whether in the assembling of controlled experimental setups, the design and implementation of 'large technical systems' (Hughes 1987; Summerton 1994) or the production of novel measuring instruments (Gramaglia and Mélard 2019; Gabrys 2016), sensors have been widely studied as 'lively' devices that detect, inscribe, capture and record, even if they do not always do so explicitly as 'sensors' (Waller and Witjes 2017; Gabrys 2009, 2019; Gabrys and Pritchart 2018; Helmreich 2019; Suchman, Follis, and Weber 2017; Edwards 2004; Walford 2017; Spencer et al. 2019).

Sensor practices – Practising sensing

In a technical sense, sensors are devices that capture and record data which are then transmitted, stored, analysed and linked to other data sets. Oscillating between civilian, police and military domains, sensors are inscription devices (Latour and Woolgar 1986). Inscription devices were originally conceptualised in science studies as crucial elements of laboratory equipment that '[transform] pieces of matter into written documents' (Latour and Woolgar 1986: 51), thus creating a reference to the reality in question. Sensors, however, often are no longer part of a confined laboratory space, but are crucial elements in the 'production of security in "laboratory" conditions' (Amicelle et al. 2015: 299). As such, sensors enable new forms of interacting with the world at a distance through socio-technical infrastructures mediating between actors across space (Latour 1999). In short, sensing infrastructures include not only mechanical sensing but also a delicate interplay between humans, artefacts and discourses (Gabrys and Pritchard 2018). As much work on knowledge infrastructures in STS and beyond has shown, conceptualising raw data as neutral and objective is a bad idea (Bowker 2008; Gitelman 2013). Because data are always processed and subject to infrastructures, sensors not only produce 'raw data' but also often, as we argued above, problematise the relation between epistemic practices and their environment (Waller and Witjes 2017).

This volume aims to explore some of the complex and often invisible political, cultural and ethical processes that contribute to the development of sensors and their data infrastructures (see Bowker et al. 2010; Edwards 2010; Star 1999). By doing so, it shows how sensors reduce complexity and selectively produce a version of the world measured. In this way, the power of sensor networks not only 'work[s] through the sensory capacity of artifacts' (Kim 2016: 400), but through the embeddedness of sensory capacity in a broader socio-technical network. While making sensing activities possible in the first place, this embeddedness allows for the sense-making of multiple data traces produced through sensing practices by collecting and combining them in what Latour (1987) called centres of calculation. Sensing traces are thereby not just collected in one centre of calculation – keeping the chains of translations stable – but are collected, compared and calculated in multiple centres, where their meaning is reinterpreted and re-stabilised (see e.g. Egbert 2019).

The sensors discussed in this volume perceive the world like a security regime, producing probabilities and possibilities alike (Amoore 2013). Monitoring and measuring people, processes and practices, sensors are framed as a means to increase security by diminishing uncertainty and enabling action against perceived, known and unknown threats and risks. Sensors – as infrastructural actors – thus produce, standardise and enact a certain notion of security. They transform diffuse ideas of a dangerous and threatening world into an experienceable and graspable entity; we might say that they perform ontological politics (Mol 1999). Yet the visibility that is produced through the sensors also creates invisibilities, depending on who gets included in or excluded from the broader sensing regime. Sensors are becoming part of a knowledge/power configuration that is built on the distinction of in/visibility (Foucault 1979, 1991). In this sense, new sensory infrastructures re-materialise already existing social orders, and are re/generative of dominant cultural, historical, political and economic relations. Sensors are shaping what type of 'politics take hold along with these technologies' (Gabrys 2016: 18), as novel modes of data gathering lead to 'new configurations of engagement, relationality, sensing, and action' (Gabrys 2016: 23). For the realm of security this means that novel forms of sensing might not only inform security politics and practices, but enable novel understandings of what security is and ought to be in a specific context: while each sensor is tasked to transmit data that are thought to be relevant for security purposes, the processes of measuring and monitoring render certain issues visible that might have been hidden before, thus co-constructing novel or previously unexpected security issues. Often, the enactment of security rests on prediction through algorithmic means (Suchman et al. 2018). In what Mackenzie (2015) called the production of prediction, machine learning systems and similar applications enact the world so that they can sort, reorder and find patterns (see Schüll 2014). As such, the method of machine learning builds practices that resolve the inherent indexicality of data usage in algorithms, consequently connecting the abstract formulations of computer code to an experienced world (Ziewitz 2017).

Thinking security through and with sensors

To approach security as a social practice of sensing embedded in broader socio-political contexts, critical security studies (CSS) can provide valuable insights into how security is thought and enacted in different settings, and how it continuously involves constructions of insecurity (Aradau and Van Munster 2008; Buzan et al. 1998; c.a.s.e. collective 2006; Huysmans 2000). Work in this field has done much to show that security fears are not 'out there' to be discovered, but are constructed in the process of securitisation (Buzan et al. 1998). Security is here understood as a discourse of power that can be invoked to frame a particular object or subject as a vital threat to society, the state or public order. This has broader political effects and legitimises the use of extraordinary measures to tackle the perceived threat. This call to engage with the practices enacted in the name of managing risk and uncertainty is also met by Amoore's work on the politics of possibility. Not accepting discourses of a global risk society (Beck 1992) in which we are entering an age of uncertainty, she argues that it is not so much a question of whether or how the world is more dangerous but how specific representations of risk, uncertainty, danger and security are distinctively writing the contours of the world (Amoore 2013: 7). The figure becomes the ground. Security as predictive technoscience, as Suchman et al. (2018: 2) have elaborated, rests on an 'apparatus of distinction' (Perugini and Gordon 2017: 2) that turns the suspect/enemy into an anticipatory target with the help of information based on real-time tracking, data mining and the imagination of an omnipotent sensorium (see Latour and Hermant 2006).

To study security critically thus requires a focus on practices and the modes of governing they shape and promote (Amicelle et al. 2015; Huysmans 2006). Recent work in CSS, that is sometimes linked to the 'material turn' of the field, has shifted the focus from discourse to technologies and materialities, and from conceiving 'security' in terms of performative constructions to highlighting its implication in networks and associations. In this line of work the 'technologization' of security (Ceyhan 2008) and the logics and rationale that are undergirding security practices has received increased attention (see Amichelle et al. 2015: 295). This shared interest in the materiality and ontology of security issues and the mutual influences of technological devices and security practices is precisely what has spurred an inspiring and engaged conversation between STS and CSS (see Valkenburg and van der Ploeg 2015; Bellanova and Duez 2012; Jeandesboz 2016; Schouten 2014; Olbrich and Witjes 2017; Leese 2016).

As a contribution to this exchange, this volume is a joint effort of scholars at the intersection of STS and CSS to come to terms with the messy and complicated properties of sensors as important and powerful elements of security infrastructures[1]. The following chapters can be read as attempts to make the processes and practices of sensing in/security visible. Engaging with the multiple entanglements of sensing practices, data infrastructures and in/security in different parts of the world, they empirically explore the contingencies of sensory knowledge, the standardisation process of security infrastructures and transgressions of boundaries between civilian and military spheres. They address the question of how sensors shape, shift and constitute domains of national and international security policy, and hence explore the role of sensor infrastructures in the constitution of and mediation between state and non-state actors.

Coming from various academic lineages, the authors in this volume speak to these themes from multiple perspectives using a variety of case studies from diverse regions. In jointly presenting their views on sensing security, the authors seek to illuminate some of the shared concerns from different fields about surveillance, control, social sorting, border practices and social exclusion, and envisioned security futures as enabling and enabled by sensing infrastructures.

Making sense of sensing in/security: Introducing the chapters

The issue of in/visibility is particularly relevant in the chapters that explore the ways in which sensors and their data infrastructures are either deliberately kept out of sight – whether physically hidden underground or in remote areas, or hidden from attention behind technical terms – or powerfully deployed to create climates of in/security among those being or assuming to be sensed. Martin Tironi and Matthias Valderrama's fascinating account of aerial surveillance in Chile addresses the latter. Over the past ten years, a climate of fear and insecurity has developed in Chile, a feeling that is widespread in Las Condes, one of the country's wealthiest municipalities. Inspired by the techno-imaginary of 'smart cities', the local government has introduced a series of 'innovative' and 'dynamic' surveillance technologies as part of its efforts to manage and secure urban spaces and wage 'war on crime'. However, residents and local organisations have protested against the use of these technologies, citing profound over-surveillance and raising important questions about the use of such security devices. The authors show how the skies over modern cities are increasingly occupied by new monitoring and datafication devices.

[1] Within STS and related fields, approaches like ANT or new materialism make the case that the distinction between singular objects and a broader structure of which they are part, i.e. being something or being part of something is not a pre-given quality of the actors involved but emerges out of the situated enactment – including the seemingly innocent observer (Barad 2007; Latour 1996; Mol 2002).

Drawing on qualitative interviews and participant observation, Tironi and Valderrama propose that vertical surveillance capacities must be analysed not only in terms of the surveillance and control they generate but also the affective atmospheres that they deploy in urban space and the ways in which these atmospheres are activated or resisted by residents. Reflecting on aerial sensing technologies, they show how these open up an affective mode of governance by air in an effort to establish atmospheres or microclimates in which one experiences (un)expected sensations such as safety, disgust or indifference. The air, they argue, emerges as an ambience that must be controlled and securitised by the use of aerial sensors and technologies that generate a vertical distancing between control rooms and the experiences of entities that coexist with/under the aerial gaze of such technologies of sensing in/security (see Adey 2010; Graham and Hewitt 2013; Klauser 2010; Weizman 2002).

Sensing infrastructures are increasingly disseminating and performing across the urban space techniques that are specific to borders, and especially to 'smart' borders, such as algorithmic profiling, biometrics recognition, scanning and screening. Drawing on fieldwork conducted in New Town Kolkata in India, Ilia Antenucci explores how, in contrast to popular narratives of smart cities as seamless interconnected spaces, the processes of urban digitisation entail bordering practices that work through the sensing networks and devices that are becoming more and more embedded in everyday life – bus shelters, water and electricity meters, garbage bins, home automation, apps and so on. She discusses the political effects of ubiquitous sensing networks from two perspectives. First, it is suggested that sensing infrastructures introduce a new distribution of the sensible (Rancière 2000), setting boundaries between the different aspects of reality and perception, and measuring them incessantly; in this sense, the border operates at an ontological and epistemic level. Second, the chapter goes beyond the paradigm of surveillance/dataveillance to look at the nexus between algorithmic modelling, preemption and security decisions (Amoore 2013; De Goede et al. 2014) in the government of digital cities. This chapter contributes to an understanding of algorithms as creating new regimes of visibility and worth that are politically charged.

This chapter contributes to an understanding of algorithms as creating new regimes of visibility and worth that are politically charged. At the same time, a new regime of invisibility is created, in which the code strings and operative systems that process urban data remain largely inaccessible not only to citizens but also to the city agencies that are expected to act upon data. In the following vignette, Alex Taylor and Julia Velkova show how data centres facilitate and make possible the work of sensing media, the tracking and collection of data and the production of metric cultures while remaining curiously absent in discussions of digital security infrastructures. Their chapter introduces readers to the sterile technological spaces where sensor data are secured. As a critical intervention in recent scholarship on data centres that sees them as striving to remain invisible (see Holt and Vonderau 2015: 75), Taylor and Velkova draw on empirical work inside the buildings that store the vast volumes of sensor data now produced on a daily basis. They show how data are persistently imagined in terms of 'flows', like a constantly moving and circulatory form that never stays still – an imaginary that overlooks data's situatedness and the static sites of digital information storage and accumulation where different technologies of sensing – human, mechanical and digital – intersect. Following Taylor and Velkova into the data centre, we understand how these centres are not just enablers of new sensor-based security regimes, but also the sensory mirrors of the quantified, metrified societies that they infrastructurally help to produce.

These chapters are in conversation with the two visual vignettes that invite the observer to explore cities' hidden, invisible and secretive sensing infrastructures. The visual vignettes in this volume are a method by which sensing technologies can be differently seen, accessed and understood, both by analysts and by those with whom we as scholars might wish to share our work. Making visual vignettes for sensor stories brings novel forms of research communication into conversation with novel forms of sensing. Finding ways to communicate about our wired and wireless world is a task of demonstrating the mutual co-constitution of security and insecurity.

The first vignette, by Evan Light, Fenwick Mackelvey and Simon Hackbarth, explores how International Mobile Subscriber Identity (IMSI) catchers, commonly known as Stingrays, allow users to determine which cellphones are being used in a given location, to intercept phone calls, text messages and internet traffic, and to send fake text messages. The past ten years, the authors argue, have seen a rise in the use of IMSI catchers by police departments, intelligence agencies and any number of non-state actors to monitor cellphones. More recently, both commercial and non-commercial systems and products have emerged that aim to detect the use of IMSI catchers – so-called IMSI catcher catchers. IMSI catchers repurpose mobile telephone infrastructure as a surveillance device. Rather than embedding surveillance in mobile standards, IMSI catchers are technically a hack, collecting data not meant to be technically shared by our phones with anybody but a legitimate network provider. Drawing on the concept of infrastructural parasitism (Gehl and McKelvey 2019), the authors approach IMSI catchers as a parasitic surveillance device wherein the vulnerabilities and weaknesses in infrastructure might entice intelligence agencies and others. They argue that infrastructural weaknesses become opportunities for spying and surveillance as IMSI catchers feed on vulnerabilities in wireless code just as the Edward Snowden disclosures revealed how the 5 Eyes exploited vulnerabilities and the interconnection points of the global internet (see Musiani 2015). Rather than seeing infrastructure as one coherent system, such parasitism invites consideration of infrastructure as a plurality of technical projects that coexist with each other in a parasitic chain (see Serres 1980). Inspired by Anna Tsing's work on the matsutake mushrooms and their pickers that prototypes a landscape story which 'requires getting to know the inhabitants, human and not human', they look for IMSI catchers within this urban environment as transient objects that can only be discovered by getting to know their enabling environment and human contact points.

Chris Wood then invites us to walk with satellites and explore the meanings held within the GPS satellite network (typically hidden behind the hegemony of user interfaces). He contends that rather than being concentrated in the ways an individual interacts with technical objects and interfaces, an experience of space is supported by the multiple human and non-human objects which form GPS infrastructures. Wood uses walking workshops which leverage GPS diagnostic tools to speculate on themes and phenomenologies across such networks. In doing so, this visual vignette brings our attention back to the infrastructure by leveraging architecture to create an experience where GPS fails, thereby inspiring reflection on how meaning emerges across the entire network, rather than being concentrated in the hands of the user. To make GPS infrastructure visible, Wood chooses architectural sites that have the potential to disrupt its usually smooth operation, such as spaces with limited lines of sight with the sky (e.g. narrow streets or building complexes with covered walkways and underpasses). During the walk, each person was given an android smartphone running an app which reverse-engineers the process of locating to show participants where the satellites are in relation to them. After walking around the site individually for some time, the attendees reconvened and drew and wrote responses to the experience around perceptions of infrastructure and surveillance. By gaining insights into how a hidden but essential technology operates, Wood suggests we are enabled to reflect on that technology's implications.

The chapters by Francis Lee and Erik Aarden both examine the different enactments of health security and the legitimisation of political actions on the grounds of contingent knowledge production, focusing respectively on the theme of sensor-based knowledge and related processes of infrastructuring. : This basis for legitimisation is not new in STS or critical security studies, but it deserves special attention when it comes to the analysis of security regimes. In the ongoing COVID-19 crisis, these two chapters are even timelier than we hoped they would be. Drawing from post-ANT sensitivities and fieldwork at the European CDC (ECDC), Lee discusses how different practices of sensing and making sense of the world have been used to argue for the distribution of responsibility in the case of a salmonella outbreak. By utilising the method of genetic sequencing and finding genetic similarities between geographically distributed mutations of the bacteria, the team at the ECDC concluded that the disease had its origin in a specific country. Yet this mode of sensing has been contested on the grounds of another sensing practice that follows the bacterium through transport routes and logistical infrastructure. Applying what Lee calls shoe-leather epidemiology, the opposition argued that there is no identifiable causal link connecting the outbreak and the country. Thus different sensing practices and infrastructures have been applied to support different political claims in global health security regimes.

Similarly, Aarden uses the case of the Million Death Study (MDS) in India to show how human sensors are deployed and sensitised in order to create new forms of national health statistics. This new form of infrastructuring, he argues, brings into opposition two distinct matters of concern within the existing health security regime: first, the increasingly prevalent discourse on global health security, with its focus on 'exceptional events that may be anticipated with jointly developed digital sensing methods'

(Aarden, this volume). This marks an interesting shift in governance practices, as it means a transition from classical biopolitical governance towards the effort to prepare for singular and unpredictable events (Collier and Lakoff 2008). Thus the MDS marks an attempt to contest a security regime that is built towards a 'politics of possibility' (Amoore 2013). Second, the MDS applies a distinct form of sensing in opposition to the established clinical system. Combining interviewer skills for what the study calls 'verbal autopsies' with standards for interpretation and machine learning applications, MDS is hoped to 'access data on causes of death closer to the source and interpret that data more accurately' (Aarden, this volume). In this context, 'more accurately' also means overcoming the bias towards urban regions inherent to the clinical system. MDS sensing infrastructure contests not only the way of sensing but also what is managed within the health security regime, highlighting health issues of the rural households and those of low socioeconomic status.

In the cases of the ECDC and the Million Death Study, the different sensing infrastructures are becoming each other's brick wall and object of demolition (see Star 2002: 116). Providing different enactments as socio-political arguments for or against something, the focus shifts to the interplay of these diverse assemblages as infrastructures of contestation, where different enactments must be managed through negotiations (Mol 2002). Sensing infrastructures not only sense a specific world but also make sense of a socio-political arrangement.

Discursive visions and perceptions of the world, entangled with the usage of technologies, are equally important to understanding the way social orders are established. Visions of an (un-)foreseeable future often drive the reordering of security regimes, as Jutta Weber explores in her essay on wild cards as challenging traditional security doctrines. By focusing on highly unlikely, but potentially devastating events, a shift of orientation towards risky futures becomes the new mode of ordering in regard to thinkable interventions – also reflected in national security programmes. In this situation another boundary is renegotiated: the way the (vision of a) future influences contemporary security orders. 'Thinking the unthinkable' creates future risks that call for action in the present. This dystopic performance of a potential future as a mode of establishing a social order has been reflected in STS research for some time now (Jasanoff and Kim 2009). With her contribution, Weber points at a specific form of reordering the present – not only by probable or possible events but also highly unlikely ones through the description of these wild cards. Sensing and making sense of the future and the present, in this case, works in a fundamentally different way to algorithmic or calculative forms of knowledge production, challenging our assumptions of what a sensor is and can be. Enacting security risks through wild cards goes beyond the notion of probability and realises non-calculative politics of possibility (Amoore 2009).

