Ball, K. Di Domenico, M. & Nunan, D. (2016) 'Big data surveillance and the body-subject'. *Body and Society*, vol. 22, no. 2, 3, pp. 58-81.

DOI: [10.1177/1357034X15624973](https://doi.org/10.1177/1357034X15624973)

This article is part of a special issue of the journal *Body & Society* on Surveillance and Embodiment: Dispositifs of Capture, edited by M. French & G. J. D. Smith.

This is the open access (accepted, peer-reviewed) final article.

Big Data Surveillance and the Body-subject

Abstract

This paper considers the implications of big data practices for theories about the surveilled subject who, analysed from afar, is still gazed upon, although not directly watched as with previous surveillance systems. We propose this surveilled subject be viewed through a lens of proximity rather than interactivity, to highlight the normative issues arising within digitally mediated relationships. We interpret the ontological proximity between subjects, data flows and big data surveillance through Merleau-Ponty's ideas combined with Levinas' approach to ethical proximity and Coeckelberg's work on proximity in the digital age. This leads us to highlight how competing normativities, and normative dilemmas in these proximal spaces, manipulate the surveilled subject's embodied practices to lead the embodied individual towards experiencing them in a local sense. We explore when and how the subject notices these big data practices and then interprets them through translating their experiences into courses of action, inaction or acquiescence.

Key Words: big data, Levinas, Merleau-Ponty, normativity, proximity, subjectivity, surveillance

With the world's media hailing the present as 'the Age of Big Data' this article considers its implications for theories of the surveilled subject.¹ Big data describes a range of socio-technical and commercial trends resulting in the storage, analysis and further usage of huge amounts of data generated by social networks and mobile devices. While both public and private sector organizations seek to capitalize on big data analytics to improve products and services, the data flows which feed big data originate in the mundane, everyday online activities of millions of people. This renders the everyday subject 'surveilled' by definition, yet it is difficult for the subject to comprehend exactly how to evade, resist or negotiate big data practices as – strictly speaking, in terms of embodied practices – there is nobody directly watching them. Ultimately, the data scientists and business people who interpret the results of big data analysis are very far removed from the individuals who provide the data. Recent debates around big data practices in fields as diverse as higher education, energy consumption and health, however, highlight moral questions relating to the 'harvesting' of data from individuals by companies to feed their big data activities. We take these concerns as a cue and propose a shift in how the surveilled subject is theorized in this setting. Rather than focus on Foucauldian treatments of surveillance, which assume a direct gaze as their central feature, we suggest an alternative approach based on the notion of intersecting proximities – rather than relationalities – between subjects, each other and big data surveillance practices. While Foucault's later work began to address more closely the problematic of the subject, we feel that even these perspectives recursively return to questions of institutions and 'governmentality', which occur at a more macro level of analysis and do not offer sufficient explanatory power for our purposes. Having said this, we acknowledge recent work such as that of Btihaj Ajana (2012) who skilfully connects governmentality with the local in the context of biometrics.

Instead we propose an approach to the surveilled subject which is founded on a notion of proximity rather than interactivity with surveillance. We use Merleau-Ponty's (1968) posthumous work to establish ontological proximity between subjects, data flows and big data surveillance. We then draw on Levinas' approach to ethical proximity in conjunction with Coeckelberg's work on proximity in the digital age, to highlight the normative issues which arise in digitally mediated human relations. Accordingly, competing normativities circulate in these proximal spaces between subjects, others and big data users. For example, normativities about the ethics of interpersonal relations, perhaps concerning care, communication and self-expression on the one hand, and ontological consumercentred normativities about convenience, customization, economy or value, on the other. At the intersection of competing normative codes, we predict that the normative dilemmas inherent within the politics of proximity will be felt, lived and experienced by the embodied subject in rich and interesting ways.

In order to map the traces of lived surveilled subjectivity, we propose a research agenda investigating how individuals negotiate, experience and feel these moral dilemmas in a very local sense. We argue that coming to terms with big data surveillant subjectivity involves recognizing not just the presence of a data flow about one's activity but the avowed manipulations of embodied practice through the circulation of competing normativities which occurs. We question the points

at which, and under what conditions they are noticed and what pragmatic courses of embodied action, inaction or acquiescence result. The article begins with a discussion of big data and its origins, with some examples from current debates surrounding it. We then build our theory of the surveilled subject and propose some conclusions around how this might be explored empirically.

‘Big Data’: The Terms of Reference

Big data is defined as ‘high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making’ (Gartner, 2013). The concept emerged as a label to describe a number of factors around the changing landscape of commercial and government data collection, use and application. Following the expansion of eCommerce in the early 2000s, businesses realized they had huge information resources about their operations that could reveal new insights about how best to compete (Degli Esposti, 2014). Information about customer purchase patterns, sales, their business and supply chain partners, and sentiment analyses from social media data became cheaper to store and exploit using new analytical techniques (Jacobs, 2009). New types of business activity emerged: some companies were very effective at analysing their own datasets while others (notably consultancies) offered analytical services to those companies who were less adept at data analysis (Davenport and Harris, 2007). A lucrative market for data has also emerged, where firms sell datasets about potential customers, customer profiles and their creditworthiness (among other things) to those who require them. While data use by corporations was once a means to an end, a mechanism for generating more value from customers, for some companies, such as Google, Facebook, Twitter and others, the collection of data has become an ‘end in itself’. The NSA (National Security Agency), for example, recently completed a new data centre with an assumed capacity of 12 exabytes, or 12 trillion megabytes of data (Hill, 2013). By comparison, researchers have suggested that a theoretical recording of all human speech ever would require only five exabytes (Klinkenborg, 2003).

A key component of any big data strategy is to generate what is termed ‘actionable insight’ for firms using it (Degli Esposti, 2014). Particularly in marketing settings, the object is to leverage insight about consumers gleaned from data in order to ‘persuade’ (or manipulate) them into buying a product or using a service and to target marketing efforts more effectively. Sometimes data collection does not even require active use of a device by a person. Data collection is often automated and passive (Nunan and Di Domenico, 2013), created by automatic sensors in, for example, cell phones, water meters, cars and even buildings. Inferences about human behaviour are drawn from analysis of these data streams. Big data can simply be described as business intelligence on a grand scale, and the overwhelming focus on big data has been about the potential positive impacts on corporations and societies, primarily in terms of cost ‘efficiencies’ (Manyika et al., 2011). Some, however, have questioned its ethics given that it is so grounded in data streams taken from individuals as they use everyday technologies. By definition, this renders those whose data are incorporated in any big data activity a surveilled subject, compromises privacy² and has

broader social implications (boyd, 2010). It enables a creeping extension of both commercial and governmental surveillance into different aspects of the private sphere. One practical consequence of big data is the increasing reliance on algorithm-based analytics. This represents a shift away from segmenting or profiling an abstraction of individual characteristics into groups and a move towards predictive analytics, the use of continually adjusted quantitative models to predict human behaviour on an individual level. Such analytical techniques serve to enable surveillance of future behaviour – what Nigel Thrift calls ‘the political economy of propensity’ rather than current or past behaviour (Thrift, 2008; see also Palma’s, 2010; Siegel, 2013). Because of ubiquitous media and its reliance on complex analytics to convey different messages to users, Savage (2013) has argued that these analytical methods now are the stuff of social life. They comprise modes of instantiating social relationships and are a form of bodily inscription, operating through new normativities and practices. Their instantaneity and ubiquity mean that data analytics are much more lively and ‘in-use’, rather than applied post-hoc to a dataset by a social scientist. In an everyday sense, these ethical questions are very salient given the expansion of big data into public interest settings, such as energy consumption, education and health. Here we see some tough questions being raised about individual privacy and surveillance exposure in the face of autonomous data streams which the individual cannot control.

As part of smart city infrastructures (Klauser and Albrecht, 2014), for example, smart meters allow householders to analyse and hence manage their electricity consumption. However, this information is also available to electricity suppliers and other partners involved in smart city projects. Patterns of life within the home become visible in new ways. Legal scholars in both Europe and North America have begun to question the legalities of smart metering in relation to data protection legislation (Knyrim and Trieb, 2011; McNeil, 2011). At the same time electrical and software engineers are trying to find ways to protect the anonymity and unique electricity consumption footprints of those whose homes have smart meters (Efthymiou and Kalogridis, 2010).

The use of learning analytics in distance education is a similarly controversial area (Prinsloo and Slade, 2014). Universities use both raw and analysed data on student performance to guide the student through the learning process but also inform the university about the performance of cohorts and learning materials themselves. Slade and Prinsloo (2013) note that students rarely give informed consent for their data to be used in this way and feel uncomfortable with some aspects of the tracking involved. They argue that learning analytics lies at the conjunction of two separate sets of normativities: with education as an economic endeavour and as a process which promotes learning, understanding and self-improvement.

Self-improvement is also a theme in the health field. Here, different body-worn devices have been available on the market for some time, linked to the growing ‘quantified self’ (QS) movement. Popular devices such as the Fitbit or Jawbone, which are worn on the wrist, enable the individual to create a picture of their activity over time. The business model of some of these organizations,

including Fitbit, is to harvest individuals' health data and then sell it on to health care providers for marketing purposes. For example Nafus and Sherman (2014) argue:

The QS movement attracts the most hungrily panoptical of the data aggregation businesses in addition to people who have developed their own notions of analytics that are separate from, and in relation to, dominant practices of firms and institutionalized scientific production. (Nafus and Sherman, 2014: 2)

Recently it was revealed that users' Fitbits were automatically uploading data to the web concerning the details of when they had sex (Payne, 2014). Fitbit immediately rectified the problem by withdrawing the uploaded data from the public domain and advising users about privacy settings but the debate highlighted how these data, once shared, are completely out of the control of users. This concern expressed by Payne (2014) is similar to that expressed by the students in Slade and Prinsloo's (2013) study and by smart metering engineers: that individuals can experience a lack of control over data collection, gathering and use, and were uncomfortable with their data being harnessed by third parties in a manner commensurate with big data practices.³ This uncertainty is magnified when multiple data sources can be combined to form new and previously unanticipated forms of surveillance. One example is when researchers used facial recognition techniques to combine public biographical data available via the LinkedIn social network with other public, but anonymous, photos from a major dating site (Acquisti et al., 2011). Another is the ability by which, given sufficient computing power and motivation, aggregated and anonymous data may be de-anonymized, as happened with anonymized individual health records in the US (Ohm, 2010).