This question of how the future is being made sense of through sensors is also one that drives the visual vignette by Katja Mayer and Eblis ibn Shah. They explore the notion of human sensors and an interesting genealogy of prediction within security domains, based on the practice of consulting occult seers during the Cold War to create predictions in a politically tense and potentially unforeseeable situation. Prediction, aside from risk calculation, became a fascinating element of security order, as Mayer and ibn Shah argue. The ways in which they provocatively put the spiritual human and an alternative construction of the future and security side by side questions the dominance and the apparent objectivity of predictions, thereby creating a space to reflect on often implicit assumptions about practices of future-taming and future-making.

In their chapter 'Visual vignette as a format', Mascha Gugganig and Rachel Douglas-Jones situate vignettes within the shifting grounds of STS's knowledge infrastructures and discuss its affordances for work in STS. While their project originates in the anthropological embrace of multimodal, imaginative work (Collins, Durrington, and Gill 2017; Elliott and Culhane 2017), the authors put their experimental engagements with analysis and communication of research into conversation with the efforts to work across media that have also been gaining prominence in STS (Ballestero and Winthereik, forthcoming; Dumit 2017; Jungnickel 2020; Le Bot and Noel 2016). Gugganig and Douglas-Jones then review the capacities of the Sensing In/Securities visual vignettes to bring forward critical aspects of our sociotechnical world, and offer a guide for those who might be inspired to experiment with the format and its potentials of working with images alongside text, and to stay with the dissonance produced when a conventional tool (PowerPoint) is pressed into alternative, imaginative use.

The third major theme of this volume, sensors as boundary infrastructures and bordering practices, is addressed by Annalisa Pelizza and Wouter Van Rossem, who take up the question of reordering security and its boundary infrastructures by focusing on a network of migration hotspots. In this fascinating account, the authors combine empirical insights and a textual experiment to explore how 'architectures of sensor networks and trans-national security orders' can influence each other. First, the hotspots are what the authors call nodes of equivalence, where standards and procedures are homogenised, creating a space of comparability that connects diverse national and transnational actors. Second, new forms of boundaries of responsibilities are drawn, and new forms of labour divisions between sensors at the periphery (i.e. migration hotspots) and centres of calculation are established. The double movement of renegotiating borders within the system of border security infrastructures and, at the same time, the blurring of boundaries between national security regimes shows the potential impact of sensor networks on social order(s).

In her chapter, Ciara Bracken-Roche contributes to the discussion of sensors and the renegotiation of boundaries and borders by showing how drones do not obey traditional bounds of state and security. The transgression of traditional boundaries between different spatial and political spaces is the result of the economic interests of industrial actors. Drones, as sensing devices, transitioned from the military domain into the realm of civic applications, performing a securitisation of risk and publics through technologies constructed for military needs. Bracken-Roche argues that domestic drones are commonly framed by industry groups as benign sensing technologies as compared to militarised drones, while at the same time security professionals deploy particular narratives about drones to suit economic and political agendas. The chapter highlights how drones in Canada, in both civilian and military applications, represent a technological zone (Barry 2001, 2006) and how these sensing machines dramatically shape public spaces and impact individuals across various contexts.

Aiming towards an at least temporary demolition of disciplinary borders, the experimental chapter by Jan-Hendrik Passoth, Geoffrey C. Bowker, Nina Klimburg-Witjes and Godert Jan van Manen addresses questions of, and experiments with, possible forms of engagement between social science, hacking and security policy through a conversation on 'Infrastructres, Security and Care' over the course of two years. Their aim is (at least) twofold. First, they explore novel ways of listening to, and discussing and engaging with people who are experts on sensors outside academia – yet explicitly not in a sense of extracting knowledge and information, which almost always creates the risk of patronising or exploiting the 'expert engineer', but instead as a form of mutual exchange of perspectives, questions and issues. Second, the contribution is an experiment with novel formats, looking for ways to integrate these engagements into an academic, edited volume while being sensible to the different work logics as well as the different disciplinary logics of crediting (academic) work and the challenges that bear on traditional processes of academic peer-review.

The (supposed) invisibility of sensors and sensing infrastructures in the making of security issues and politics has provoked us to engage with the issue of representation in research and the form, normativity and power of written words in more experimental ways. The three visual vignettes in this book all aim at breaking up the 'division of labor' of text as content and image as its illustrator as they engage the reader/viewer to critically reflect and rethink the dialectic between visuals and text. The genre of visual vignettes considers research, data analysis and dissemination tools as methodological infrastructure. It challenges us to reconsider the norms of common research, writing and communication practices that have defined STS, often borrowed and adapted from neighbouring disciplines. Methodological infrastructures, like all infrastructures, are made and remade, leak and break and get fixed and repurposed. As such, this format allows us to make sense of sensors by creating new forms of visibility and tangibility, reflecting the multi-modal data that sensors capture, transmit and are part of.

Conclusion

Sensors and sensing infrastructures are neither neutral nor innocent but imbricated with politics at all levels, from international migration to sensing genetic evidence for disease outbreaks, from biometric to aerial surveillance, from huge data centres to satellites and tiny cellphone sensors eavesdropping on our conversations. Sensors often do invisible work, while simultaneously making (perceived) threats experienceable. We might thus say that where there are sensors, there is also governance. But then, where are the control rooms, and how are agencies arranged between people, things and politics in sensing security infrastructures? Building on and linking work from science and technology studies, security studies, critical data studies, sociology and anthropology, this edited volume tackles these questions as it seeks to understand the role of sensors in the making of transnational security infrastructures. Sensors contribute to the production of in/security in manifold ways, producing in/visibilities and modes of in- and exclusion. Sensing realties raises questions of what is being sensed in which way, and visible to whom. Sensing therefore draws boundaries on different levels, sorting actors into sensed populations, regulating access to sense-making tools or producing discipline through the visibility of sensing processes. The relation between in/visibility and in/security is hence not always straightforward. In/securities are the result of in- and exclusion processes of at least three different dimensions, which are reflected in the content and form of this book: in/visibility of sensing, sensing as knowledge production, and the construction of (new) borders.

First, *the in/visibility of sensing devices and possible processes of infrastructural inversion*. Here we bring together work in STS on the (in)visibility of infrastructures with studies interested in security and surveillance. Research in STS and adjacent fields on the nexus of visualisation and materiality has continuously engaged with questions of how 'things are made visible' and 'which things are made visible', and investigates 'the politics of visible objects' (Kuchinskaya 2014; Rose and Tolia-Kelly 2012: 4). The emergence of sensors is connected to the social orders they co-constitute. Yet STS has not only illuminated the tendencies of infrastructures to fade into the background, but also shown that there is movement, a process, in which some (parts of) infrastructures become visible and move to the foreground whereas other infrastructures or their parts become invisible. Thus it is important to ask when we make these infrastructures of sensing visible and to what end. Sensors tend to become invisible or so much part of our daily life that the enactment of in/security only becomes visible to certain stakeholders, while others are only included as objects of enquiry, but excluded from the sensor data-informed security discourse. Visibility thus becomes not an effect but an issue, as surveillance 'has become increasingly unaccountable and less and less visible to ordinary people' (Lyon 2015).

Second, the collection contributes to work *interested in the social construction of sensor-based knowledge and related processes of infrastructuring*. As Star (2002: 116) put it: 'One person's infrastructure is another's brick wall, or in some cases, one person's brick wall is another's object of demolition'. Through different sensing practices, different versions of the sensed world are created, including or excluding issues, people, sensations and geographical places, creating the basis for different argumentations and rationales. As such, sensing infrastructures are always political, as they enact varying matters of concern (Latour 1999). Taking up this observation, the contributions to this volume exemplify how different ways of sensing become the basis for making or contesting political arguments on security issues. This dynamic is illustrated by health infrastructures and the question of sensing health incidents. The impact of sensors can – at the moment of writing this chapter – be observed live in the tracking of the pandemic of COVID-19. Political and health care systems have a tremendous impact on how the tests are distributed and how the distribution of the virus is made visible.

Lastly, the book engages with *sensors as boundary infrastructures and bordering practices*. Information streams and communication structures are often integral elements of the way a state or other big institutional setting is organised (Mukerji 2011). Sensor infrastructures are no exception. They play an important role in the production of political entities, social orders and manifold boundaries by moments of performative integration of actors. This integration – and with it also always moments of exclusion – can be explored from at least two different perspectives. Starting from the idea of infrastructuring (Pipek et al. 2017), the spread of trans/national networks defines moments of connectability and the forms of possible interactions between different elements within these networks. Are you using the same protocols, the same standards (Bowker and Star 1999), and is the distribution of tasks compatible with broader systemic practices? With the production of transnational sensor infrastructures, national boundaries seem to be pierced and weakened while other boundaries are produced.

This collection contributes to a growing literature on the diverse processes of both securitisation and normalisation as integral to these infrastructures, along with their performativity in the making of boundaries and borders. Instead of solely focusing on specific sensory devices and their consequences, the book engages with the emergence of sensing infrastructures and networks, and how sensing devices become invested with socio-political significance. By paying attention to sensors as an important part of the material equipment of security practices, this collection unpacks sensing as situated practices of constructing, reconfiguring, stabilising and disrupting in/security. As such, it encourages us to be both critical and hopeful that networks of in/security can withstand drives to build all-encompassing surveillance regimes. There are always modes of contingency and practice which exceed the panopticon – which is necessarily always incomplete, but whose power is multiplied by the belief that it is all-encompassing. Securing our futures entails living joyfully with insecurity.

References

Adey, P. (2010). Vertical security in the megacity: legibility, mobility and aerial politics. *Theory, Culture & Society*, 27(6), 51–67.

Amicelle, A., Aradau, C., & Jeandesboz, J. (2015). Questioning security devices: Performativity, resistance, politics. *Security Dialogue*, 46(4), 293–306.

Amoore, L. (2006). Biometric borders: Governing mobilities in the war on terror. *Political Geography*, 25(3), 336–351.

Amoore, L. (2008). *Risk and the War on Terror*. (London; New York: Routledge).

Amoore, L. (2009). Lines of sight: on the visualization of unknown futures. *Citizenship Studies* 13(1): 17–30.

Amoore, L. (2011). Data derivatives: On the emergence of a security risk calculus for our times. *Theory, Culture & Society*, 28(6), 24–43.

Amoore, L. (2013). *The Politics of Possibility: Risk and Security Beyond Probability*. (Durham, NC: Duke University Press).

Andrejevic, M., & Burdon, M. (2015). Defining the sensor society. *Television & New Media*, 16(1), 19–36.

Aradau, C. (2010). Security that matters: Critical infrastructure and objects of protection. *Security Dialogue*, 41(5), 491–514.

Armstrong, D. (2019). The social life of data points: Antecedents of digital technologies. *Social Studies of Science*, 49(1), 102–117.

Barad, K. (2007). *Meeting the Universe Halfway: Quantum Physics and the Entanglement of Matter and Meaning.* (Durham, NC: Duke University Press).

Barry, A. (2001). *Political Machines: Governing a Technological Society*. (London; New York: Bloomsbury Academic).

Barry, A. (2006). Technological zones. *European Journal of Social Theory*, 9(2), 239–253.

Bates, J., Lin, Y.-W., & Goodale, P. (2016). Data journeys: Capturing the socio-material constitution of data objects and flows. *Big Data & Society*, 3(2), 1–12.

Beck, U. (1992). *Risk Society: Towards a New Modernity*. (SAGE Publications).

Belcher, O. (2019). Sensing, territory, population: Computation, embodied sensors, and hamlet control in the Vietnam War. *Security Dialogue*, 50(5), 416–436.

Bellanova, R., & Fuster, G. G. (2013). Politics of disappearance: Scanners and (unobserved) bodies as mediators of security practices. *International Political Sociology*, 7(2), 188–209.

Bijker, W. E., Carlson, W. B., & Edwards, P. N. (1997). *The Closed World: Computers and the Politics of Discourse in Cold War America*. (Cambridge, MA: The MIT Press).

Bijker, W. E., & Law, J. (1992). *Shaping technology/building society: Studies in sociotechnical change.* (Cambridge, MA: The MIT Press).

Bowker, G. C. (2014). Big data, big questions| The theory/data thing. *International Journal of Communication*, 8(2043), 5.

Bowker, G. C., Baker, K., Millerand, F., & Ribes, D. (2010). Toward information infrastructure studies: Ways of knowing in a networked environment, in J. Hunsinger, L. Klastrup, & M. Allen, eds, *International Handbook of Internet Research Springer* (Dordrecht: Springer), pp. 97–117.

Bowker, G. C., & Star, S. L. (2000). *Sorting Things Out: Classification and its Consequences*. (Cambridge, MA: The MIT Press).

Broeders, D., & Hampshire, J. (2013). Dreaming of seamless borders: ICTs and the pre-emptive governance of mobility in Europe. *Journal of Ethnic and Migration Studies*, 39(8), 1201–1218.

Callon, M. (1986). The sociology of an actor-network: The case of the electric vehicle, in Callon, J. Law, & A. Rip, eds, *Mapping the Dynamics of Science and Technology: Sociology of Science in the Real World* (Basingstoke: Palgrave Macmillan UK), pp. 19–34. Callon, M. (1991). Techno-economic networks and irreversibility, in J. Law, ed., *A Sociology of Monsters: Essays on Power, Technology and Domination* (London: Routledge), pp. 132–161.

Callon, M., & Law, J. (1989). On the construction of sociotechnical networks: Content and context revisited. *Knowledge and Society*, 8, 57–83.

Callon, M., & Muniesa, F. (2005). Peripheral vision: Economic markets as calculative collective devices. *Organization Studies*, 26(8), 1229–1250.

Collier, S. J., & Lakoff, A. (2015). Vital systems security: Reflexive biopolitics and the government of emergency. Theory, *Culture & Society*, 32(2), 19–51.

Collins, S. G., Durington, M., and Gill, H. (2017). Multimodality: An invitation: Multimodal anthropologies, *American Anthropologist*, 119, 142–146.

Dijstelbloem, H., & Broeders, D. (2015). Border surveillance, mobility management and the shaping of non-publics in Europe. *European Journal of Social Theory*, 18(1), 21–38.

Dumit, J. (2003) *Picturing Personhood. Brain Scans and Biomedical Identity*. Princeton, NJ: Princeton University Press. Dumit, J. (2017) Game design as STS research, Engaging Science, Technology and Society 3, 603–612.

Edwards, P. N., Mayernik, M. S., Batcheller, A. L., Bowker, G. C., & Borgman, C. L. (2011). Science friction: Data, metadata, and collaboration. *Social Studies of Science*, 41(5), 667–690.

Egbert, S. (2019). Predictive policing and the platformization of police work. *Surveillance & Society*, 17(1/2), 83–88.

Elliott, D., & Culhane, D. (2017). *A Different Kind of Ethnography: Imaginative Practices and Creative Methodologies.* (Toronto: University of Toronto Press).

Ezrahi, Y. (2012). *Imagined democracies: Necessary political fictions.* (Cambridge: Cambridge University Press).

Felt, U. (2015). Keeping technologies out: Sociotechnical imaginaries and the formation of Austria's technopolitical identity, in S. Jasanoff & S.-H. Kim, eds, *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power.* (Chicago, IL: Chicago University Press), pp. 103–125.

Foucault, M. (1979). *The Will to Knowledge, The History of Sexuality: Volume 1* (R. Hurley, transl.). (London: Penguin).

Foucault, M. (1991). *Governmentality, in The Foucault Effect: Studies in Governmentality.* (Chicago, IL: University of Chicago Press), pp. 87–104.

Gabrys, J. (2014). Programming environments: Environmentality and citizen sensing in the smart city. *Environment and Planning D: Society and Space*, 32(1), 30–48.

Gabrys, J. (2016). *Program Earth: Environmental Sensing Technology and the Making of a Computational Planet.* (Minneapolis, MN: University of Minnesota Press).

Gabrys, J., & Pritchard, H. (2018). Sensing practices, in R. Braidotti & M. Hlavajova, eds, *Posthuman Glossary*. (London: Bloomsbury), pp. 394–395.

Gehl, R., & McKelvey, F. (2019). Bugging out: Darknets as parasites of large-scale media objects. *Media, Culture & Society*, 41(2), 219–235.

Graham, S., & Hewitt, L. (2013). Getting off the ground: On the politics of urban verticality. *Progress in Human Geography*, 37(1), 72–92.

Goede, M. D. (2012). *Speculative Security*. (Minneapolis, MN: University of Minnesota Press).

Gitelman, L. (2013). *Raw Data is an Oxymoron*. (Cambridge, MA: The MIT Press).

Graham, S. (n.d.). Foucault's boomerang: The new military urbanism. Retrieved 30 May 2019, from OpenDemocracy website: https://www.opendemocracy.net/en/opensecurity/foucaults-boomerang-new-military-urbanism/

Haggerty, K. D., & Ericson, R. V. (1999). The militarization of policing in the information age. *Journal of Political and Military Sociology*, 27(2), 233.

Hecht, G. (2006). *Nuclear Ontologies. Constellations,* 13(3), 320–331.

Helmreich, S. (2019). Reading a wave buoy. *Science, Technology, & Human Values*, 44(5), 737–761.

Hilgartner, S. (1992). The social construction of risk objects, in L. Clarke & J. F. S. Jr, eds, *Organizations, Uncertainties, And Risk*. (Boulder: Westview Press), pp. 39–53.

Holt, J., & Vonderau, P. (2015). 'Where the internet lives': Data centers as cloud infrastructure, in L. Parks & N. Starosielski, N, eds, *Signal traffic: Critical Studies of Media Infrastructures*. (Champaign, IL: University of Illinois Press), pp. 71–93.

Huysmans, J. (2011). What's in an act? On security speech acts and little security nothings. *Security Dialogue*, 42(4/5), 371–383.

Jensen, C. B. (2008). Power, technology and social studies of health care: An infrastructural inversion. *Health Care Analysis*, 16(4), 355–374.

Jungnickel, K. (2020) *Transmissions: Critical Tactics for Making and Communicating Research*. (Cambridge, MA: MIT Press).