Hence, while the term 'big data' may be relatively new, it does exhibit some continuities with surveillance practices; indeed, direct surveillance practices which occurred in the past. As Heilbroner (1967) noted, despite the excitement accompanying new technologies, they are typically incremental, especially when seen in retrospect. So it is with big data. While being presented as a fundamentally new organizational strategy, the technologies that drive big data can be seen as incremental in the context of the growth of information technology over the last four decades. Yet, looking beyond the volume of data, a key consequence of big data is the way it serves to break down boundaries between different sources of data, thus allowing the combination of information from different social domains. In describing big data, one must therefore separate the political discourse surrounding the concept from the technologies from which it arose. The promotion of policies around big data in 'western' contexts serves as an aspiration for the role of data in providing competitive advantage to economies and as a means of providing wider legitimacy to the continuing collection and combination of data. Thus, we are forced to ask what the 'big' in 'big data' refers to. While the etymology of the term encourages a focus on the volume of data, it refers in fact instead more to the ubiquity of data, the completeness of coverage over contemporary lives. It is this ubiquity, the knowledge of a near-complete record of individual lives, which removes the need for a priori decisions on commencing surveillance. In democracies, with clearer legal protections of the line between public and private, big data extends existing surveillance technologies in its ability to co-opt the key economic actors – the corporations – and

thus gain a window into the private. The levels of ubiquity in terms of data collection, previously only available in tightly controlled political environments, are therefore now available universally. More than this, through the increasingly embedded role of online social networks and location-sensitive mobile devices in social activity, the boundaries between surveillance and the surveilled subject become blurred. When specifically quizzed about some big data practices, as they were in the research cited above, subjects express familiar ethical concerns about privacy and surveillance. However, the question we are grappling with in this article is how we think about the surveilled subject for the rest of the time. In our view, big data succeeds in extending the scope of surveillance by co-opting individuals into de facto surveillance of their own private lives, offering a challenge to contemporary understandings of the surveilled subject.

The Big Data Surveilled Subject

With big data, the surveilled subject is now much more closely but sometimes unknowingly enmeshed in surveillance assemblages and subject to multiple lines of sight by virtue of the latter's ubiquity. These lines of sight are embedded in the software applications associated with everyday electronic device use. When theorizing the surveilled subject this poses two challenges. The first is that, in contrast to surveillance practices in the workplace, or in public space using CCTV, the subject is not caught in a direct gaze. Instead they are enmeshed in a political – or political-economic – relationship with those collecting and using data by virtue of the latter's capacity for direct social shaping for economic gain. The second is that the surveillance to which they are subject arises in a milieu of other key connections, such as with friends, family, associates, employers, campaigning groups and gaming activities, that are mediated by the same electronic devices. To respond to such challenges we suggest that a new understanding of the surveilled subject has two elements. First, reflecting the indirectness of the big data surveillant gaze, our thinking is founded on the notion of proximity rather than interactivity with surveillant data flows. We outline how surveillant proximity is one of the many proximities in which subjects find themselves. We use the contrasting theoretical perspectives of Levinas and MerleauPonty to problematize proximity. Second, we suggest that understanding the normativities which circulate within these proximal relationships enables a tracing of moments of surveilled subjectivity within the flow of everyday life. We develop a research agenda based on embodied moments of noticing, the affective sensibilities and bodily inscriptions which engender a sense of everyday lived surveilled subjectivity.

Proximal Surveillant Relations under Big Data

We begin with the notion of proximity. Big data has engendered new social practices, which are designed to generate data but which also enmesh the subject in the surveillant assemblage by inscribing the body in new ways. So, for us, the concept of proximity does two things: first, it helps to encapsulate the background presence of data streams in everyday life and establishes an ontological proximity between the subject and big data surveillance, which is enacted through embodied practice. By extension, it locates the lived body as a central site of interest. Second, it

allows us to refer to an ethical proximity concerning the normativities which surround the manner in which social relations are conducted in digitally mediated contexts.

To delve further into this issue we first turn to the posthumously published work of Maurice Merleau-Ponty (1968), who elucidates the ontological proximities which we think might characterize an indirect surveillance relationship. In *The Visible and the Invisible*, Merleau-Ponty attempts to unpack the proximal relationship between the subject and the world, not only in terms of one's visible presence within that world, but how one develops an 'openness' (1968: 37) towards that world when one is not actively engaged within it. Because of one's capacity to perceive, reflect and then to reflect again upon one's reflections ('hyper-reflexivity'), he argues that objects as perceived by the subject are already overwritten with the body's perceptual capacities.⁴ Indeed, Merleau-Ponty argues that the body:

must plunge into the world instead of surveying it, it must descend toward it such as it is instead of working its way back up toward a prior possibility of thinking it – which would impose upon the world in advance the conditions for our control over it. (1968: 39)

It is within these progressive immersive oscillations between the sensing body and the world that a space of connection emerges. As he beautifully states, this space is 'a sort of straits between exterior horizons and interior horizons ever gaping open' (1968: 132), thus establishing an idea of the embodied subject continually sensing, incorporating and constituting the world. Merleau-Ponty portrays the sensing body, palpating and co-creating the world, and proximity emerges as the qualitative connection between one's own embodied perceptions and the worldly phenomena with which one acts and interacts, and on which one reflects.

Therefore, one's visible presence in the world is but one point in a complex existential process of reflection, hyper-reflection and engagement. But this 'world' is not a simple one, and to reduce perception to 'brute vision', as he terms it, is to miss a trick. Merleau-Ponty argues that to look at the world one must be part of that very world that one seeks to regard. One must coexist with the other(s). In *The Visible and the Invisible*, he explains:

We understand then why we see the things themselves, in their places, where they are, according to their being which is indeed more than their being-perceived – and why at the same time we are separated from them by all the thickness of the look and of the body; it is that this distance is not the contrary of this proximity, it is deeply consonant with it, it is synonymous with it. It is that the thickness of the flesh between the seer and the thing is constitutive for the thing of its visibility as for the seer of his corporeity; it is not an obstacle between them, it is their means of communication. (1968: 135)

Proximity, then, is an embodied sense of nearness, a shared presence which is detected, perceived and incorporated by the subject in their lifeworld. Through the socio-technical practices which accompany big data, a connection-space, or chiasm, of various degrees of intensity, forms between the self and ontologically proximal data streams. For our purposes, the implication is that the

subject does not have to be fully conscious of or interacting with a surveillant data stream to be subject to it. They can be living with – and through – its enablers and consequences in digital contexts. Affective and embodied consciousness of this shared presence can be raised within a research setting and this is our point of departure.

Our next step is to consider how this ontological proximity to data streams might intersect with other proximities in the subject's lifeworld. At this point we turn to Levinas so that we can begin to highlight how digitally mediated self–other relations, which also happen to feature surveillant data streams, are fraught with moral dilemmas and competing normativities. Levinasian proximity is different from the proximity described by Merleau-Ponty: it relates to the ethics inherent within self–other relations. Levinas (1996) explains proximity as referring to the already existing ethical responsibility that one has for the immediate others who surround one and for humanity itself. The other is characterized by the social and moral conditioning to which we have been subject throughout our lives and is always present to some degree within the self:

Anarchically, proximity is a relationship with a singularity, without the mediation of any principle or ideality. It is the summoning of myself by the other (autrui), it is a responsibility toward those whom we do not even know. The relation of proximity does not amount to any modality of distance or geometrical contiguity, nor to the simple 'representation' of the neighbour. It is already a summons of extreme exigency, an obligation which is anachronistically prior to every engagement. An anteriority that is older than the a priori. (Levinas, 1996: 81)

The notion of a morality that is inherent to being-in-the-world is discussed at length by Levinas (1989) in the essay 'Is ontology fundamental?' Here, he introduces the face, which appears throughout his work as the foundation of his ethics, particularly in *Totality and Infinity* (1969). For Levinas, the face represents the irreducible other (autrui) which signifies itself. Attempts to comprehend or signify the other against a 'horizon of being', in profile against and comparison with all being, are violent acts because of the partial negation of the face – that is, the irreducible being – of the other. That same partial negation also renders total dominance of the other, total enslavement, possession and, ultimately, murder, impossible within the realm of relationality. The face also does not exclusively refer to the human face. In a final essay 'Peace and proximity' (1996), Levinas implies that it can refer to different parts of the body, in their complex expressivities. He quotes from Vasily Grossman's novel *Life and Fate*, a story of political detainees travelling to Moscow, having to queue, to make the point:

[She] had never thought that the human back could be so expressive, and could convey states of mind in such a penetrating way. Persons approaching the counter had a particular way of craning their neck and their back, their raised shoulders with shoulder blades tense like springs, which seemed to cry, sob and scream. (1996: 167)

When considered in these terms, it seems inappropriate to refer to an organization using big data techniques as a Levinasian 'other'. Levinas' analysis relates to direct, immediate relations between humans (Levinas, 1991). However we can see how big data practices are an instant moral problem

from the Levinasian point of view. The surveilled subject is always seen in profile, against a 'horizon of being', and hence surveillance is always going to be ethically and morally questionable because of its inherent reductionism. It is perhaps more appropriate, then, to consider the relevant relational contexts in which it arises. Interestingly, reductionism arises as an issue here as well. Coeckelberg (2011), in particular, outlines how proximity can be paradoxical. In examining mobile and online media, he critiques their claim to 'connect' people who are distant in space. This claim that one can keep up or even intensify existing connections, and start up new relationships, is a paradox in that the media that make it possible for relationships to be distant promote distance rather than proximity. 'The paradox is that while presented as a solution to the problem of distance in the global village, it is at the same time its very condition' (Coeckelberg, 2011: 133). It exacerbates the Levinasian paradox: that in digitally mediated relationships it is even more impossible to be ethically responsible for the other, and the presence of the face of the other – its irreducibility – reminds us of that impossibility and moral dilemmas abound. Levinas states:

When I have grasped the other in the opening of being in general, as an element of the world where I stand, where I have seen him on the horizon I have not looked at him in the face, I have not encountered his face. The temptation of total negation, measuring the infinity of this attempt and its impossibility – this is the presence of the face. (1996: 9)

For Levinas, it is the moral obligations that circulate between humans, and how those are enacted, which are important. It is these obligations which create ethical proximity, however problematic and impossible that may be. This is a critical point in our argument, because in our view the silent ubiquity of big data surveillance assemblages and the practices they engender can also carry and inscribe a moral message which intersects with an already existing digitally mediated human–human relationality. The reductionism inherent in all forms of social relations is intensified in today's digitally mediated world (Coeckelberg, 2011). Furthermore, the presence of digital data streaming from these activities into the hands of powerful corporations and governments places self–other relations in a double bind. Not only do they present a moral challenge to the way human beings relate to each other, the whole way of relating is opened up to surveillance by third parties, introducing more moral dilemmas (Sewell and Barker, 2006) and competing normativities.