Klauser, F. R. (2010). Splintering spheres of security: Peter Sloterdijk and the contemporary fortress city. *Environment and Planning D: Society and Space*, 28(2), 326–340.

Kim, E.-S. (2016). The sensory power of cameras and noise meters for protest surveillance in South Korea. *Social Studies of Science*, 46(3), 396–416.

Latour, B. (1987). *Science in Action: How to Follow Scientists and Engineers through Society*. Cambridge, MA: Harvard University Press.

Latour, B. (1996). On actor-network theory. A few clarifications plus more than a few complications. *Soziale Welt*, 47(4), 369–381.

Latour, B. (1999). On recalling ANT, in J. Law & J. Hassard, eds, *Actor Network Theory and After*. (Oxford: Wiley-Blackwell), pp. 15–26.

Latour, B. (2005). *Reassembling the Social: An Introduction to Actor-Network-Theory*. (Oxford; New York: Oxford University Press).

Latour, B., & Woolgar, S. (1986). *Laboratory Life: The Construction of Scientific Facts* (2nd ed.). (Princeton, NJ: Princeton University Press).

Latour, B., & Hermant, E. (2006). *Paris: Invisible City*. http://www.bruno-latour.fr/sites/default/files/downloads/viii_paris-city-gb.pdf

Larkin, B. (2013). The politics and poetics of infrastructure. *Annual Review of Anthropology*, 42(1), 327–343.

Law, J. (1994). *Organizing Modernity: Social Ordering and Social Theory*. (Hoboken, NJ: Wiley-Blackwell).

Law, J. (2009). Seeing like a survey. *Cultural Sociology*, 3(2), 239–256.

Law, J., & Mol, A. (2001). Situating technoscience: An inquiry into spatialities. *Environment and Planning D: Society and Space*, 19(5), 609–621.

Law, J. (2002). *Aircraft Stories: Decentering the Object in Technoscience*. (Durham, NC: Duke University Press).

Leese, M. (2016). Exploring the security/facilitation nexus: Foucault at the 'smart' border. *Global Society*, 30(3), 412–429.

Le Bot, J., & M. Noel. (2016). 'Making and doing' at 4S meeting (Denver): Let's extend the experiment! EASST Review, 35(1) https://easst.net/article/making-and-doing-at-4s-meeting-denver-lets-extend-the-experiment/ [accessed 24 March 2020].

Lyon, D. (2002). Everyday surveillance: Personal data and social classifications. *Information, Communication & Society*, 5(2), 242–257.

Lyon, D. (2003). *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. (London; New York: Routledge).

Mackenzie, A. (2017). *Machine Learners: Archaeology of a Data Practice.* (Cambridge, MA: The MIT Press).

Martin, L. L. (2010). Bombs, bodies, and biopolitics: Securitizing the subject at the airport security checkpoint. *Social & Cultural Geography*, 11(1), 17–34.

McCosker, A., & Graham, T. (2018). Data publics: Urban protest, analytics and the courts. *M/C Journal*, 21(3). http://journal.media-culture.org.au/index.php/mcjournal/article/view/1427

Mitchell, T. (2011). *Carbon Democracy: Political Power in the Age of Oil.* (London; New York: Verso).

Mol, A. (2002). *The Body Multiple: Ontology in Medical Practice.* (Durham, NC: Duke University Press).

Mukerji, C. (2011). Jurisdiction, inscription, and state formation: Administrative modernism and knowledge regimes. *Theory and Society*, 40(3), 223–245.

Musiani, F. (2015). Practice, plurality, performativity, and plumbing: internet governance research meets science and technology studies. *Science, Technology, & Human Values*, 40(2), 272–286.

Parks L., & Starosielski, N. (2015) *Signal Traffic: Critical Studies of Media Infrastructures.* (Champaign, IL: University of Illinois Press).

Poechhacker, N., & Nyckel, E.-M. (2020). Logistics of probability. Anticipatory shipping and the production of markets, in M. Burkhardt, K. Grashöfer, M. Shnayien, & B. Westerman, eds, *Explorations of Digital Cultures.* (Lüneburg: Meson Press).

Pelizza, A. (2016). Developing the vectorial glance: Infrastructural inversion for the new agenda on government information systems. *Science, Technology, & Human Values,* 41(2), 298–321.

Pipek, V., Karasti, H., & Bowker, G. C. (2017). A preface to 'Infrastructuring and Collaborative Design'. *Computer Supported Cooperative Work* (CSCW), 26(1/2): 1–5.

Ruivenkamp, M. , & Rip, A. (2014) Nanoimages as hybrid monsters, in C. Coopmans, J. Vertesi, M. Lynch & S. Woolgar, eds, *Representation in Scientific Practice Revisited.* (Cambridge, MA: The MIT Press), pp. 177–200.

Ruppert, E. (2011). Population objects: Interpassive subjects. *Sociology*, 45(2), 218–233.

Ruppert, E. (2012). The governmental topologies of database devices. *Theory, Culture & Society*, 29(4/5), 116–136.

Ruppert, E., Isin, E., & Bigo, D. (2017). Data politics. *Big Data & Society*, 4(2), 1–7.

Salter, M. B. (2004). Passports, mobility, and security: How smart can the border be? *International Studies Perspectives*, 5(1), 71–91.

Schüll, N. D. (2014). *Addiction by Design: Machine Gambling in Las Vegas.* (Princeton, NJ: Princeton University Press).

Serres, M. (1980). *The Parasite.* (Grasset: Paris).

Slota, S. C., & Bowker, G. C. (2016). How infrastructures matter, in U. Felt, R. Fouché, C. A. Miller, & L. Smith-Doerr, eds, *The Handbook of Science and Technology Studies.* (Cambridge, MA: The MIT Press), pp. 529–554.

Spencer, M., Dányi, E., & Hayashi, Y. (2019). Asymmetries and climate futures: Working with waters in an indigenous Australian settlement. *Science, Technology, & Human Values*, 44(5), 786–813.

Star, S. L., & Ruhleder, K. (1996). Steps toward an ecology of infrastructure: Design and access for large information spaces. *Information Systems Research*, 7(1), 111–134.

Star, S. L.; & Bowker, G.C (2002). How to infrastructure?, in Leah A. Lievrouw & Sonia Livingstone, eds, *The Handbook of New Media: Social Shaping and Consequences of ICTs.* (London: Sage), pp. 151–162.

Star, S. L (1995). The politics of formal representations: Wizards, g urus, and organizational complexity, in S. L. Star, ed., *Ecologies of Knowledge: Work and Politics in Science and Technology.* (Albany, NY: SUNY Press), pp. 88–118.

Starosielski, N. (2015). *The Undersea Network.* (Durham, NC: Duke University Press).

Tironi, M. (2017). Regimes of perceptibility and cosmopolitical sensing: The earth and the ontological politics of sensor technologies. *Science as Culture* 27(1), 1–7.

Trischler, H., & Weinberger, H. (2005). Engineering Europe: Big technologies and military systems in the making of 20th century Europe. *History and Technology*, 21(1), 49–83.

Tufekci, Z. (2014). Engineering the public: Big data, surveillance and computational politics. *First Monday*, 19(7). https://firstmonday.org/article/view/4901/4097

Valkenburg, G. (2017). Security technologies versus citizen roles? *Science as Culture*, 26(3), 307–329.

Vertesi, J. (2015). *Seeing Like a Rover: How Robots, Teams, and Images Craft Knowledge of Mars*. (Chicago, IL: University of Chicago Press).

Walford, A. (2017). Raw data: Making relations matter. *Social Analysis*, 61(2), 65–80.

Waller, L., & Witjes, N. (2017). Sensor publics: Report from a workshop on the politics of sensing and data infrastructures. *EASST Review*, 36(2), retrieved from https://easst.net/article/sensor-publics-report-from-a-workshop-on-the-politics-of-sensing-and-data-infrastructures/

Walters, W. (2011). Rezoning the global: Technological zones, technological work, and the (un-) making of biometric borders, in V. Squire, ed., *The Contested Politics of Mobility: Borderzones and Irregularity*. (London: Routledge).

Wang, B. Y., Raymond, N. A., Gould, G., & Baker, I. (2013) Problems from hell, solution in the heavens? Identifying obstacles and opportunities for employing geospatial technologies to document and mitigate mass atrocities', *Stability: International Journal of Security & Development*, 2, 1–18.

Weizman, E. (2002). Introduction to the politics of verticality. Open Democracy, 23. Available at https://www.opendemocracy.net/en/article_801jsp/

Winner, L. (1980). Do artifacts have politics? *Daedalus*, 19(1), 121–136.

Witjes, N., & Olbrich, P. (2017). A fragile transparency: Satellite imagery analysis, non-state actors, and visual representations of security. *Science and Public Policy*, 44(4), 524–534.

Ziewitz, M. (2017). A not quite random walk: Experimenting with the ethnomethods of the algorithm. *Big Data & Society*, 4(2), 1–13.

Zureik, E., & Hindle, K. (2004). Governance, security and technology: The case of biometrics. *Studies in Political Economy*, 73(1), 113–137.

Micro-climates of (in)security in Santiago

Sensors, sensing and sensations

Martin Tironi
Matías Valderrama

Abstract

Over the past ten years, a climate of fear and insecurity has developed in Chile. Despite the low homicide and crime rates, Chileans generally feel unsafe. This feeling is widespread in Las Condes, one of the country's wealthiest municipalities. Inspired by the techno-imaginary of 'smart cities', the local government has introduced a series of 'innovative. and 'dynamic' surveillance technologies as part of its effort to manage and secure urban spaces and wage 'war on crime'. These measures include the deployment of aerostatic surveillance balloons and more recently, highly sophisticated drones that deliver 'personalised warnings' in parks and streets. These drones and balloons offer the municipality a new vertical perspective and allow it to have a presence in the air so that it can give the residents a feeling of security. However, residents and local organisations have protested against the use of these technologies, citing profound over-surveillance and raising important questions about the use of these security devices. In this chapter, we argue that vertical surveillance capacities must be analysed not only in terms of the surveillance and control that they generate, but also the affective atmospheres that they deploy in the urban space and the ways in which these atmospheres are activated or resisted by residents. We reflect on how these technologies open up an affective mode of governance by air in an effort to establish atmospheres or micro-climates in which one experiences (un)expected sensations such as safety, disgust or indifference.

Keywords Drones; video surveillance; security; affective atmosphere; Santiago.

Introduction: The occupation of the urban sky

The skies over modern cities are increasingly occupied by new flying devices of monitoring and datafication. Cities are investing significant resources in order to test 'smart solutions' based on mass data recording under the promise of greater levels of efficiency and public safety. This form of intervening in and surveilling the city from above, using devices such as drones, helicopters, satellites or aerostatic balloons, has given rise to a series of studies that seek to understand their impacts on urban life (Adey 2010; Klauser 2013; Arteaga Botello 2016). Stephen Graham (2012, 2016), has argued that expansion of the practices of tracking, identifying and setting targets of suspicion in spaces of daily life speaks to the increasing militarisation of urban management and security. Within this process one can situate the intensification of what has been called 'politics of verticality' in which control is not limited to two dimensions; instead, governments try to cover a three-dimensional volume of urban space. The air emerges as an ambience that must be controlled and securitised by the use of a series of aerial sensors and technologies that generate vertical distancing between control rooms and the experiences of those who coexist with/under the aerial gaze of such technologies (Adey 2010; Graham and Hewitt 2013; Klauser 2010; Weizman 2002).

In dialogue with this discussion of the effects of this new form of surveilling urban life from the sky, this article analyses the case of Santiago and its recent incorporation of aerostatic balloons and drones to surveil the municipality of Las Condes, one of Chile's wealthiest areas. Described as pilot projects and experimental initiatives, these surveillance devices were introduced within a frame of a 'war on crime' mobilised by the right-wing parties in an attempt to improve the climate of insecurity and fear that every inhabitant supposedly experiences on a daily basis. In spite of criticism and opposition from citizen groups, these technologies are viewed as a great 'success' by those responsible for their introduction, and have begun to be evaluated by other cities in Chile.[1]

Based on an ethnographic study of the process of implementation and operation of aerostatic balloons and drones in Las Condes, we argue that these technologies' vertical capacities should not only be analysed in terms of the surveillance and control that they generate, as tends to be the case in the literature, but also in terms of the atmospheres (Anderson 2009; Adey et al. 2013; McCormack 2008, 2014) that they deploy in the urban space. Adopting an approach from science and technology studies (STS) and perspectives informed by the affective turn, we analyse these surveillance technologies as atmospheric interventions in the city. We seek to move beyond the idea of the fixed 'impacts' of security technologies on the city to examine how the presence of these flying video surveillance devices in the urban sky participates in the deployment of what we will call atmospheres or micro-climates of (in)security.

This analysis is particularly relevant in the Latin American context, where there is a growing militarisation of the modes of securing urban spaces, particularly through the

[1] For example, the municipality of Las Condes was awarded a prize for innovation at a seminar on 'smart cities' in 2017 for the introduction of advanced technologies like the drones.

use of transnational aerial surveillance devices (Arteaga Botello 2016). It is necessary to problematise the belief that technological solutions are imported from the Global North to Latin America as stable black boxes with preset qualities and functions. We demonstrate the importance of studying how these aerial surveillance devices are re-created and re-signified in local contexts, and consider the entanglements, knowledges and situated frictions that are produced. We seek to contribute to the discussion of sensing security in the urban spaces of the Global South, and show that spaces and individuals are not only 'surveilled' through monitoring practices and data infrastructures, but also with sensors and devices that produce different levels of affect which tacitly condition emotions and atmospheres of (in)security.

Specifically, the article describes two displacements. The first is related to how the drones and balloons form part of an experimental political strategy to make residents' atmospheres and sensations more manageable with regard to security. The individuals responsible for the technology argue that the war on crime is not won solely by improving statistics, but requires intervention oriented towards influencing people's sensations and sensibilities. Second, in regard to the effort to produce sensations of security among residents, we analyse the multiple feelings and situated forms of knowledge (Haraway 1988) that the surveilled individuals experience in their everyday coexistence with the flying devices. These registers reveal how the attempt to make the city secure through the use of sensors and surveillance is exceeded by contingent and indeterminate modes of inhabiting and weaving together atmospheres, in which experiences, materialities, representations and affects mingle. In other words, the work to condition atmospheres of security among the population is far from being linearly and uniformly deployed, and is instead the result of specific entanglements and micro-resistances distributed in diverse agencies and contexts.

Atmospheres and the city

In the past few years, a cluster of publications has emerged, mainly based on cultural geography and non-representational theory, that is interested in understanding territory and technologies beyond their physical or discursive qualities, emphasising the need to incorporate the sensorial and affective dimensions that they involve (Thrift 2004; Anderson 2009; Bisell 2010). The consideration of affects in the construction of spatiality, environments and urban practices pays attention to how emotions and affectivities shape perspectives, forms of behaving and doing, the deployment of peculiar modes of production and the appropriation of space. While this approach has been particularly important for examining infrastructures and practices of urban mobility (Bisell 2010; Merriman 2016; Simpson 2017; Tironi & Palacios 2016), it also has begun to be used in surveillance studies to explore how technologies oriented towards the control of spaces and populations install particular atmospheres in the space (Adey et al. 2013; Adey 2014; Ellis et al. 2013; Klauser 2010).

A relevant concept for this work is 'affective atmospheres' (Anderson 2009; Ash & Anderson 2015; Bissell 2010; McCormack 2008, 2014; Stewart 2011). Understood as heterogeneous and ambiguous configurations in which presences and absences, the visible and invisible are connected, this concept reveals that the issue of affects goes far beyond a purely subjective matter and is rooted in material and social circumstances, bodies and imaginaries, creating realities that influence how people feel and act (Bissell 2010). The qualities of affective atmospheres cannot be reduced to words or numbers, because they circulate and are felt through various senses, involving sight, smell, taste sound and any other form that affects bodies, both human and non-human. Affective atmospheres manifest themselves performatively before they are manifested through discourse. Prior to a conscious discourse, the concept of affective atmospheres presents as circulatory and pre-narrative: 'they are neither fully subjective nor fully objective but circulate in an interstitial place in and between the two' (Adey et al. 2013: 301).

Exploring the idea of atmosphere, McCormack (2008) suggests that this concept is commonly defined in two ways: in a *meteorological sense* as the gaseous layer that surrounds a celestial body like the Earth and in which the entities that inhabit the planet breathe and live, and in an affective sense as an affective situation or environment that surrounds or envelops a group of entities under a general or shared feeling or state, such as when one defines a festive atmosphere during celebrations. An important element for our argument is related to the vague and diffuse nature of atmospheres: their qualities are not given and cannot be causally attributed, but are instead registered in and through sensing bodies (McCormack 2008: 413). They have the capacity to condition subjectivities and situations in a distributed and absorbing manner that is at once invisible and indeterminate (Böhme 1993; Bissell 2010). This idea is shared by Anderson (2009), who considers that affective atmospheres are ambiguous because they are not only generated by the things or subjects that perceive them but are always present in the diffuse intersection or entangling of both.

This ontologically dynamic status of atmospheres requires that attention be paid to the conditions that give life to them, overcoming a vision in which the atmosphere is conceived of as something 'out there'. On the contrary, it is important to explore the materiality of atmospheres, how they are sensed and experienced, and how this atmospheric sensibility affects our participation in the world. In this sense, Ingold (2012) suggests that atmospheres should be understood as a becoming-with, that is, rather than representing fixed entities, they arise from the entanglements between multiple entities or forces (humans, chemicals, weather, wind and so on) in particular places, and are perceived in different ways by different sensing bodies. As such, the urban ceases to be a well-defined container and is woven through environments and situations that constitute the threads of the city. As Anderson puts it, 'atmospheres are perpetually forming and deforming, appearing and disappearing, as bodies enter into relation with one another. They are never finished, static or at rest' (Anderson 2009: 79).

The conditioning and design of atmospheres

Atmospheres shape how people feel and think about the spaces they live and breathe in, so it has become of great interest how atmospheres can be 'designed,' 'engineered,' 'sealed off,' 'intervened in' or 'intensified' by different means. Through their composition of various elements, atmospheres can deeply absorb many actors in almost unnoticed ways. As Edensor and Sumartojo (2015) argue, this may depend on the skills of professional and non-professional designers of atmospheres and how they composite, curate or manipulate different materials through design.