Competing Normativities

A critical research nexus, then, concerns the normativities which circulate within this milieu, and, specifically, how these are lived and experienced by subjects. In big data surveillance, these normativities are carried by a hybrid array of humans and non-human materialities which represent the surveillance apparatus (Ball, 2002) and are inscribed through social practices of manipulating and using devices and their features which feed big data infrastructures. Indeed Klauser and Albrechtstlund argue that normativity in big data settings arises from 'the study and identification of different normalities' (2014: 282) as they appear in data streamed from everyday settings. Thus, they cite examples from Smarter City projects which emphasize the pursuit of 'connectivity', 'digitization' and 'the intelligent response to needs'. They also cite examples from quantified self-tools to be used for 'self-improvement', 'greater productivity' or 'healthy living'. Each of these

normalities is to be reinforced through the collection and analysis of data as digitally mediated everyday life unfolds. As they argue, the aim is:

the management of multiplicities (of circulating people, of tracked activities, etc.) as a whole, through techniques that 'work within reality, by getting the components of reality to work in relation to each other, thanks to and through a series of analyses and specific arrangements ..' (2014: 282–3)

Hence, these normativities concern how one should live one's life in a way which is also readily encodable in data. This is the key to understanding – and theorizing – the experience of the surveilled subject in the age of big data. The moral dilemmas that arise occur in both ethical and ontological proximity to the subject, occur within digitally mediated self–other relationships, and are experienced as productive as well as repressive.⁵

Furthermore, and echoing our earlier discussion about ethical concerns as a continuity from past to present surveillance practices, the notion of circulating and competing normativities is also well established within studies of surveillance. Many empirical studies of surveillance in action have highlighted how surveillance communicates value systems to the surveilled. Drawing on Scott's (2011) analysis, these normativities could extend to appropriate bodily conduct, sexual relationships, working lives, economic and career opportunities, communicative disclosure, personal loyalties, as well as more fundamental issues concerning power, control and human rights. But these normativities would not just concern appropriate conduct in the intersubjective context but conduct which was convenient for big data surveillance: conduct, in other words, which is easily reducible to a data stream and conducted in conjunction with the big data surveillance assemblage. Indeed, normativities around surveillance include common understandings of how one may benefit from participation in a big data assemblage.

In addition to the examples cited earlier from smart meters, education and health, detailed ethnographic work by Christina Nippert-Eng (2010), which charts individuals' perceived 'islands of privacy', also approaches this issue. Nippert-Eng (2010) shows the efforts made by all kinds of individuals to maintain their boundaries between the self and the world, and how new social codes and norms are generated. Everyday materialities such as wallets, garden fences and medicine cabinets gain new significance in her analysis. Helen Nissenbaum (2010) offers the concept 'contextual integrity' to similarly chart how different social contexts exhibit different privacy values. This is a phenomenon which is also well documented in relation to workplace surveillance, and is known as 'meta-communication' (Ball and Margulis, 2011). 'Meta-communication' refers to how the configuration of employee monitoring and the feedback of monitoring information to employees are infused with messages concerning managerial priorities and judgements as to appropriate behaviours (Stanton and Weiss, 2000). When monitored tasks are deemed more valuable or critical than non-monitored ones, workers will pay greater attention to those tasks and will afford greater importance to the behaviours that monitoring reinforces (Brewer, 1995). Similarly, in high-density CCTV areas, individuals worry more about being a victim of crime if they are aware of the cameras (Gill and Spriggs, 2005). Conflicts have arisen within consumer

spaces such as restaurants when customers make use of hidden surveillance techniques such as 'google glass' to take images of staff and other customers as well as the food and the setting. Upsetting the everyday norms of interaction, this has been interpreted as an invasion of privacy both for staff and other customers who have not knowingly consented or even have been lulled into a false sense of security by the establishment banning such devices, which are not always detectable.⁶

We therefore argue that it is important to consider the normativities which are implicit within and reinforced by forms of big data surveillance as, when encountered, they will interweave in the subject's lifeworld and intersect with other normativities. It is the enactment and instantiation of those norms which is deemed valuable to big data surveillance. It begins at, returns to and constitutes a horizon of being against which all are in profile.

The Big Data Surveilled Body-subject

Ultimately, big data surveillance means that we need to think about the surveilled subject differently. We propose a new focus on the lived normativities which stem from bodily engagement in sociotechnical practices and which render big data surveillance more or less proximal to the subject. To engage as a big data surveilled subject is to come to terms with the proximity of the competing normativities which arise in digitally mediated settings and to come to terms with the manipulation and normative steering to which one is subject. Such a phenomenon can be studied in the flux and flows of everyday life, without necessarily directly referring to surveillant data streams. Examples of such phenomena might concern notions of revitalization and empowerment in relation to one's health and wellbeing or one's centrality in a virtual community of sportspeople that might be achieved by uploading one's step, mood, run or cycle data to the cloud. Other normativities might emerge around sustainable living if one's family home was wired up to the smart grid and its energy consumption shared with one's neighbours, local authority and energy supplier. Within these milieux one is likely to find traces of surveilled subjectivity which can then form the basis of a discussion around compliance, resistance and politics. What are the minuscule doubts, dilemmas and hunches – so often experienced as visceral sensations – around these practices? What questions do subjects have about them and by what rationales do they comply? And to what extent are there patterns within and between different domains of practice in relation to how these normativities are circulated, mobilized and lived?

A focus on normativities, then, adds an analytical layer where there is a lack of direct or conscious inter-relationality between the surveilled subject and the surveillant other. Perhaps this is the reason why big data surveillance processes are so difficult to identify at the level of the subject. It is a fragment of a relation, distal and heavily intermediated, but it can also have a sudden, non-negotiable and destabilizing presence if attention is drawn to it. Negotiation, reflection and engagement are required at the level of the self. Those moments where surveillance is rendered interactional, rather than proximal, are the moments when it becomes noticed as such. This may be the point at which one asserts 'I am not the person you are looking for'; 'I am not the recalcitrant

worker'; 'I am not the flawed consumer' – 'I have nothing to hide, I am who I am'. Those moments of noticing – however momentary they are – become moments of connection, as the individual realizes their place in a much larger infrastructure and notices the identity category to which they are assigned, and when they assert that they are self-not-other. They signify an involuntary entanglement within the infrastructures which constitute everyday life. 'Nothing to hide nothing to fear' becomes a statement of self-worth, a defiant speech-act which re-establishes ontological security and allows the everyday to continue. Realizations of one's engagement with surveillance can be profound as the terms of engagement are revealed. These terms are rarely one's own. This is why a focus on normativity is so crucial.

This additional analytical layer also strongly interpellates developments in body studies which concern a move towards body as process, body as assemblage and embodied trans-subjectivity (Blackman, 2012; Blackman and Venn, 2010). The types of digitally mediated activities which instantiate big data practices articulate the lived body in new ways, creating new registers of bodysubjectivity deeply embedded in everyday worlds, which are sometimes difficult to observe but which powerfully bind humans to the relations in which they are immersed. This emphasis on proximity and normativity reinforces the argument that the body is a central site when studying surveillance. It is the pinnacle of proximity and, through its co-constitutive relationship with the world, recursive reiterations of the lived and social body have the potential to inscribe, incorporate and forge meaning around digital phenomena such as big data surveillance. As Merleau-Ponty argued, one's physical body, 'le corps propre', is not merely an object, but also an enduring condition of experience and perception. He referred to the body as 'la chair du monde', an ontology of 'the flesh of the world' (Merleau-Ponty, 1964, 1968). Ball (2005, 2009) and Di Domenico and Ball (2011) already highlight the embodied, intersubjective and contested way in which the subject is exposed to surveillance. Elsewhere we have argued that the subject is always already exposed to surveillance, because exposure can be addressed as a pre-relational default state (Di Domenico and Ball, 2011; Harrison, 2008). The subject is perpetually turned to the exterior and open to the other, available to be read and signifying but beyond intentionality, will and purpose. Embodied actions are available to be read by others, even when alone, because of the existing representations which are circulating. A second point relates to how the body is contested terrain in surveillance processes. For those who surveill, it is the source of truth about the individual (Ball, 2005). The more of the lived body that is remediated into information flows the more value is created for those who want that information (Bolter and Grusin, 2000; Waldby, 2000). For those who surveill, the impulse is to surface and capture lived interiority to denote truth, authenticity and value within the surveillance dispositif (Ball, 2005, 2009; Lianos, 2003). But at times this may not coincide with an individual's lived, embodied identity and their sense of morality, and this is how the contestation arises. For example, reactions to the Snowden revelations demonstrate that such noticing immediately produced constructions of collectivity, where one's subjection to surveillance signified a subjection which is greater than that of the individual alone. Apart from the obvious resignation and frustration of being subject to such scrutiny, there is a feeling that a trans-subjective sense of that particular surveillance practice has emerged which will then inform shared embodied

noticings and renewed sensitization of the proximity of surveillance in all kinds of settings: a collective version of the embodied sensing theorized by Merleau-Ponty (1968).