This point has been addressed in depth by Peter Sloterdijk in his spherology and his question about the conditions for the origins and persistence of life on Earth. From a fast disappearing world where security was afforded by traditional theological and cosmological narratives, Sloterdijk (2011, 2016) sees a modern transition to societies that attempt to produce their immunities through technical means by the design of interiors or spheres that protect or contain life: 'Spheres are air conditioning systems in whose construction and calibration, for those living in real coexistence, it is out of the question not to participate. The symbolic air conditioning of the shared space is the primal production of every society. Indeed, humans create their own climate; not according to free choice, however, but under preexisting, given and handed-down conditions" (2011: 47–48).

For Sloterdijk, the twentieth century will be remembered for the development of 'atmotechnics' – innovations or technologies for atmospheric design or climate creation: 'Air-design is the technological response to the phenomenological insight that human being-in-the-world is always and without exception present as a modification of "being-in-the-air"'(2009: 93). As Sloterdijk shows, the recognition of our ontological condition of being always enfolded in atmospheres in coexistence with others is directly exploited in gas warfare, through the use of chemical weapons to make the enemy's air unbreathable. The terrorist principle of intervening in the environment (the atmosphere) instead of the system (the enemy's body), was generalised to everyday life through the design of interiors like shopping malls, casinos, clinics and hotels. Air purification is no longer sought, but rather air design is intended to intervene directly in the atmospheres of these spaces with air conditioning and special fragrances in order to induce pleasurable sensations in people and promote consumption (2009: 94). Similarly, Böhme (1993) signals the 'increasing aestheticization of reality', where we find the everyday making of atmospheres through the aesthetic work of multiple objects (like stage sets, advertising, landscapes, cosmetics, gardens, music, art and so on) by sentient or observer subjects.

Within this growing conditioning of the air, atmospheres are becoming objects of concern for security. Based on Sloterdijk's spherology, Klauser (2010) proposes that we think about the efforts to develop an urban security agenda as an entanglement of practices, technologies and architectures of policing, surveillance and enclosure that are not only oriented to the ground but also increasingly to the air. According to this view, security is becoming an atmosphere formation force, splintering the urban volume into multiple psycho-immunological spheres of protection. With the development of drones and everyday security technologies, Peter Adey (2014) speculates that security becomes more alive, encompassing and immersive, registering and resembling the sensibilities of the sensing bodies in the city. Feelings of greater 'security,' 'tranquillity' or 'hospitality' are intended to be engineered and contained atmospherically through the arrangement of surveillance technologies, posters, air conditioning, music and so on, providing new forms of sensing and controlling (Adey et al. 2013). Therefore, in the discussion of the military nature of vertical technologies for security, there is a need to turn our attention to the creation of micro-climates through the affective relationships between the sensorial presence of these technologies and the ambiguous and diffused feelings that they may produce in everyday life.

Following this literature on the – always partial and fragile – modes of creating self-sealed atmospheres, we believe that aerial surveillance technologies are used to try to generate 'a state of being immersed in a psycho-immunological sphere of protection' (Klauser 2010: 327). Here we do not emphasise how individuals are disciplined and/or controlled, but demonstrate instead how the ambiguous aerial intervention activates sensations and forms of sensibility, politically and affectively configuring urban life. Following Rancière (2000), we understand politics as an ontological operation that defines the sensible, that is, what is visible and thinkable, what can be spoken and what is unspeakable or noise. But this 'partition of the sensible' (2000: 12) may operate under a regime that Rancière calls 'police', in which an effort is made to distribute functions and capacities between the public and the private, that which can be perceived and named. In this sense, we will show how these aerial surveillance technologies seek to provoke specific affective atmospheres, and to reconfigure the city's sensible distribution.

At the same time, we focus on the resistance to these efforts to design and condition atmospheres of security. The situational nature of affective atmospheres, which are constantly being built and becoming-with, requires that we examine surveillance situations as moments of dispute and negotiation. As Edensor & Sumartojo (2015) suggest, the enfolding of an atmosphere is always conditioned by social, historical and cultural contexts as well as the personal background and trajectories of each body. Thus, rather than considering the entities absorbed or immersed in an atmosphere as passive and uncritical actors with no agency, they are seen instead as actively constituting their own sensory experience. They can resist, modify and charge the atmosphere with unwanted or unforeseeable tones or sensations for their designers. Therefore, it is relevant to show how an atmosphere can be felt and experienced in unexpected ways by different sensing bodies.

On an empirical level, this kind of atmospheric intervention is examined using the example of the municipality of Las Condes and its increasingly introduction of sensitive and aerial technologies to fight crime. Here we propose to understand these surveillance air balloons and drones as a means of affective atmosphere creation or air design, in the sense that such security technologies modify the mood and sensibility of the area's inhabitants. The aerial presence of these technologies, sensing and registering urban spheres, affects how bodies feel, interact and live in the urban space. In this sense, we wanted to explore not just what people feel about these surveillance aerial systems, but also 'how [the systems] act as sensors working on the human body and generate affects in human bodies' (Lupton 2017: 8).

This chapter is based on two periods of fieldwork. The first was conducted in 2015 and focused on aerostatic balloons, and the other took place in 2017 and centred on the use of drones. We conducted approximately 20 interviews with key stakeholders such as municipal officers, council members who supported and opposed the use of these technologies, members of social organisations, attorneys, residents and others. In addition, ethnographic work was carried out in the urban sites where these balloons and drones were situated. We went on guided walks, had conversations with residents and visited the mobile operation centres for these technologies. Finally, the study includes a thorough review of secondary documents, including media coverage of the controversies and legal and administrative documents that were generated through the introduction and judicialisation of these technologies.

The climate of insecurity and surveillance technologies in Las Condes

Although Chile has historically reported some of the lowest homicide and victimisation rates in Latin America, a feeling of insecurity and fear has intensified over the past few years. This sensation is constantly mentioned in public opinion surveys, which suggest that people believe crime is rising, and public security appears as one of the key concerns of the population (CEP 2017). This climate of insecurity has been particularly present in the municipality of Las Condes, which is one of the wealthiest in the nation. A series of high-impact crimes took place in 2014, including ATM, jewellery store and vehicle robberies, and two explosions in metro stations. City council members and residents staged *cacerolazos* – protests during which participants bang on pots and pans – and called for specific measures to be implemented to win the 'war on crime'. This feeling calls into question the low crime statistics that had been reported in the municipality at the time. Some believed that crime reporting did not manage to capture the 'real' level of criminality in the area and in the country in general due to factors such as under-reporting of crimes. For others, such as Las Condes Mayor Francisco de la Maza, citizens' fear was driven by high-impact news coverage that generated a sensation that was different from the 'reality' of crime in the municipality (Las Condes Municipal Council 2014a 10).

In response to these events, the Municipality of Las Condes introduced a series of 'technological solutions' – categorised as 'innovative' and 'smart' – in order to ensure complete, flexible surveillance of the urban space and thus reduce criminality in the area. These have included the deployment of a video surveillance system based on aerostatic balloons, algorithm-based camera control systems, facial recognition and license plate detection, citizen security app SOSAFE, panic buttons and anti-carjacking systems, lenses with integrated video cameras for guards and most recently the use of drones that provide 'personalised warnings' in public squares.

In this paper, we focus on the transnational spread and adoption of the balloons and drones for video surveillance in the municipality. Rather than centring the discussion on the effectiveness of these aerial technologies when it comes to detecting and reducing crime, or the legal aspect of the violation of privacy, our intention here is to reflect on how these technologies intervene in urban sensibilities. We argue that these technologies have a capacity beyond that of detecting, recording and discouraging crime, an 'affective capacity' to condition atmospheres of security among residents.

Aerostatic balloons

Aerostatic surveillance balloons (for a more complete analysis, see Tironi & Valderrama 2016), were presented in September 2014 as one of the most important smart innovations of the municipality of Las Condes. Former mayor Francisco de la Maza proposed the purchase of these 'high technology aerial cameras', as they were successfully being implemented in the university town of College Station, Texas. He argued that if the municipality had two or three of these cameras 'nearly the entire municipality of Las Condes could be surveilled' right down 'to the size of an ant' (Las Condes Municipal Council 2014b:, p. 9). In response to this proposal, a service commission travelled to Texas to learn about the scope and characteristics of the surveillance system.

The Skystar 180 tactical aerostatic system was developed by the Israeli firm RT Aerostats, which was founded by a retired colonel named Rami Shmueli, who had served in Beirut and Gaza. The device consists of a helium balloon measuring 5.7 metres in diameter that can fly up to 300 meters. A video camera with night vision that can swivel 360° degrees is hung from the device, allowing someone up to 5 km away to be observed. The elements are connected by an electrical cable to a compact trailer, and the set is operated from land by two or three agents in a van or enclosure near the trailer. The corporate brochure describes the device as the perfect tool for surveilling fixed sites such as military bases, temporary military camps, strategic facilities and borders where there are high risks of hostility. While the balloons were initially designed for military use and were deployed on the Gaza Strip and more recently on the US-Mexico border, the company has expanded its scope, selling the military intelligence system to local police departments such as the College Station traffic control unit and to security services for massive events such as Rio de Janeiro's Carnival or the 2015 Climate Change convention in Paris.

After learning about the technology in College Station, the Las Condes service commission returned to Chile convinced that they should buy it. In order to bring the balloons to the Chilean context, they sought to erase or minimise the military origins of the technology, invoking it as a global, civilised tool that had been adapted for Santiago’s urban context. In interviews and news pieces, the mayor, councillors and municipal directors constantly emphasised the balloons’ capacity to capture evidence of crimes and to have a ‘dissuasive effect’ on criminal behaviour and drug dealing when criminals recognise that they are under the gaze of the camera. In addition, it was stressed that the balloons would provide more dynamism and flexibility in surveillance and management of the public space, covering a greater visual radius. This would eliminate the need to install many fixed cameras and would decrease oversight costs, identifying broken pipes or traffic lights, crowds of people or traffic problems more quickly. Moreover, the balloons were described as ideal for the topography of the municipality – characterised by hills and considerable variations in altitude – since they would eliminate the need for traditional short-distance fixed cameras. It was argued that the terrain necessitated an aerial, vertical vision with greater range for city management.

Efforts were also made during the negotiations to downplay the military and Israeli roots of the equipment and to ‘Chileanise’ it by creating an alliance between RT Aerostats and the Chilean security technologies firm Global Systems, transferring knowledge and technical capacities for the use of the technology. The military intelligence functions of the balloons were removed from the bidding terms, and the equipment was described as a ‘surveillance and traffic control system’. Moreover, part of the financing was taken from the municipality’s transit department.

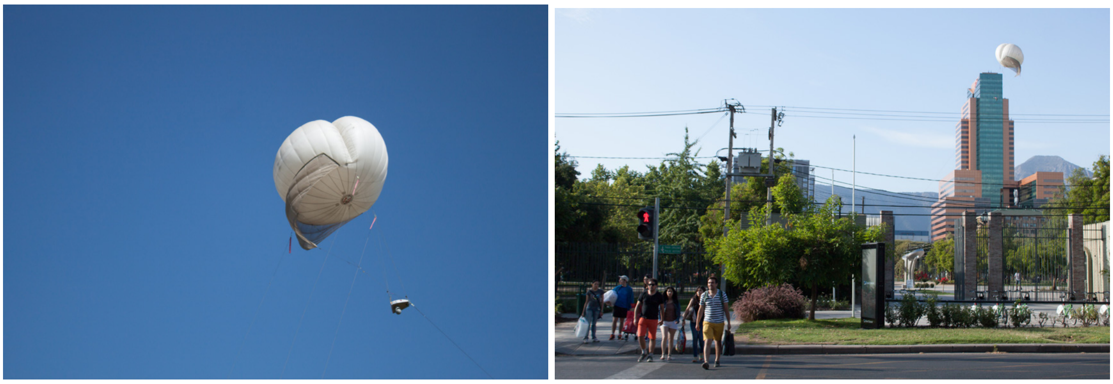


Fig. 1 Surveillance balloon in Las Condes

Once the bid was awarded in May 2015, the Municipality of Las Condes established a rental contract with Global Systems for two balloons, one mobile and one fixed, and also delegated their operation and maintenance to the company. The new operators lacked detailed knowledge of the device’s surveillance capacities and possibilities, which meant that trainers had to travel from Israel for two months to prepare the Chilean staff behind the balloons. Two Global Systems staff members were assigned to five- or six-hour shifts for each balloon. They shared administrative tasks such as recording events, controlling the balloon's height, monitoring the wind and controlling the camera using a joystick.[2]

Were it not for the balloon operators, surveillance would be neither complete nor 'intelligent', because there are no analytics or sophisticated algorithms for interpreting the images. As such, the judgement of the operators themselves, in terms of their criteria for prioritising what to focus on, assumed a special importance. Wind, climate, geographic conditions and the restrictions set by the General Civil Aeronautics Directorate (DGAC) regarding maximum heights were also important conditions for the surveillance system's capacities. For example, some of the main obstacles to visibility were the force of the wind, tree-tops and high buildings, the latter generating blind spots that could not be accessed (field notes from 26 October 2015). According to one municipal director, the cameras had to follow roadways 'but it is very hard to find something on a roadway because everything is moving and the camera is moving' (Director, Municipality of Las Condes). In fact, the operators interviewed told us that they had not detected any ongoing crimes, just traffic accidents, couples having sex in public and 3-7's (people behaving suspiciously). The balloon operators believe that the devices do not reduce crime definitively, but just displace it: 'The fact that the balloon is there and the bad guys see it, persuades. I personally feel like they just go someplace where there are no cameras.' (Operator 1, Global Systems). The balloons are thus catalogued as 'just another complement' to other municipal safety policies, which the employees believe were already quite good.

Drones

The introduction of drones for video surveillance in Las Condes did not emerge as a result of a decision made at the top of the municipality's administration as was the case with the balloons, but through a proposal made by a municipal worker. A former police officer and municipal inspector from the Las Condes Security Direction was a big fan of drones and had considerable experience of using them recreationally. Connecting his hobby to his policing of the municipality, he began to draft a proposal for using drones in public safety work. In January 2017, after word got out that the municipality of Providencia was thinking about using a drone system, the proposal began to gain traction in the mayoral administration of Joaquín Lavín. The idea was discussed on two occasions by the Municipal Council. In contrast to the case of surveillance balloons where a large amount of money was spent without an assessment of their efficiency, the council members unanimous supported a 'pilot project' of drones for surveillance with an initial period of evaluation and testing.

Following a public bidding process, in March 2017 the Las Condes Municipality purchased two DJI Matrice 600 Pro drones from the Dronestore (Zalaquett y Avendaño

[2] All of the staff assigned to monitor the cameras were women, because the spokespeople said that they would be less voyeuristic than men (Tironi & Valderrama 2019).

Limitada.), the Chilean authorized DJI dealer. Da-Jiang Innovations (DJI) is a Chinese company founded in 2006 and based in Shenzhen, widely considered China's Silicon Valley. This company has pushed the design of drones for non-military purposes such as film-making, agriculture, security, search and rescue, energy infrastructure and recreational uses, becoming the world leader in the civilian drone industry. The Matrice model was specifically designed for industrial applications. It weighs around 9 kilos and has an emergency parachute and a modular design that makes it easy to mount additional modules. It can travel at a maximum speed of 65 km/h and can fly autonomously for up to 32 minutes. The system also has a DJI Zenmuse Z30 camera weighing 549 grams with an optical zoom of at least 30x and digital zoom of at least 6x, which allows for a broad range of vision.

The municipality decided to train the staff required to manage the new technology internally. The municipal inspector who contributed to the process of adopting the drones agreed to train seven operators (including five municipal inspectors) in the aerial technology. Three of these employees would go on to form part of the Municipal Aerial Surveillance Brigade, which became responsible for drone operations to support the work of the Las Condes Public Security Direction. The brigade's work began in April 2017, initially supporting the 'Vacation Phone' plan which consists of 'taking care of' residents' homes when they are on vacation. However, the focus quickly changed because, as the municipality explained, 'It was very difficult to take care of them or know if something happened, because we were only looking from outside of the gate, so we could only know whether or not someone had broken the gate or opened a window' (Las Condes Public Security Direction). Furthermore, the regulations regarding drone use in urban space establish that in order for homes to be surveilled, each property owner has to submit a notarised letter to the municipality authorising the drones to fly over their house. This limiting factor (there could be 2,000 homes assigned to a single flight) caused the municipality to change its focus to surveillance of public squares, parks and other public spaces. As a council member stated, 'The purpose of the drones ended up being the squares… there was a lot of alcohol and drug use in certain squares' (Council Member A, Las Condes). The devices became a tool for surveilling and patrolling the 15 plazas where most complaints of drug dealing and alcohol abuse were focused. The sophisticated cameras mounted on the drones allowed them to obtain evidence that could be used in police or prosecutor's office investigations.

The purpose of the drones' use was not the only element to undergo changes. Once introduced in Las Condes, the devices acquired new 'Chilean-style' functionalities. As one member of the brigade said, a drone is 'like a tailor-made suit' to which one can add elements in order to respond to certain requests or needs. First, in response to an announcement made by the mayor on social media, drones were equipped with speakers connected to a radio so that the operator (municipal inspector) could interact with the people who were committing crimes or required assistance. Another drone was subsequently outfitted with special LED lights for night monitoring (field notes, 13 November 2017). For the winter of 2018 a thermal camera was added to one of the drones to monitor and sanction the use of chimneys on days of high environmental pollution. The drones were thus catalogued as 'Chilean' and unique, manifesting an intervention in their design and functionalities.

The implementation of the drones was accompanied by a strong municipal communications drive to publicise their benefits. The mayor himself used Twitter to defend the measure, publishing images and videos, and directly addressing questions and criticism posed by residents who were opposed to the technology. The municipality claimed that the drones had increased surveillance and optimised municipal resources, becoming more effective than a guard and more precise, flexible and inexpensive than the surveillance balloons. The media exposure of the drones was such that they were included in a local military parade.