Conclusion: Towards a Politics of Proximity

Big data has its origins in business information use. As a set of practices, it has now diffused into both private and public settings and is used to target products and services more efficiently as well as to manage infrastructures. We have argued that this has a set of continuities with surveillance practices from the recent and more distant past, both in terms of ethical reactions to it and in terms of the power structures it sustains. Big data enables corporations, through experimentation with analytics, and the offering of applications which gather data on individuals, not only to collect and store their details but also encourage them to live in new ways. As Savage (2013) has identified and Klauser and Albrechtslund (2014) have argued, data analytics are much more lively and in-use, closely aligned with embodied life as it unfolds. By using the notions of proximity which arise in Merleau-Ponty (1968) and Levinas (1969), and by synthesizing extant empirical work on the experience of surveillance, we have suggested that, in an age of big data, where devices stream huge amounts of information about individuals to organizations, the surveilled subject can be understood in a new way. We suggest that the socio-technical practices that accompany these data streams can instantiate new normativities about how life should be lived in order to feed those data streams so that subjects may incorporate new practices into their embodied lives. Examining the depth and nature of individuals' normative engagement with these new socio-technical practices, particularly around their capacity to collect information, can reveal the lived subtleties and flows in subjection to surveillance. Further, using Merleau-Ponty's work on the embodied, sense-based nature of proximal social relations, we have suggested that prior to surveillance being 'noticed' as such, surveillant relations are rendered proximal by these normativities, which circulate as they are incorporated into the lived practices of subjects. The socio-technical practices which enable big data are diffuse and ubiquitous and so considering surveillance relations as proximal a priori relativizes surveillant encounters in the flows of everyday living. Our focus on proximity sidesteps some of the difficulties associated with establishing connectivity between watcher and watched via a 'gaze', which is perhaps dictated by 'traditional' surveillance theory (Lyon, 2007). It also sidesteps the confounding analytical move which suggests that a lack of awareness of surveillance denotes no subjection to it. We suggest that, while we may examine surveillance practices and identity categories as having a direct link, this link is often accomplished through a heavily intermediated chain of actors. As such, to take this conceptual article into the empirical realm, we suggest that a focus on shifts in normativities surrounding socio-technical practices and relationships with devices could be illuminating and open up space for new politics as well. When methods of big data become established in everyday life, the new proximal, relational and practice-based norms which emerge are worthy of study.

Notes

1. See: http://www.nytimes.com/2012/02/12/sunday-review/big-datasimpact-in-the-world.html?pagewanted=all&_r=40 and <http://www.bbc.co.uk/programmes/b01rt4c7> (accessed 8 April 2014).
2. Lyon (2001: 2) defines surveillance as: 'The collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered', which 'does not usually involve embodied persons watching each other'.
3. See: <http://www.theguardian.com/technology/2014/jun/03/how-activitytrackers-remove-rights-personal-data> (accessed 17 February 2015).
4. We note here that Merleau-Ponty is moving towards a post-Cartesian conceptualization of the body, or at least he speaks of the body's ability to incorporate and constitute the social simultaneously. We also acknowledge that Merleau-Ponty's work is foundational in the work of Crossley (2001), who clearly articulated a post-Cartesian body sociology. Within surveillance studies, the emphasis has always been on the post-Cartesian body, with reference made to the work of, inter alia, Hayles (1999) and Grosz (1994).
5. We acknowledge that spaces of ethics, resistance, play and engagement are to be afforded in our analysis. We also understand that subjects who generate information through their personal devices, internet activities and participation in social networks, and who experience the thrill of self-exposure (McGrath, 2004), are still 'immaterial labourers' for those organizations which possess the means of surveillance (Lazzarato, 1996; Murakami Wood and Ball, 2013).
6. An account of a dispute over using 'Google Glass' in a restaurant is reported in the Seattle Times: <http://blogs.seattletimes.com/allyoucaneat/2013/11/26/diner-using-google-glass-asked-to-leave-restaurant/> (accessed 27 November 2013).

References

- Acquisti A, Gross R and Stutzman (2011) Faces of Facebook: Privacy in the age of augmented reality. Presented at BlackHat Conference, Las Vegas, 4 August.
- Ajana B (2012) *Governing through Biometrics: The Biopolitics of Identity*. London: Palgrave Macmillan.
- Ball K (2002) Elements of surveillance: New research and future directions. *Information, Communication and Society* 5(4): 573–590.
- Ball K (2005) Organization, surveillance and the body. *Organization* 12(1): 89–108.
- Ball K (2009) Exposure: Exploring the subject of surveillance. *Information, Communication and Society* 12(5): 639–657.
- Ball K and Margulis T (2011) Monitoring and surveillance in call centres: A review and synthesis. *New Technology, Work and Employment* 26(2): 113–126.
- Blackman L (2012) *Immaterial Bodies: Affect, Embodiment, Mediation*. London: Sage.
- Blackman L and Venn C (2010) Affect. *Body & Society* 16(7): 7–28.

Bolter J and Grusin R (2000) *Re-mediation: Understanding New Media*. Cambridge, MA: MIT Press.

boyd d (2010) Privacy and publicity in the context of big data. Presented at WWW Conference, Raleigh, NC, 29 April.

Brewer N (1995) The effects of monitoring of individual and group performance on the distribution of effort across tasks. *Journal of Applied Social Psychology* 25: 760–777.

Coeckelberg M (2011) What are we doing? Microblogging, the ordinary private, and the primacy of the present. *Journal of Information, Communication & Ethics in Society* 9(2): 127–136.

Crossley N (1995) Merleau Ponty, the illusive body and carnal sociology. *Body & Society* 1(1): 43–63.

Crossley N (2001) *The Social Body: Habit, Identity and Desire*. London: Sage.

Davenport TH and Harris JG (2007) *Competing on Analytics: The New Science of Winning*. Boston, MA: Harvard Business School Press.

Degli Esposti S (2014) What big data meets dataveillance: The hidden side of analytics. *Surveillance and Society* 12(2): 209–225.

Di Domenico M and Ball K (2011) A hotel inspector calls: Exploring surveillance at the home–work interface. *Organization* 18(5): 615–636.