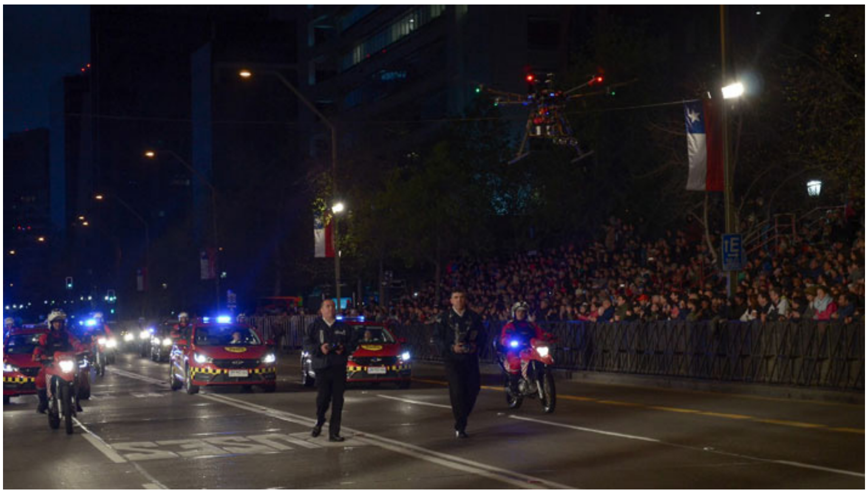


Fig. 2 Military parade with drones

The daily use of the drones is as follows: the drones are launched from five closed areas agreed on by the municipality and the DGAC. An operations centre has been installed in each of these areas, and the drones are assembled there. Operators review the flight requirements such as battery loads, ensure that the trip memory of the drone is restarted and verify that the weather conditions are optimal. Drones are not used if it is raining or windy. They can still fly in these conditions, but they use more energy and thus have a shorter autonomous flight time. The flight route varies but cannot exceed 500 meters from the departure area or last more than 32 minutes (battery life). The devices' actual use depends on the mission that is to be completed for that day. Specific requests submitted by the Investigation Police (PDI) require the drones to be as unobtrusive as possible, identifying the suspects but then hiding their lights so that the suspects' behaviour does not change (field notes, 13 November 2017). In contrast, the patrolling of public plazas to discourage people from committing crimes involves making the drone's presence known. The operators may turn on the lights or interact through the speakers in these cases. One of the drone operators said that 'often just placing the drone over the plaza makes the people causing trouble leave' (Revista Drone Chile 2017: 17). This is indicative, again, of the importance of the presence/absence of this kind of technology in the urban sky, an issue that we will further explore in the next section.

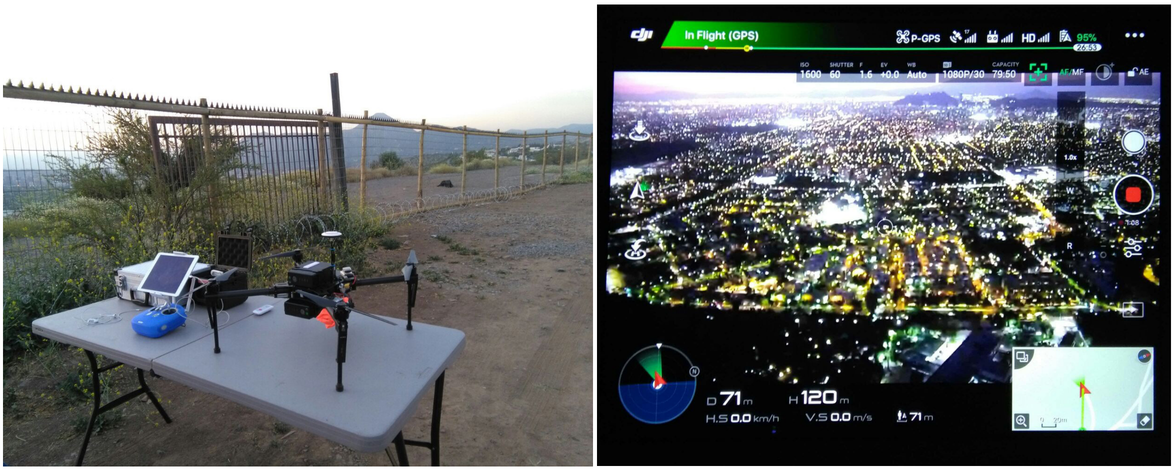


Fig. 3 Drone assembly and aerial view

Conditioning atmospheres of security in Las Condes

The analysis of the incorporation of these two technologies in the municipality of Las Condes shows how the purposes of the surveillance systems were reconfigured as they were imported into Chile and inserted into the urban space. Efforts were made to erase the military origins of the drones or balloons by trying to 'Chileanise' the technologies and give them new applications. But at a deeper level, and based on the discourses of those responsible for them, their capacities went further than detecting or discouraging crime. They also had a less visible or less publicly recognised affective capacity. The municipality is aware that both the drones and balloons are not only a technical solution, but also an instrument that intervenes in and reconfigures the dominant 'climate of insecurity,' which is associated with feelings of fear and anguish on the part of residents. For example, the municipality's Security Direction representative stated:

> Las Condes is the municipality in which crime has fallen the most over the course of this year, but people continue to feel fear. The fear that people feel does not reflect reality. Today people can say, 'Yeah, the numbers are down but I am still afraid and I know there is crime because I see it.' And that is a reality. It is a highly subjective matter because it is a feeling, and it is an enormous challenge to address. (In Reyes 2017)

It has become necessary to try to manage and shape residents' feelings. Decreasing fear is not just a matter of operations, but is mainly sensible and environmental. This has led officials to seek out ways of managing people's feelings, to combat fear, anxiety or panic. It is not only important to manage the issue of crime using functional instruments or by declaring decreases in crime rates. It has also become necessary to manage the sensations and affective climates around people's security. The solution is not limited to increasing the number of security agents or putting more fixed cameras on corners.

It involves creating secure atmospheres and making people feel that they are living in a sphere of constant protection and care.

Along these lines, the Las Condes Public Security Direction has implemented various initiatives in public spaces in an effort to increase the sensation of security, such as lighting streets, erasing graffiti and installing home alarms. These measures are all meant to decrease the sensation of 'disrepair' or -lack of protection' in certain neighbourhoods. The introduction of aerial video surveillance technologies has come to constitute another step in this atmospheric conditioning agenda. The audible and/or visible presence of drones and balloons above Las Condes, and the meanings attached to these technologies connected to their 'smart' nature, seek to establish an air design or conditioning of certain affective relationships between the residents and their environments, generating the sensation that they are being 'protected' or 'surveilled' on an ongoing basis. The aerial surveillance technologies are conceived by their proponents as having the ability to trigger perceptions and feelings of security among residents and passersby. As such, the presence of the drone was considered from the outset as a way of amplifying the presence and power of the municipality in and over the neighbourhoods. 'Some communities have told us that they want a drone to be sent there. In that sense, the drone can be assimilated by being there, in the sense of making its presence known' (Las Condes Safety Direction). Similarly, during our field trips in the communities, some residents (including children) mentioned that the balloons made them feel like they were being observed, which produced a feeling of more security and tranquillity, for example when they were walking at night.

These examples show the capacity of these technological devices (balloons and drones) to make some people feel emotions of security. The operations are part of an attempt to decrease crime rates but also to manage affective atmospheres. We see a form of surveillance emerging here that seeks to internalise a norm, not through a certain action, but by evoking and intervening in the sensations of security in human bodies, this based on the assumption that affecting bodies emotionally can contribute to generating atmospheres or micro-climates of greater security.

Excess, violence and ambiguity

The affective capacities of these technologies in regard to conditioning atmospheres are never unidimensional or confined to a single intention of those who seek to produce sensations of security. We identified feeling of displeasure, vulnerability, indifference and even insecurity in some actors; these sensations go against the sensations of security that were sought, but they nonetheless coexist in urban space despite the intention of the municipal authorities.

An attorney from Las Condes, and other residents, filed a remedy of protection against the balloons, arguing that their mere presence symbolically generated the same level of displeasure as seeing military officials with machine guns in the street. The balloons' omnipotent and omnipresent observation disrupted their social lives, generating a feeling of vulnerability. The attorney insisted on this:

> You have a military device that was built for war operated by a mayor, not even a mayor, by private operatives who are recording a large, unspecified number of people, 24 hours a day every day in public and private spaces. It seems the closest thing to a Western world nightmare
> (Independent attorney).

Activist organisations also filed lawsuits against the balloon and drone operators, denouncing the violation of privacy and limitations on freedom of movement brought about by these aerial technologies. The devices' vertical nature simulated 'a combination of the panopticon and the Eye of Sauron' over the city (Opposition D, Derechos Digitales). According to the NGO Derechos Digitales, residents have changed their way of life because of the balloons' proximity. One of the complainants had a balloon located 90 meters from her home and said:

> I can imagine the clarity with which they can see my bedroom and it gives me chills. I have to keep my windows closed and I can't live the way I used to live because I feel like I am being watched 24 hours a day, seven days a week
> (in Garay 2015).

These descriptions seek to emphasise the negative effects of the presence and over-surveillance of these technologies, making visible the affective states of vulnerability and precarity that these devices activate in the municipality through their mere presence in the sky. The efforts to 'militarise public safety' are also criticised in an attempt to stop the propagation of these aerial tools in other spaces.

> What we could call the "pacification" or "civilization" of military equipment does not have to do with changing its name. It has to do with the disproportionate use of force…. No matter how dangerous a neighborhood may be, you don't go in like Rambo with a machine gun firing or tank. You have to react proportionally. This is the same with the balloons. You can paint it, you can civilize it… the problem is not so much its appearance but what it is.
> (Opposition C, Corporación Fundamental).

A sort of military ontology is manifested that re-emerges despite the municipality's attempts to whitewash the military tints of the technologies. In addition, residents say that although the technologies may inhibit criminals' actions they also affect the behaviours of residents in the public space because they know they are always being watched.

> If you know that they may be watching you, you stop doing certain things… if I know that I am in a radius in which a drone might be surveilling me, I will behave in the way in which the drone wants me to behave.
> (Opposition E, Fundación Datos Protegidos).

These surveillance technologies are again ascribed a capacity for generating an affective atmosphere in their radius of vision – which is indeterminate and dynamic –, changing both behaviour and sensations by making the presence of these technologies visual or audible. When we asked activist organisations how they interpreted the adoption of these devices, some said that they were sensationalist measures 'more showy than effective' (Opposition F, Derechos Digitales) because they mainly serve 'to provide the feeling that something is being done about crime' (Opposition E, Fundación Datos Protegidos). If local authorities managed to decrease crime rates, this would not necessarily have an impact on people because they would be guided more by perceptions and sensations. The activist organisations thus felt that the balloons and drones were highly demonstrative technologies designed to establish a presence in the public space and win votes for local officials whether or not they actually reduced or displaced crime. Despite these arguments, the remedies of protection against the technologies' use have been dismissed and their operation has continued.

Parallel to the public debate about these legal remedies of protection, on our visits to Las Condes we found a multiplicity of sensations that complicate the affections that were intended to be activated in the population. The residents stated that the balloons or drones did not necessarily provide security and often made them feel like they were being 'tattled on,' 'as if the devil were watching'. But the opinion that was repeated most frequently on our ethnographic visits regarding the placement of the balloons and drones was that crime has continued, showing a certain indifference to their presence. 'Everything is still the same,' was one of the phrases most frequently uttered by the residents of the Colón Oriente area, who asserted that drug dealing and crime continued to take place even with the presence of the balloon: 'The people who were committing crimes were afraid in the beginning, but after a while they got used to them' (Resident from the Colón Oriente). Furthermore, due to their daily coexistence with these technologies in the sky, people demonstrated forms of situated knowledge (Haraway, 1988), recognising certain frictions, fragilities and problems that the technologies experienced in their contexts of operation. For example, some residents pointed to blind spots, mainly the treetops that blocked their view, or technical limitations like helium charge or battery life, gusts of wind and the height restrictions that they had to follow. Other residents criticised the discriminatory capacity of these technologies, saying that both the drones and the balloons were there 'to protect the rich', and speculating about where their cameras are focused. This manifests the asymmetric partition of the sensible. The position of these aerial technologies speaks of a vertically defined distribution of feelings in the urban volume that establishes certain neighbourhoods and squares as more 'dangerous', 'insecure' or 'necessary to fly over' than others, thus reproducing socioeconomic differences and accentuating processes of stigmatisation and criminalisation. In sum, the multiplicity of micro-climates is not represented in public debates or even imagined by those responsible for these aerial devices, who do not consider the performativity of their located and sensitive presences.

Conclusions

In this chapter, we have shown how the introduction of aerial surveillance technologies involves multi-sitedness, relations, strategies and re-designs, both discursive and material. In the two cases analysed here, we can see an attempt to 'de-militarise' and 'de-politicise' these vertical technologies, performing them as 'civilised' tools suitable for the context of Las Condes, or even 'Chileanize' them, despite their transnational origins. The justification of the vertical regime of surveillance established by the municipality of Las Condes has been based on its supposed efficiency and greater capacity to surveil and identify 'suspicious' or 'conflictive' behaviours and spaces. However, we have tried to show that these technologies are not exclusively deployed to detect or discourage criminal acts, but also to intervene in citizens' atmospheres of security.

During our research, we were able to observe how drones and balloons are used to try to activate a governmentality based on sensations, that is, to condition and produce micro-climates of security in the population. In response to the misalignment between the quantification of crime and the way the population feels, the people who promote these technologies use them not only as a tool to reduce and deter criminal conduct, but also to affect, intervene in and conduct citizen perceptions and sensations. As such, the devices analysed here are not only handled as technical instruments, but also as mechanisms for installing micro-spheres of psycho-immunological protection in the city (Sloterdijk 2009, 2016; Klauser 2010). Or, to cite Rancière (2000), these technologies are mobilised to reconfigure the politics of the sensible, that is, to impact the 'partition of the sensible' by trying to regulate the orders of the visible, the audible, the utterable and the doable. Thinking about drones and balloons as the inscription of a specific politics of the sensible – which for Rancière is the reduction of the multiplicity of the idea of consensus and normalisation – implies recognising the ontological orders that these devices seek to install by influencing ways of sensing and being in the city.

If there is a tendency to disassociate the human as a sentient entity from technologies as a simple passive reflection of human will, in this chapter we have tried to demonstrate the ways in which these technologies intervene in the urban environment in affective terms. In other words, our analysis allows us to situate the discussion regarding security technologies beyond the understanding of them as tools for detecting a reality 'out there' to be disciplined and modulated, but rather to conceive them as a technique of deploying a vertical politics of affects that reconfigures ways of feeling, living and inhabiting the urban space.

However, it is important to note that atmospheres are always fragile and ambiguous, producing themselves in an always vague and situated manner, and often indifferent to efforts to design and control them at will. The intended micro-climate on the part of the municipality of Las Condes inevitably coexists with varied sensations that exceeds its programme. Many residents expressed emotions that challenge the possibility of conditioning safer atmospheres, experiencing at times displeasure, violence, discrimination or indifference. The goal of the municipality to artificially induce residents to ‘breathe’ more security is situated in a territory of excesses and disputes, recalcitrant to any kind of programming. Officials can use drones and balloons to try to control the types of affects and atmospheres that are experienced in the municipality, but in their entanglements and frictions with their surroundings, these devices have the potential to exceed the intentions and wills of their operators (Simondon 1989), performing other atmospheres and modes of feeling. In this sense, the emotions and affective atmospheres produced by the drones and balloons do not depend on their intrinsic or objective qualities, but the different agencies involved. In this sense, bodies do not only feel the qualities of the atmospheres produced by the drones and balloons differently, but also often act in unanticipated, recalcitrant ways that complicate agents’ attempts to condition/control the urban space.

In this article, we sought to recognise the importance of studying the operations of atmospheric conditioning introduced by aerial surveillance technologies, and the redefinitions that this suggests for surveillance and control practices in Latin American cities (Arteaga Botello 2016). We also analysed the ways in which these atmospheres are rearranged in the process of being activated by different bodies situated in specific socio-material contexts. In this sense, far from analysing the ‘security’ of these technologies as a technical effect of increasing the capacity for observation and data collection, we have tried to understand it as an event that emerges from the entanglement of bodies, varied climatic forces, materialities and sensations.

References

Adey, P. (2010). Vertical security in the megacity: Legibility, mobility and aerial politics. *Theory, Culture & Society*, 27(6), 51–67.

Adey, P., Brayer, L., Masson, D., Murphy, P., Simpson, P., & Tixier, N. (2013). 'Pour votre tranquillité': Ambiance, atmosphere, and surveillance. *Geoforum*, 49, 299–309.

Adey, P. (2014). Security atmospheres or the crystallization of worlds. *Environment and Planning D: Society and Space*, 32(5), 834–851

Anderson, B. (2009). Affective atmospheres. Emotion, *Space and Society*, 2(2), 77–81.

Arteaga Botello, N. (2016). Política de la verticalidad: drones, territorio y población en América Latina. *Región y sociedad*, 28 (65): 263–292.

Ash, J., & Anderson, B. (2015). 'Atmospheric methods', in P. Vannini, ed., *Non-Representational Methodologies* (New York, Routledge), pp. 44–61.

Bissell, D. (2010). Passenger mobilities: Affective atmospheres and the sociality of public transport. *Environment and Planning D: Society and Space*, 28(2), 270–289.

Böhme, G. (1993). Atmosphere as the fundamental concept of a new aesthetics. *Thesis Eleven*, 36(1), 113–126.

CEP (Centro de Estudios Públicos). (2017), Estudio de Opinión Pública September–October 2017. In CEP Chile. Retrieved from https://cepchile.cl/cep/site/edic/base/port/encuestacep.html.Edensor, T., & Sumartojo, S. (2015). Designing atmospheres: Introduction to special issue. *Visual Communication*, 14(3), 251–265.

Ellis, D., Tucker, I., & Harper, D. (2013). The affective atmospheres of surveillance. *Theory & Psychology*, 23(6), 716–731.

Garay, V. (2015). Organizaciones interponen recurso de protección contra los globos de vigilancia de Las Condes y Lo Barnechea. ONG Derechos Digitales. Retrieved from: https://www.derechosdigitales.org/9331/recurso-de-proteccion-contra-los-globos-de-vigilancia-en-las-condes-y-lo-barnechea/

Graham, S. (2011). *Cities under Siege: The New Military Urbanism*. (New York: Verso).

Graham, S. (2016). *Vertical: The City from Satellites to Bunkers*. (New York: Verso).

Graham, S., & Hewitt, L. (2013). Getting off the ground: On the politics of urban verticality. *Progress in Human Geography*, 37(1), 72–92.

Haraway, D. (1988). Situated knowledges: The science question in feminism and the privilege of partial perspective. *Feminist Studies*, 14(3), 575–599.

Ingold, T. (2012). The atmosphere. *Chiasmi International*, 14, 75–87.

Klauser, F. R. (2010). Splintering spheres of security: Peter Sloterdijk and the contemporary fortress city. *Environment and Planning D: Society and Space*, 28(2), 326–340.

Las Condes Municipal Council (2014a, 2 October). Regular Session No. 832. Retrieved from *Las Condes* https://www.lascondes.cl/descargas/transparencia/alcalde_consejo/actas/secciones_ordinaria/2014/ORD_N_832_02_OCTUBRE_2014.pdf

Las Condes Municipal Council (2014b, 25 September). Regular Session No. 831. Retrieved from Las Condes https://www.lascondes.cl/descargas/transparencia/alcalde_consejo/actas/secciones_ordinaria/2014/ORD_N_831_25_SEPTIEMBRE_2014.pdfLupton, D. (2017). How does health feel? Towards research on the affective atmospheres of digital health. *Digital Health*, 3, https://doi.org/10.1177/2055207617701276

McCormack, D. P. (2008). Engineering affective atmospheres on the moving geographies of the 1897 Andrée expedition. *Cultural Geographies*, 15(4), 413–430.

McCormack, D. P. (2014). Atmospheric things and circumstantial excursions. *Cultural Geographies*, 21(4), 605–625.

Merriman, P. (2016). Mobility infrastructures: Modern visions, affective environments and the problem of car parking. *Mobilities*, 11(1), 83–98.

Rancière, J. (2000). *La partage du sensible: Esthétique et politique*. La fabrique éditions.

Revista Drone Chile (2017). Drones en tareas de seguridad y vigilancia. Retrieved from http://www.revistadronechile.com/revista-digital/

Reyes, C. (2017). Javiera Benítez, la socióloga a cargo de enfrentar la delincuencia en Las Condes: 'La gente sigue sintiendo temor'. El Mercurio. Retrieved from http://www.emol.com/noticias/Nacional/2017/08/02/869274/Javiera-Benitez-la-sociologa-a-cargo-de-enfrentar-la-delincuencia-en-Las-Condes-La-gente-sigue-sintiendo-temor.html

Sloterdijk, P. (2009). *Terror from the Air*. Los Angeles, CA: Semiotext(e).

Sloterdijk, P. (2011). *Bubbles. Spheres Volume I: Microspherology*. Los Angeles, CA: Semiotext(e).

Sloterdijk, P. (2016). *Foams, Spheres Volume III: Plural Spherology*. Los Angeles, CA: Semiotext(e).

Simondon, G. (1989). *Du mode d'existence des objets techniques*. Paris: Aubier.

Simpson, P. (2017). A sense of the cycling environment: Felt experiences of infrastructure and atmospheres. *Environment and Planning A: Economy and Space*, 49(2), 426–447.

Stewart, K. (2011). Atmospheric attunements. *Environment and Planning D: Society and Space*, 29(3), 445–453.

Tironi, M., & Palacios, R. (2016). Affects and urban infrastructures: Researching users' daily experiences of Santiago de Chile's transport system. *Emotion, Space and Society,* 21, 41–49.

Tironi, M., & Valderrama, M. (2016). Urbanisme militarisé et situation cosmopolitique. Le cas des ballons aérostatiques de surveillance à Santiago du Chili. *Revue d'anthropologie des connaissances* 10(3), 433–470. Recuperado de: https://www.cairn.info/resume.php?ID_ARTICLE=RAC_032_0433

Tironi, M., & Valderrama, M. (2019). The militarization of the urban sky in Santiago de Chile: The vision multiple of a video-surveillance system of aerostatic balloons. *Urban Geography,* 1–20.

Thrift, N. (2004). Intensities of feeling: Towards a spatial politics of affect. *Geografiska Annaler,* 86B(1),57–78.

Weizman, E. (2002). The politics of verticality. Open Democracy. Retrieved from https://www.opendemocracy.net/ecology-politicsverticality/article_801.jsp

Smart cities, smart borders *Sensing networks and security in the urban space*

Ilia Antenucci

On the outskirts of Kolkata, West Bengal, a satellite township called Rajarhat New Town is being transformed into a smart city, as part of the '100 Smart Cities' programme launched by the Indian government in 2015. The township was originally designed, about thirty years ago, as a Special Economic Zone (SEZ) for the IT industry but has now become a paradoxical space where corporate enclaves and slums, upscale hotels and unfinished constructions uneasily coexist. The projects for New Town reiterate the narrative, crafted by major commercial players, of smart cities as smoothly interconnected systems, and promise that the extensive distribution of computing technologies will turn this urban purgatory into an efficient and harmonious environment. This chapter deconstructs this storyline and draws attention to the ways in which processes of digitalisation entail the distribution of border technologies across the urban space. I also discuss how these bordering processes might constitute distinct politics of knowledge and aesthetics, as well as new techniques of security and urban government.

In her work on the introduction of biometric borders in the context of the post-9/11 'war on terror', Louise Amoore (2006) explains how these have become ubiquitous and bring risk profiling techniques into every realm of social life. Smart borders are informed by an anticipatory logic that seeks to identify, assess and authorise (or not) individuals in such a way that 'the body itself is inscribed with, and demarcates, a continual crossing of multiple encoded borders – social, legal, gendered, racialized and so on' (2006: 337). More recently, Holger Pötzsch (2015) has described the emergence of a socio-technical apparatus – what he calls the 'iBorder' – made of biometrics, dataveillance and AI, which generates

> bordering processes that disperse locally as well as across transnational space. In these processes, individuals become objects of governance to be analysed and assessed, but also serve as implicit contributors to the database enabling algorithm–driven mappings of patterns of behaviour and association. (Pötzsch 2015: 23)

In the past few years, studies on the introduction of smart borders have explored how digital technologies and algorithmic calculations are transforming security practices and responses to terrorism and migration movements in Europe and North America (de Goede et al 2014; Leese 2016). At the same time, scholars have noted that smart borders are increasingly seeping into the city and neighbourhoods (Amoore 2006; Amoore, Marmura and Salter 2008) as part of new military and security paradigms, emerging in the US and UK, which problematise urban life (Graham 2012). However, work remains to be done to chart the specific, situated ways in which smart borders permeate and constitute urban environments, especially in cities outside the US and UK, where the category of military urbanism might not be equally relevant.

At the same time, critiques of smart cities abound, and point to the risks of technocratic governance, surveillance, perpetuation of inequality and social engineering (Crang and Graham 2007; Halpern et al. 2013; Kitchin and Perng 2016). Again, Stephen Graham (2012) has pointed to the ways in which the digitalisation of urban life spreads and normalises technologies that were developed for military purposes. Overall, though, this critical literature has hardly ever crossed over to a more timely and comprehensive discussion of borders in smart cities. Borders have a polysemic, heterogeneous and dynamic nature (Balibar 2002; Mezzadra and Neilson 2013). They work along, within and beyond the territorial limits of states as instruments of differential inclusion and exclusion that continuously filter and stratify the circulation of people and things. This chapter illustrates how, by creating a connected and sentient environment (Crang and Graham 2014; Thrift 2014; Gabrys 2016), digital infrastructures also perform and distribute border functions across the urban space.

In the making of smart cities, as Rob Kitchin and Sung-Yueh Perng (2016) note, code becomes embedded in urban infrastructures, services and utilities, and government practices, in modalities that are always contingent and situated. Cities under digitalisation can be seen as a patchwork of millions of socio-technical assemblages where code is, at once, produced through and productive of multiple sets of relations with other material and discursive elements (Kitchin and Perng 2016; Dourish 2016). Empirical studies confirm how diverse and complex these relations can be. For example, Ayona Datta (2017) observes how the strategies to forge new smart citizens in the wake of India's 100 smart cities challenge merge a global imaginary of smart citizenship with the issues and struggles of postcolonial citizenship, resulting in hybrid and vernacular forms of digital engagement in Indian cities. In his work on data-driven urbanism in Delhi, Sandeep Mertia (2017) illustrates how the forms of knowledge production, forms of authority and identities in and about the city are being reconfigured through sensing/computing infrastructures in ways that are contingent and very much affected by contextual factors. The socio-technical assemblages that compose a smart city have a political significance that demands attention. For this reason, I look at the frictions and barriers that exist around and through these assemblages from the angle of borders. The point here is neither to fetishise the notion of borders, nor to offer a fixed spatial representation of instrumented cities. Rather, looking at urban digitalisation through the lens of borders is a way to attend to the distributed, situated and often microscopic relations of power that permeate smart infrastructures.

This chapter is based on the examination of planning documents, direct observation and interviews with informants involved with the process of urban digitalisation at various levels. It is organised as follows: The first section explores how popular narratives of smart cities as harmonic, seamless systems have been crafted through a set of assumptions and topoi, in accordance with specific commercial strategies. The second section reviews the history of smart developments in New Town, and illustrates how digitalisation has in fact taken place through zoning processes. In the third section, I examine the dissemination of border techniques across digitalised infrastructures, objects and apps of common use, and how the promises of smart urban harmony actually turn into the multiplication of points of control and filter into every aspect of urban life. The fourth section investigates how sensing and computing systems reconfigure categories of perception and knowledge, as well as relations, by setting boundaries and filters, and how borders are active at an ontogenetic level. In the conclusions, I situate these analyses in a broader perspective, and argue that processes of digital bordering cannot be classified merely as examples of surveillance or dataveillance. Instead, I suggest that they be viewed as infrastructures of preemption and anticipatory government.

Smart city narratives

> It can be said that Smart cities of the Future will be smoother, more social, and more open than they are today (Alexander Vancolen, Marketing & eMobility Team Leader at Bosch Belgium).[1]

Arrows in vivid colours run between skyscrapers, ports, parks and highways. Footage of people using smartphones and tablets flows quickly across screens. Wall-size dashboards show interactive maps, graphics and figures. Smiling testimonials tell stories of success and profess their faith in a digital future. What I am describing is not the commercial video for smart city solutions released by a single major provider. It is essentially the same video used by virtually all of them. IBM's Smarter Cities, CISCO's Smart+-Connected, Microsoft's City Next and SAP Future Cities are only some of the products on the growing market of urban digitalisation. And even while they compete against each other to secure contracts with city governments, these and other corporate players contribute to forge a model of a smart city that is, to a large extent, homogeneous. Their

[1] https://www.smart-circle.org/smartcity/blog/smart-cities-future-will-smoother-social-open/

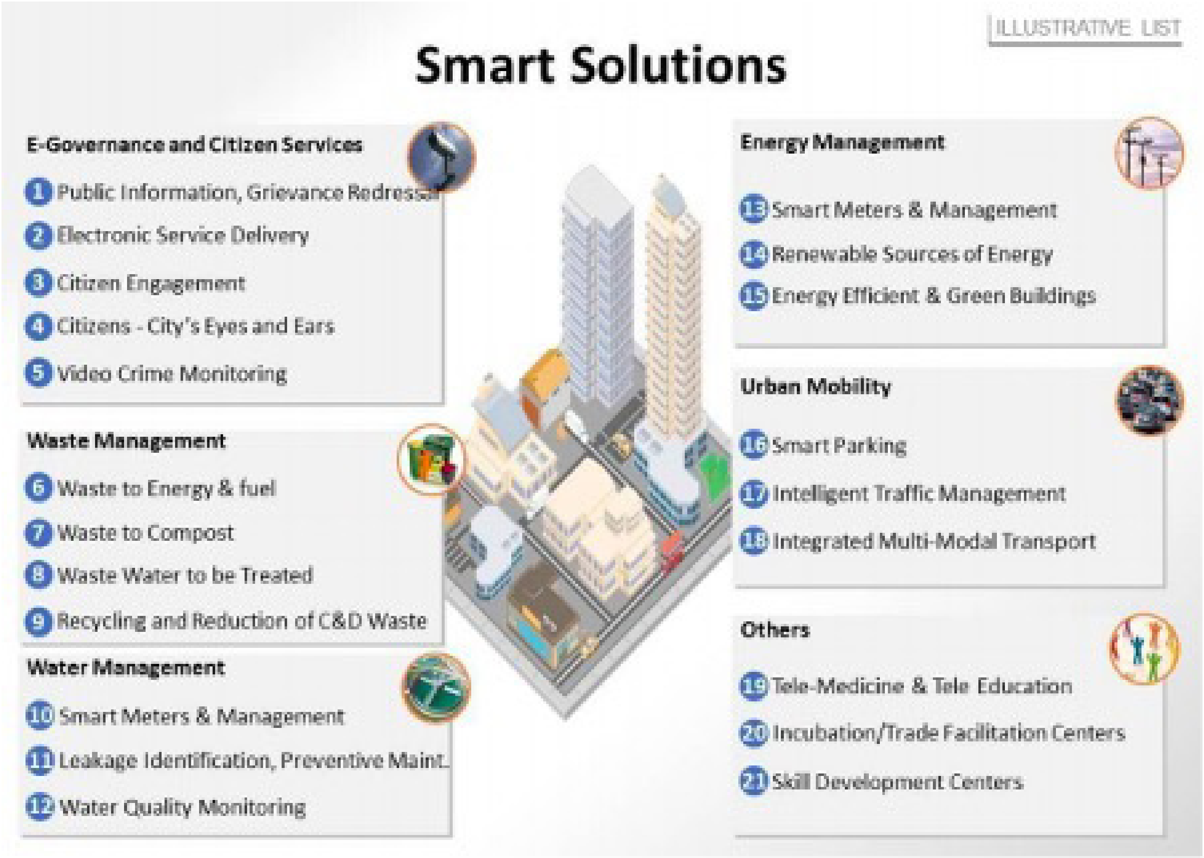
corporate documents and advertising resort to the same imaginary, the same jargon, the same visual style. The key topics in these narratives – efficiency, sustainability, resilience – are perhaps better described as topoi, such is the frequency and the uniformity with which they recur. In all these smart city systems, the focus is on 'breaking the silos' between different urban datasets – traffic, waste, pollution, energy, crime, social programmes, healthcare, education and so on - and creating one integrated platform for the analysis of data – a single view of the city. This is achieved by distributing IoT (Internet of Things) networks across the city, and by running analytics across disparate domains, from sensors and video cameras to social networks.

All these corporate documents present the creation of smart cities as a smooth, harmonious process, based on the assumption that more automation necessarily equals more efficiency, safety and sustainability for all, and that the integration of systems will proceed seamlessly.

Scholars have critically investigated the genesis and evolution of the predominant smart city discourse and the underpinning commercial strategies. Donald McNeill (2015) demonstrates how the launch of IBM's Smarter Planet campaign in 2008 signalled a substantial restructuring of the company, which sold its PC division to Lenovo in 2004 with the intention of concentrating its business in the emerging sector of IT consulting. Having identified cities as a high-potential market, IBM started to focus on aggressively promoting its solutions for urban management. Analysing these commercial strategies, Ola Söderström, Till Paasche and Francisco Klauser (2014) suggest that popular narratives of smart cities can be read as a form of 'corporate storytelling'. Drawing on the concept of 'obligatory passage points' (OPP) proposed by Michel Callon, the authors show how IBM has forged discourses that present its smart technologies 'as the only solution for various urban problems [, which] hence becomes an OPP'. (2014:310).

In 2011, the tech colossus officially registered the term 'smarter cities' as a trademark, while continuing Smarter Planet's powerful advertising strategy, including free consultancy for municipalities, international conferences, research papers, videos and so on. Across these different outlets, the city is presented as a 'system of systems' – a theme then adopted by some of IBM major competitors, such as Microsoft and Cisco – and broken down into nine 'pillars', which represent the relevant sectors that have to be digitally integrated to optimise urban government. In other words, the city, along with all its issues and components, is translated into the language of data and algorithms (Söderström, Paasche and Klauser 2014: 313). Datafication and automation are associated with a number of beneficial results – transparency, efficiency, cost-effectiveness, inclusiveness, sustainability, safety and so on – up to the point that they become synonyms for better government and liveability. The processes of interconnection of infrastructures, devices, data and management practices are supposed to happen linearly and without friction, and to be inherently virtuous. It is largely through the articulation between these discursive moves and the considerable economic power of a colossus like IBM that the mainstream label of smart city has taken shape. As this storyline continues to be echoed among tech companies, consultants, city officers and media, the smart city is uncritically presented as a progressive and even necessary evolution of the urban condition.

The narratives of smart cities mobilised in New Town Kolkata do not deviate much from the corporate version. On the website of the India Smart Cities Mission – the government programme within which the transformation of New Town is taking place -–smart cities are vaguely defined as 'clean and sustainable environments', where 'layers of smartness' are added onto comprehensive infrastructural development (Smart Cities Mission, n.d). The list of technological solutions that make a city smart resembles quite closely the dominant commercial models. The city is broken down into relevant components – administrative services, waste management, energy, water, mobility, health and business – that are supposed to be equipped with digital technology and managed via analytics. (Fig 1).



ILLUSTRATIVE LIST

Smart Solutions

E-Governance and Citizen Services
1 Public Information, Grievance Redressal
2 Electronic Service Delivery
3 Citizen Engagement
4 Citizens - City's Eyes and Ears
5 Video Crime Monitoring

Waste Management
6 Waste to Energy & fuel
7 Waste to Compost
8 Waste Water to be Treated
9 Recycling and Reduction of C&D Waste

Water Management
10 Smart Meters & Management
11 Leakage Identification, Preventive Maint.
12 Water Quality Monitoring

Energy Management
13 Smart Meters & Management
14 Renewable Sources of Energy
15 Energy Efficient & Green Buildings

Urban Mobility
16 Smart Parking
17 Intelligent Traffic Management
18 Integrated Multi-Modal Transport

Others
19 Tele-Medicine & Tele Education
20 Incubation/Trade Facilitation Centers
21 Skill Development Centers

Fig. 1 Image from the Smart Cities Mission website (source: smartcities.gov)

The core idea of adding 'layers of smartness' presupposes a linear development process, where technological elements and governmental practices interconnect progressively and without friction. New Town's municipal authorities have also perpetuated this narrative throughout activities of dissemination and citizen engagement conducted with the help of consultants, such as British company Future Cities Catapult. In the workshops and events organised for the middle class residents of New Town during 2016, participants were educated about the benefits of upcoming digitalisation, and invited to contribute ideas as to how to add more smart solutions to pre-selected areas of intervention – water and energy, transport, security, health and administrative services. The outcome of this 'participative' design phase is shown in the image below: a green, harmonious landscape whose relevant components are provided with sensing technologies and interconnected (Figure 1).

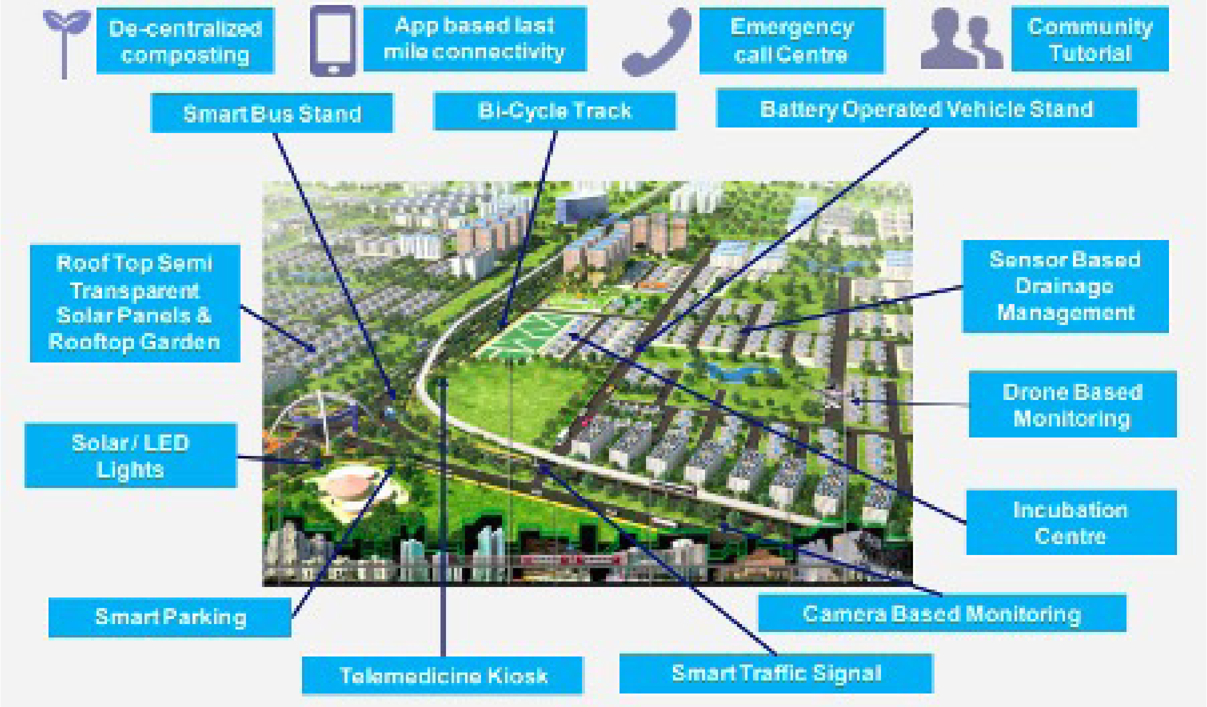


Fig. 2.2 Rendering of the Smart Area Based Development in New Town (source: Smart City Proposal, Annex. 3, n.d.)

Digital zoning

In 2015, New Town Kolkata applied for the Smart Cities Challenge, a competition-based funding scheme launched by the Indian Government with the aim of transforming 100 cities into digital and sustainable cities, and worth approximately US$ 15 billion overall. Before that, the development of New Town had progressed quite controversially.[2] The township was planned in the early nineties as a Special Economic Zone (SEZ) for the IT industry in the rural area of Rajarhat, on the north-eastern fringes of Kolkata. Strong protests rose as the former ruling Left Front government forcibly expropriated land from farmers and villagers; thousands faced police brutality, were jailed or killed. In the following years, business parks, gated communities and luxury shopping malls began to rise alongside wastelands, villages and slums. Many of the dispossessed farmers remained in the area, living in informal settlements and taking up precarious, low-paying jobs as domestic workers, security guards and street vendors. Largely driven by speculation, the development of New Town was hampered by the financial crisis of 2008, resulting in a paradoxical cityscape of unfinished infrastructure,

[2] For a detailed account of the history of New Town see Dey, I., Samaddar, R., and Sen, S. K. (2013), Beyond Kolkata: Rajarhat and the dystopia of urban imagination (Routledge India).

unsold houses, highly securitised enclaves and stray cattle. In 2011, Ananya Roy described the township as 'the ghost town of homegrown neoliberalism, one where the ruins of the suburban middle-class dream are starkly visible' (Roy 2011: 275). Attracted by the low cost of labour and land, several IT firms such as IBM, Tata Consultancy Services, Wipro and Accenture established branches in New Town, where they run the more basic and menial tasks of the industry such as software beta testing or business process outsourcing (Rossiter 2016). As New Town seemed to be stuck in a condition of suspended development, and disturbingly veering towards urban dystopia (Dey et al. 2013) the Smart City Challenge probably appeared to local authorities and investors as a chance to resurrect the fortunes of the township.

The Smart City Proposal (SCP) for New Town is not a very consistent document. Developed through negotiations among several public agencies, consultants and economic stakeholders[3], the proposal revolves around 'Pan City Solutions', a system of integrated digital infrastructures and software for the management of the city. On the one hand, in tune with the standard vision of smart cities promoted by IT firms and consultants, the SCP aims to develop a sensing urban environment, where infrastructures – from bus shelters to waste bins, from water meters to streetlights – are extensively provided with sensors, GPS trackers and cameras, while several urban services are provided via mobile applications. The data sourced from sensing infrastructures are then integrated, cross-checked and processed via analytics into a single command and control room. On the other hand, however, and quite at odds with its claim for innovation, the plan includes very basic elements of urban development – i.e., pavements, public toilets and streetlights. Overall, Pan City looks like a sort of vernacular version of mainstream smart city projects, where the effort towards fast digitalisation coexists with the need to provide basic infrastructures and services in the area. The contradiction between the aspiration towards a global model of urban development and conditions of widespread poverty, inequality and lack of essential facilities is crucial to understanding how borders intervene in the process of digitalisation.

In the first stages of the development of New Town, marked by political disputes and social unrest, the implementation of digital technologies took place behind the walls of upscale private developments protected with security checkpoints, biometric identification, x-ray scanning and CCTV. Within the gates of business districts like Ecospace or Tata's Gitanjali Park, smart infrastructures – high-speed Internet, security software and Building Automations Systems (BAS) that control ventilation, temperature, power systems and water through the IoT – have been running for a few years now. The informal sector is kept out of these enclaves, or only admitted as a service workforce – cleaners, guards, gardeners. More generally, a large part of the population of New Town still struggles to access the Internet and digital devices. According to the Internet and Mobile Association of India (IAMAI), India has approximately 450 million Internet

[3] These include The New Town Kolkata Development Authority (NKDA), the Housing Infrastructure Development Corporation of West Bengal (HIDCO), Future Cities Catapult, Cisco, the American Chamber of Commerce in India (AmCham India), the Confederation of Indian Industry (CII) and the National Association of Software and Service Companies (NASSCOM).

users (IAMAI 2019), slightly more than one third of the overall population. But while technology is becoming cheaper and more accessible for wide strata of the population, smartphones, laptops, computers and Internet connectivity are still out of reach, at least on a regular basis, for households and individuals that live in slums and work precariously in the informal sector. Between the smart world of tech companies and the life of New Town's urban poor there is a gap of income, education and social agency that persists in the processes of urban digitalisation.

At this stage, Pan City is designed as an Area Based Development (ABD). Through digital citizen polling on the MyGov website, one district of New Town has been selected to be transformed into a smart area, where the new technologies and management systems will be first tested and implemented. The zone identified coincides with Action Areas IA and IC, the most densely populated in New Town, the closest to the periphery of Kolkata and to the IT hub of Salt Lake Sector V. In Action Areas IA and IC, the implementation of infrastructures is more advanced than in the rest of the township, urbanisation appears slightly more consistent and informal settlements have been largely cleared out. Strategic facilities, like a water treatment plant and the central bus station, are located here, as are some of New Town's most important business sites and landmarks, such as the NKDA headquarters and the monumental Biswa Bangla Gate. Meanwhile, outside the borders of the designated smart zone, large portions of New Town remain deprived of basic services and infrastructures. In Action Area II, just a few miles away, cutting-edge IT campuses are punctuated by informal markets and bustees that running water and sewerage do not reach. The landscape remains similar in the residential towers of Action Area III, a little further east, where seemingly abandoned building sites and the skeletons of unfinished towers stand out among wastelands. Such entanglements of hyperdevelopment and deprivation are far from uncommon in most megacities in the country; in fact, they can be seen as a major feature of Indian urbanisation (Schindler 2014). The same applies to the increasing securitisation of private and public spaces, over the past two decades, that filters the interactions between different urban worlds, while also introducing new forms of exploitation of informal labour (Gooptu 2013). So far, at least in New Town, digitalisation has not reversed these tendencies, but has rather grafted onto them. Smart developments have largely concentrated within clusters of privilege, and access to them has been restricted on the basis of class and labour control.

This overview illustrates how the making of smart New Town Kolkata is taking place through the formation of hubs and enclaves where digital implementation is concentrated. I refer to this process, which is in sharp contrast to narratives of smart cities as seamless, harmonic environments, as digital zoning. As we learn from a rich body of literature, zoning techniques are always infused with political effects and power relations. Much attention has been paid, for example, to the key role played by the creation of Special Economic Zones (SEZs) and logistical corridors in positioning countries like China and India, and South-East Asia more generally, in the global economy and political relations, as well as in transforming forms of accumulation and extraction, labour relations, normative arrangements and lifestyles (Ong 2006; Easterling 2008; Mezzadra and Neilson 2013). There are no zones without borders, and zoning processes, be they on a larger or smaller scale, are often the occasion where techniques for monitoring and filtering the movements of people and things are tested or recalibrated. The processes of urban zoning have often been associated with notions of enclavism (Atkinson and Blandy 2005) or enclave urbanism (Angotti 2013), to describe how the creation of gated, securitised compounds for residential, commercial or leisure purposes increasingly marks neoliberal urban developments and goes hand in hand with rising inequalities between social groups. Many elements of the development of New Town in recent years, including the creation of gated communities and business parks, can be seen as examples of enclavism. However, this category does not exhaust the complexity of the zoning processes that are associated with the smart city projects. Urban digital zones have emerged in multiple, flexible and informal ways, and have produced multifaceted effects. Some of the zones that I have described in this section, such as New Town's Area Based Development and SEZs, are formally established via legal acts, while others, i.e. corporate enclaves, are demarcated de facto, in informal but no less effective ways, through conspicuous securitisation and the restriction of access to a certain class of citizens. These zoning processes, through which smart infrastructures are being tested and implemented, reflect the patterns of inequality and social hierarchisation that have shaped the creation of New Town since the beginning. Rather than connecting the urban environment seamlessly and inclusively, as the smart city narratives promise, the processes of digitalisation embed extant socio-spatial borders and produce new ones, which separate and filter the population of New Town along the lines of class and social agency.

Ubiquitous borders

Not only are borders traced around digital infrastructures in the making of smart cities; they also become incorporated in a wide range of mundane objects and activities, and therefore become ubiquitous across the urban space. The computing systems on which smart city projects rely are, indeed, built around algorithmic techniques of classification, identification and profiling that are currently in use for the management of national borders, as well as for policing and crime investigation. The smart solutions laid out in the Pan City Solution for New Town disseminate border technologies across every domain of urban administration, from water supply to tax policies, as well as in a number of everyday activities, like getting on a bus or taking out the rubbish.

As mentioned in the previous sections, New Town's Area Based Development (ABD) is supposed to be the first step of the proposed smart city. Not dissimilarly from many other smart city projects, the ABD is designed as a space where ideally every house, vehicle, public area and piece of infrastructure is equipped with sensing devices, connected to the urban network, and managed via a single, central platform. According to the New Town Smart City Proposal (2016), the urban components that will be integrated in the digital platform include:

- Air Pollution monitoring: sensors for air quality monitoring will be installed on streetlights and display real-time data on LED display boards in strategic locations of the area;

- Smart parking: nine smart parking areas with parking sensors installed in streetlights to collect data from the cars. At least four have been introduced already, in partnership with Indian app Park24x7 – a mobile app that allows users to book in advance and pay for their parking online;[4]

- Sewerage and Drainage monitoring: Sensor-based drainage covers will send signals to the control room about the quantity of rainfall in the area, and will activate pumps to avoid waterlogging. More sensors will be installed to monitor sewerage and drainage and transmit the data to the Pan City control room;

- Project Zero – Solid Waste Management. All waste collection vehicles will be equipped with GPS and tracked by the control room. Sensor-based e-bins will be installed in public areas and tracked through Off-Site Real-Time Monitoring (OSRT);

- Smart Metering: All conventional meters for water and electricity will be replaced with smart meters. This will allow remote meter reading, monitoring of load profiles and monitoring of tampering/ pilferage by consumers from the control room. The water distribution pipes will be equipped with Supervisory Control and Data Acquisition (SCADA) systems, including sensor-based transducers and flow meters;

- Safety and Security: CCTV cameras will be set up on streetlights for 24/7 surveillance. Real-time video content analysis will be performed in the control room. 2000 intelligent streetlights will be installed, as well as panic buttons at key points, connected to the control room for emergency response. Drones will monitor civic services such as road conditions, streetlights, littering and waste management;

- Health: Telemedicine kiosks will be installed in every block to deliver primary medical services. Healthcare for residents will be managed via mobile apps and a Smart Watch programme supported by volunteers;

- Mobility: Public vehicles including electric buses, autos and totos will be monitored via GPS from the control room, while information on routes and timetables will be available on a mobile app.

The Pan City Control Centre is where data are gathered and visualised to monitor and manage all the critical components of the smart city in a holistic manner. Once processed via analytics, data turn into models and alerts and are displayed on a central dashboard which provides real-time diagnosis of urban components, from traffic con-

[4] https://www.telegraphindia.com/states/west-bengal/app-to-fix-parking-plights/cid/1531783

gestion to the quality of the air, from water consumption to waste disposal. In other words, in the planner's vision, the entire city becomes incorporated into a system of non-stop monitoring and risk assessment. What is commonly presented as seamless interconnection, efficiency and transparency in fact disseminates the logic and practices of border management across every domain of urban life, often on a microscopic level. Common utilities and ordinary activities become the vectors of techniques of identification, profiling and scoring. Real-time data on power consumption sent from smart meters are automatically crossed with information on housing occupancy and shared with the police to detect potential 'illegal' residents. The network of telemedicine kiosks and health-related apps elaborates profiles of both the individual and collective levels of health or disease in the city. Mobility apps record the itineraries of people across the city, as well as their use of public transport, cars, taxis or other vehicles. While streetlights and bus stops double as surveillance spots, drones provide bird's eye monitoring. As most of these projects are still underway – their implementation outsourced to private partners such as Intel, HP, SAP, Oracle and the like – or as yet exist only on paper, it is too early to assess their effects on urban life. But what matters for the sake of this discussion is that they already present the logic of the future urban environment. In the Pan City Solution, the narrative of a smoothly interconnected city translates into a landscape of ubiquitous borders. Techniques for scrutinising and filtering are built into every part of the urban sensing systems. Increasingly, the interactions between the population and the urban infrastructures and services are mediated by digital identification, and feed processes of algorithmic profiling and modelling.

Social media constitute a further domain of monitoring. From the Smart City Proposal we learn that the city is negotiating with Abzooba, an Indian company specialising in Artificial Intelligence, about installing Xpresso, the company's proprietary Natural Language Processing (NLP) software, to gather and process data concerning New Town on social media (NKDA 2016: 98). NLP is a specific segment of Artificial Intelligence (AI) which makes it possible for computers to read and understand human language and process large volumes of unstructured data, such as social media content. Xpresso was originally developed to help companies analyse customer feedback and improve their commercial strategies accordingly. In the customised version for urban management, Xpresso will help urban authorities exploit large volumes of unstructured data, such as social media content, and gain '[...] a structured bird eye view about different aspects (Police, Transportation, Healthcare, Water, Road etc.) of city and citizen sentiment (positive, negative, neutral) about each of these aspects' (NKDA 2016: 98). The application runs cognitive bots that are able to translate 'text into context',[5] understand the nuances of human expression and classify the intent of those who write. By generating actionable information, Xpresso provides real-time monitoring as well as an 'early warning system' to anticipate potential problems. When high percentages of temporal or spatial spikes in negative sentiment, such as anger or fear, or large number of complaints on selected topics are registered, the dashboard displays specific alerts. Authorities are able then to 'drill down' to view complaints in detail, and take 'corrective meas-

[5] https://www.xpressoinsights.com/about-us.html

ures' (NKDA 2016: 98).
A case study on the Abzooba website describes how Xpresso has been tested before in the management of urban data. According to the case study, Xpresso generated several benefits in urban management, including the capability to measure public opinion, make more informed decisions on new policies and better evaluate existing policies; 'safeguard the country's reputation' (sic) by monitoring social media conversations, and how these might affect overseas investors' and tourists' opinion of the country; anticipate disease outbreaks by correlating searches for specific symptoms and improving disaster response by understanding the situation on the ground; prevent and mitigate potential crisis through 'active listening'; and 'transform [the] security clearance process' by leveraging social media data for 'national security, background investigations, program integrity, insider threat detection, and more'.

Of course, Abzooba is not a pioneer in the field. Opinion mining and sentiment analysis are standard methods for the organisation of social media content and related commercial strategies. A number of systems are being developed, not only by IT corporations, but also by academic research groups, to perform real-time sentiment analysis of discrete social media streams, that assess, for example, with what degree of urgency specific urban issues are perceived by citizens (Masdeval and Veloso 2015); the spatial distribution of intolerant discourses in Italy and the community's feelings about the recovery from the earthquake in the city of L'Aquila (Musto et al. 2015); or to monitor, more generally, the 'situation' of specific urban areas that emerge from topics and emotions on social media (Weiler, Grossniklaus and Scholl 2016).

The adoption of a software like Xpresso is also part, I suggest, of the bordering processes that are shaping the making of the smart city. As explained earlier in this chapter, access to digital technologies in New Town remains far from universal. A considerable part of the township's population is not able to be active on social media on a regular basis, or ever. In this context, monitoring the city and its citizens via social media is a form of pre-selection, or differential inclusion (Mezzadra and Neilson 2013) of the data that are relevant to urban government. In other words, only the voices that can be expressed on digital platforms count as urban data (even if for monitoring purposes only); and only those who provide data count as citizens. The example of Xpresso in New Town subverts the usual understanding of dataveillance. While common concerns relate to being tracked, spied upon and manipulated through our immersion in digital technologies, there are groups of people that are not subject to dataveillance because they are excluded by their socio-economic conditions. Ned Rossiter (2016) uses the term 'post-population' to describe those who escape algorithmic controls on labour or social life but pay the price for this anonymity or 'ungovernability' with extreme precariousness and vulnerable conditions; such, for example, is the situation of the dispossessed farmers and slum dwellers of Rajarhat. In the making of smart New Town then, social media emerge as the terrain of a twofold filtering process. On the one hand, access to social media qualifies people as citizens.

On the other hand, those who count as citizens (in their capacity as data providers) are subject to practices of monitoring and profiling.

The secrecy around the algorithms and code strings that process urban data – from those generated by sensing infrastructures to social media – can be seen as a further bordering process. In the accessible documents about New Town there is no mention of the analytics settings employed in the software that runs city systems, or of the specific pools of data in use. Most likely, this information belong to the software provider, and is therefore protected by corporate cyber-security. Even the city officers and agencies that authorise interventions and elaborate policies on the basis of analytics have no access to the raw data, or to the algorithmic settings. The ways in which the profit strategies of software providers and consultants might have informed the sourcing and processing of data; or how biases and specific understandings of social and environmental categories can be silently embedded in the calculative framework – all this is withheld from public discussion and critique. Despite promises of transparency and evidence, the operational core of smart urban management remains opaque and hidden underneath layers of digital barriers, protocols and private agreements that come with the application of smart technologies to cities.

A new partition of the sensible. Borders and digital ontogenesis

The previous sections of this chapter have described how urban digitalisation proceeds by establishing borders and zones, and by disseminating border techniques – of monitoring, measuring and filtering – across infrastructures and devices of common use. But these bordering processes are active also in the sphere of perception, cognition and relations. In her book Program Earth, Jennifer Gabrys (2016) combines the notion of 'concrescence' formulated by Alfred North Whitehead and that of 'concretization', proposed by Gilbert Simondon, to describe how computing environments come into being. Sensing/computing systems, Gabrys claims, are more than assemblages, more than a mere aggregation of socio-technical elements. In fact, they are able to generate new relations between elements, new forms of connection, expression, knowledge and action; they have, in this sense, an ontogenetic quality. The making of computing environments is, therefore, a relational process where computing becomes environmental, while at the same time, the environment becomes computational. Gabrys also draws connections between this understanding of the environment and Foucault's notion of milieu as the field where security and government operate, and of environmentality 'as a spatial-material distribution and relationality of power through environments, technologies, and ways of life' (Gabrys, 2016: 187). Hence, focusing on the borders that emerge from the processes of digitalisation is a way to grasp how power relations are articulated across sensing/computing environments. As techniques of monitoring, identification and profiling become embedded into mundane objects and infrastructure, they define a distinct terrain and distinct trajectories of government.

In his book The Politics of Aesthetics (2004), Jacques Rancière argues that any social order is constructed through a specific distribution of the sensible. This concept indicates modes of perception that set the boundaries between what can be seen and not seen, said and not said, heard and not heard, measured and not measured, and ultimately, between what is licit or illicit. Social roles and forms of participation are defined through specific distributions of the sensible which can at once include and exclude. In this sense, every social and political system is in the first place an aesthetic regime – where the term 'aesthetic' refers to what is experienced through the senses – insofar as it is organised through distinct forms of perception and sensorial relations among humans, objects and nature. While Rancière's own analysis engages in a detailed examination of historical examples of the politics of aesthetics, here I appropriate the notion of 'distribution of the sensible' and put it to work in a very different context: that of analysing how smart technologies are increasingly performing bordering functions and reconfiguring urban life and government. The distribution of the sensible is, I argue, part of the ontogenetic processes discussed by Gabrys (2016), as changing forms of perception shape the ways in which relations unfold between the various environmental components. Looking at the reconfiguration of the senses and at the creation of new modes of existence that connect humans and things is key to understanding how the computing milieu is governed.

How do sensors and analytics produce new distributions of the sensible in the city, and with what effects for the human and non-human elements involved? How is this distribution of the sensible relevant to the production of security and urban government? When sensing technologies – in their various versions: trackers, beacons, cameras, wearables, smartphones and applications – are applied to urban components, they enable new modalities of perception and interaction. They remodulate patterns of attention towards the object, resource or activity concerned. They can invite and even force attention from users, or, conversely, they might deliberately avoid it, when they are invisible. They signal that a certain component is important in the urban system. They warn that what happens around it is going to be scrutinised and assessed. Whether demanding or rejecting attention from humans, sensors are attentive to selected dynamics, and at the same time, indifferent to others. In doing all this, they reconfigure the order of things, perception, thoughts and action. As described earlier in this chapter, this happens through specific techniques of monitoring and identification. Situations that had previously gone unnoticed, such as the number of people crossing the street at a certain junction, the quantity and quality of particles in the air, the amount of rubbish in a bin, become, through the application of sensors, necessary points of application of urban attention. This attention is political and unfolds simultaneously on interrelated levels. First, it demands the engagement of citizens, who are required to take part in the sensing process by sending data, remaining aware of the information available and behaving accordingly. At the same time, it also dictates the modalities in which this interaction can take place through the mediation of digital devices and platforms. Second, while contributing to the monitoring activity, citizens become objects of scrutiny themselves, through the ubiquitous practices of profiling described before. Third, it marks the specific targets of urban policies and intervention: where there are sensors, there is also government. Fourth, as a whole, sensing networks produce a new map and a new definition of what is to be perceived and lived as an urban system.

The distribution of the sensible continues through analytics processes, where the performances of urban components are broken down algorithmically into factors of normality, deviation and risk, and then reassembled into predictive models. Here again, the work of algorithms establishes distinct boundaries between what can be seen or not seen, made actionable or not. It is important to pay attention to the modalities in which analytics and modelling render urban elements, determining what is worth paying attention to and what is worth measuring. A significant epistemic move is visible here, as the very practice of measuring becomes the measure of worth itself. In other words, if something is not monitored and measured, if it is not inscribed in the computational grid and therefore it has no worth in the smart urban system. In this sense, algorithms create new regimes of visibility and worth, which are politically charged. At the same time, a new regime of invisibility is created, that of the code strings and operative systems which process urban data. As noted earlier in this chapter, these crucial components remain largely inaccessible not only to citizens, but also to the city agencies that are expected to act upon the data.

To conclude this discussion of the partition of the sensible, I maintain that the ontogenetic power that Gabrys assigns to sensing/computing environments reconfigures the order of the cognitive, aesthetic and relational processes. In other words, borders operate at an ontogenetic level, insofar as the forms of classification and filtering that come with extensive datafication are able to reshape the apprehension of reality and the relations between human and non-human elements. They reconfigure both the milieu where security and government operate and the modalities through which they operate.

Conclusions: Beyond dataveillance

What emerges from the examination of New Town smart projects is an urban landscape where bordering functions – identity verification, biometrics recognition, profiling – are immanent to the development of digital infrastructures. This is evidently in contrast with popular narratives of smart cities as seamless, smoothly interconnected spaces. I have outlined three main dimensions where borders operate. The first considers the processes of digital zoning through which smart technologies are introduced and tested in the urban territory. The second dimension concerns the fact that practices of identification and filtering are pervasively attached to objects, devices and software that are in use for everyday activities. The third dimension consists of the processes through which borders reorganise and reshape senses and perception. This is an ontogenetic dimension, where forms of measurement and classification enacted by sensing and computing systems are able to reconfigure cognitive categories and relational dynamics. In essence, border techniques are active around, across and within the sensing and computing environments, and constitute an extensive infrastructure of data sourcing, identification and profiling. These have been widely documented in the literature, along with concerns about their potential political implications. These concerns have often been registered under concepts of surveillance and dataveillance (Kitchin 2014; Tufeckci 2014). Smart cities, David Lyon (2018) argues, bring along the normalisation of surveillance, and metaphors like 'the new panopticon' (McMullan 2015) or the 'big brother city' (King 2016) have been mobilised in the media to describe cities governed from dashboards, where data about everyone and everything is gathered all the time and anonymity becomes impossible.

My intention is not to deny that cities are sites where dataveillance is particularly concentrated. I argue nonetheless that dataveillance is not an exhaustive framework for the analysis of data-driven urban governmentality, for two main reasons. First, despite the efforts of smart city planners, dataveillance often fails. The infinite amount of data gathered through sensing infrastructures does not automatically translate into government actions. Data are often dispersed among several different actors (states, municipalities, private firms, academic or non-academic researchers, NGOs, activists, hackers and so on) which pursue different and often conflicting agendas. This creates zones of opacity. Urban data can be so immense and fragmented that their potential in terms of actual, actionable knowledge remains largely underexploited. Paradoxically, there might be so much dataveillance that it makes complete dataveillance impossible. In short, data largely go to waste; or maybe big data as such is itself waste, until it is dissected by algorithms and reassembled in the form of actionable information. This is one of the problems that smart city projects like New Town are trying to address by creating central control platforms.

But even if dataveillance is applied to the fullest extent, and no data are wasted, it still does not define a logic of urban government. Dataveillance accounts for some important aspects of data-driven environments; it is a disposition (Easterling 2010) of the socio-technical assemblages we live in. But, as such, dataveillance does not explain how decisions are taken or strategies take form. Against the common emphasis on the big of big data, Louise Amoore and Volha Piotukh (2015) demand that attention be directed to the work of little analytics in contemporary forms of knowledge production and government. Through specific practices of data ingestion, partitioning and memory, the heterogeneity of life is flattened and reduced to patterns of data that are tractable for commercial or security decisions. This is exactly the logic of urban platforms like New Town. These work for urban security not by monitoring more, but by translating what is monitored into models, such as risk alerts, and possible actions. Paradoxically, data scientists and officers in the urban control rooms might be better off with less data, but sharper analytics, than with more data without an algorithmic way through. Dataveillance does not explain new forms of urban governance because it keeps the focus on the aspect of watching and on the accumulation of data, while overlooking the specific operations – scraping, skinning, connecting, drawing and, ultimately, modelling – through which algorithms make data actionable and inform decisions.

This chapter has illustrated how smart city planners in New Town seek to forge a system of urban government where, not too differently from what happens at smart borders, algorithmic calculations launched across different sets of urban data provide city officers with profiles of the performance of citizens, transport, traffic, emergency services, weather, resources, pollution and so on. The analytics chain elaborates these data to create models of future events. In the vision of smart government, these models are the grounds for political and administrative operations. Independently of governmental projects, the same activity of profiling and modelling is undertaken by private actors, such as IoT and software providers, for commercial purposes. My point here is that the border techniques ubiquitously incorporated in urban smart technologies form a preemptive apparatus. This is not limited to surveillance functions and frames a specific modality in which urban government is conceived and performed. Benedict Anderson (2010) identifies preemption as one of the logics of anticipatory action – together with the precaution of preparedness – whose specificity is that it works on undetermined, potential scenarios of the future, and that increasingly defines government in our time. Preemptive governance seeks to incorporate, not the probability, but the imagination of future possibilities into security procedures (De Goede 2012; Amoore 2013). Security, then, has become speculative (De Goede et al. 2014); algorithms do not predict, but think through data and build models of the future upon which present action can be taken. From this perspective, borders built within sensing/computing technologies appear as the (sometimes involuntary) infrastructure of new strategies of urban government, whose effects are only beginning to unfold.

References

Abzooba, 'Sentiments going viral could have adverse effects on business or governance', <https://abzooba.com/resources/case-studies/other-case-studies/sentiments-going-viral-could-have-adverse-effects-on-business-or-governance/> [accessed 17 March 2018].

Amoore, L. (2006). Biometric borders: Governing mobilities in the war on terror. *Political Geography*, 25(3), 336–351.

Amoore, L. (2013). *The Politics of Possibility: Risk and Security Beyond Probability* (Durham: Duke University Press).

Amoore, L., Marmura, S., & Salter, M. B. (2008). Smart borders and mobilities: Spaces, zones, enclosures. *Surveillance & Society, 5(2), 96–101.*

Amoore, L., & Piotukh, V. (2015). Life beyond big data: Governing with little analytics. *Economy and Society*, 44(3), 341–366.

Anderson, B. (2008). Preemption, precaution, preparedness: Anticipatory action and future geographies'. *Progress in Human Geography*, 34(6), 777–798.

Angotti, T. (2013). Urban Latin America: Violence, enclaves, and struggles for land. *Latin American Perspectives*, 40(2), 5–20.

Atkinson, R., & Blandy, S. (2005). Introduction: International perspectives on the new enclavism and the rise of gated communities. *Housing Studies*, 20(2), 177–186.

Balibar, É. (2002).What is a border?, Iin É. Balibar and others, eds, *Politics and the Other Scene* (Berlin: Verso Trade), pp. 75–86.

Crang, M., & Graham, S. (2007). Sentient Cities. Ambient intelligence and the politics of urban space. *Information, Communication & Society*, 10(6), 789–817.

Datta, A. (2018). The digital turn in postcolonial urbanism: Smart citizenship in the making of India's 100 smart cities. *Transactions of the Institute of British Geographers*, 43(3), 405–419.

de Goede, M. (2012). *Speculative Security. The Politics of Pursuing Terrorist Monies* (Minneapolis: University of Minnesota Press).

de Goede, M., Simon, S., & Hojitnik, M. (2014). Performing preemption. *Security Dialogue*, 45(5), 411–422.

Dey, I., Samaddar, R., &Sen, S. K. (2013). *Beyond Kolkata: Rajarhat and the Dystopia of Urban Imagination*, (New Delhi: Routledge India).

Dourish, P. (2016). The Internet of urban things, in R. Kitchin and S. Perng, eds, *Code and the City* (London: Routledge), pp. 27–46,

Easterling, K. (2014). *Extrastatecraft: The Power of Infrastructure Space* (New York: Verso).

Foucault, M. (2007). *Security, Territory, Population* (London: Palgrave McMillan UK).

Gabrys, J. (2016). *Program Earth: Environmental Sensing Technology and the Making of a Computational Planet* (Minneapolis: University of Minnesota Press).

Gooptu, N. (2013). Servile sentinels of the city: Private security guards, organized informality, and labour in interactive services in Globalized India. *International Review of Social History*, 58(1), 9–38.

Graham, S. (2012). When life itself is war: On the urbanization of military and security doctrine. *International Journal of Urban and Regional Research*, 36(1), 136–155.

Halpern, O., LeCavalier, J., Calvillo, N., & Pietsch, W. (2013). Test-bed urbanism. *Public Culture*, 25(2), 272–306.

Internet and Mobile Association of India (IAMAI), India Internet 2019, <https://cms.iamai.in/Content/ResearchPapers/d3654bcc-002f-4fc7-ab39-e1fbeb00005d.pdf > [accessed 20 January 2020].

King, A. (2016). 'Is Big Brother on the dark side of the smart city?', *Irish Times*, 20 October, <https://www.irishtimes.com/news/science/is-big-brother-on-the-dark-side-of-the-smart-city-1.2836981> [accessed 4 July 2018].

Kitchin, R. (2011). The programmable city'. *Environment and Planning B: Planning and Design*, 38(6), 945–951.

Kitchin, R. (2014). The real-time city? Big data and smart urbanism. *GeoJournal*, 79(1), 1–14.

Kitchin, R., & Perng, S. Y. (2016). *Code and the City* (London: Routledge).

Leese, M. (2016). Exploring the security/facilitation nexus: Foucault at the 'smart border. *Global Society*, 30(3), 412–429.

Lyon, D. (2018).T*he Culture of Surveillance: Watching as a Way of Life* (Cambridge: Polity Press).

Masdeval, C., & Veloso, A. (2015). Mining citizen emotions to estimate the urgency of urban issues. *Information Systems*, 54,147–155.

McMullan, T. (2015). What does the panopticon mean in the age of digital surveillance?', *The Guardian*, 23 July<https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham > [accessed 4 July 2018]

McNeill, D. (2015). 'Global firms and smart technologies: IBM and the reduction of cities', *Transactions of the Institute of British Geographers*, 40(4), 562–574.

Mertia, S. (2017). Socio-technical imaginaries of a data-driven city - Ethnographic vignettes from Delhi. *The Fibreculture Journal* (29), 94–114.

Mezzadra, S., & Neilson, B. (2013). *Border as Method, or, the Multiplication of Labor* (Durham: Duke University Press).

Mitra, A. (2015). Informal economy in India: Persistence and meagreness. *Agrarian South: Journal of Political Economy*, 4(2), 216–231.

Musto, C., Semeraro, G., Lops, P., & Gemmis, M. (2015). CrowdPulse: A framework for real–time semantic analysis of social streams. *Information Systems*, 54, 127–146.

Ong, A. (2006). *Neoliberalism as Exception: Mutations in Citizenship and Sovereignty* (Durham: Duke University Press).

Pötzsch, H. (2015). The emergence of iBorder: Bordering bodies, networks, and machines. *Environment and Planning D: Society and Space*, 33(1), 101–118.

Rancière, J. (2004). *The Politics of Aesthetics: The Distribution of the Sensible* (London, New York: Continuum).

Rossiter, N. (2016). *Software, Infrastructure, Labor: A Media Theory of Logistical Nightmares.* (New York: Routledge).

Roy, A. (2011). The blockade of the world-class city: Dialectical images of Indian urbanism, in A. Roy and A. Ong. eds, *Worlding Cities* (Oxford: Blackwell), pp. 295–278.

Schindler, S. (2014). The making of 'world-class' Delhi: Relations between street hawkers and the new middle class. *Antipode*, 46(2), 557–573.

'Smart City Proposal, New Town Kolkata, Annexures 2–4 ', (n.d.), *New Town Kolkata Development Authority*, <https://nkdamar.org/File/Smart%20City%201.pdf> [accessed 18 February 2018].

'Smart City Proposal', *New Town Kolkata Development Authority.* (2015). <https://www.nkdamar.org/File/SCP%20 New%20Town%20Kolkata_04042016_Draft%20Final.pdf> [accessed 18 February 2018].

Söderström, O., Paasche, T., &Klauser, F. (2014). Smart cities as corporate storytelling. *CITY*, 18(3), 307–320.

Thrift, N. (2014). The 'sentient' city and what it may portend,. *Big Data & Society,* 1(1).

Tufekci, Z. (2014). Engineering the public: Big data, surveillance and computational politics. *First Monday*, 19(7), 3.

Weiler, A., Grossniklaus, M., &Scholl, M. H. (2016). Situation monitoring of urban areas using social media data streams. *Information Systems*, 57, 129–141.

'What is Smart City', *Smart Cities Mission*, (n.d.) <http://smartcities.gov.in/upload/uploadfiles/files/What%20is%20 Smart%20City.pdf> [accessed 20 January 2018].