Efthymiou C and Kalogridis G (2010) Smart grid privacy via anonymisation of smart metering data. In: *Proceedings of the First IEEE conference on Smart Grid Communications*. 4–6 October, Gaithersburg, MD, 238–243.

Foucault M (1977) *Discipline and Punish: The Birth of the Prison*. New York: Random House.

Foucault M (1984) Space, knowledge and power. In: Rabinow P (ed.) *The Foucault Reader*. New York: Pantheon Books, 239–256.

Gartner (2013) IT Glossary. Available at: <http://www.gartner.com/itglossary/big-data/> (accessed 13 February 2015).

Gill M and Spriggs A (2005) *Assessing the Impact of CCTV*. Home Office Research Study 292. London: Home Office Research, Development and Statistics Directorate.

Grosz E (1994) *Volatile Bodies: Towards a Corporeal Feminism*. Bloomington, IN: Indiana University Press.

Harrison P (2008) Corporeal remains: Vulnerability, proximity and living on after the end of the world. *Environment and Planning A* 40: 423–445.

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

Heilbroner R (1967) Do machines make history? *Technology and Culture* 8(3): 335–345.

Hill K (2013) Blueprints of NSA's data center in Utah suggest it holds less info than thought. *Forbes*. Available at: <http://onforb.es/12jOaFk> (accessed 11 April 2014).

Jacobs A (2009) Pathologies of big data. *ACM Queue* 7(6).

Klauser F and Albrechtslund A (2014) From self tracking to smart urban infrastructures: Towards an interdisciplinary research agenda for big data. *Surveillance & Society* 12(2): 273–286.

Klinkenborg V (2003) Trying to measure the amount of information that humans create. *New York Times* 12 November.

Knyrim R and Trieb G (2011) Smart metering under Data Protection Law. *International Data Privacy Law* 1(2): 121–128.

Lazzarato M (1996) Immaterial labour. In: Hardt M and Virno P (eds) *Radical Thought in Italy: A Potential Politics*. Minneapolis, MN: University of Minnesota Press, 133–147. Available at: <http://www.generation-online.org/c/fcimmateriallabour3.htm> (accessed 4 April 2011).

Levinas E (1969) *Totality and Infinity: An Essay of Exteriority*. Pittsburgh, PA: Duquesne University Press.

Levinas E (1989) Is Ontology Fundamental? *Philosophy Today* 33(2): 121–129.

Levinas E (1991) *Otherwise than Being or Beyond Essence*. Dordrecht: Kluwer.

Levinas E (1996) Peace and proximity. In: Peperzak A, Critchley S and Bernasconi R (eds) *Emmanuel Levinas: Basic Philosophical Writings*. Bloomington, IN: Indiana University Press.

Lianos M (2003) Social control after Foucault. *Surveillance & Society* 1(3): 412–430.

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

Lyon D (2007) *Surveillance Studies: An Overview*. Cambridge: Polity Press.

Manyika J, Chui M, Brown B, Bughin J, Dobbs R, Roxburgh C, et al. (2011) Big Data: The Next Frontier for Innovation, Competition, and Productivity. McKinsey Global Institute. Available at: [http:// www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation](http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation) (accessed 5 April 2013).

McGrath J (2004) *Loving Big Brother*. London: Routledge.

McNeil SG (2011) Privacy and the modern grid. *Harvard Journal of Law and Technology* 25(1): 199–224.

Merleau-Ponty M (1964) Eye and mind. Trans. Dallery C. In: Edie J (ed.) *The Primacy of Perception*. Evanston, IL: Northwestern University Press, 159–190.

Merleau-Ponty M (1968) *The Visible and the Invisible, followed by working notes*. Trans. Lingis A. Evanston, IL: Northwestern University Press.

Murakami Wood D and Ball K (2013) Brandscapes of control: Subjects and space in late capitalism. *Marketing Theory* 13(2): 47–67.

Nafus D and Sherman J (2014) This one does not go up to 11: The quantified self movement as an alternative big data practice. *International Journal of Communication* 8(2014): 1784–1794.

Nippert-Eng C (2010) *Islands of Privacy*. Chicago, IL: University of Chicago Press.

Nissenbaum H (2010) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Palo Alto, CA: Stanford University Press.

Nunan D and Di Domenico M (2013) Market research and the ethics of big data. *International Journal of Market Research* 55(4): 505–520.

Ohm P (2010) Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review* 57: 1701–1777.

Palmas K (2010) Predicting what you'll do tomorrow: Panspectric surveillance and the contemporary corporation. *Surveillance & Society* 8(3): 338–354.

Payne C (2014) How activity trackers remove our rights to our most intimate data. *The Guardian* 3 June.

Prinsloo P and Slade S (2014) Educational triage in open distance learning: Walking a moral tightrope. *International Review of Research in Open and Distance Learning* 15(4).

Savage M (2013) The social life of methods: A critical introduction. *Theory, Culture & Society* 30(3): 3–21.

Scott CE (2011) Communist moral corruption and the redemptive power of art in 'The Lives of Others'. *Perspectives on Political Science* 40(2): 78–86.

Sewell G and Barker J (2006) Coercion versus care: Using irony to make sense of organizational surveillance. *Academy of Management Review* 31(4): 934–961.

Siegel E (2013) *Predictive Analytics*. Hoboken, NJ: John Wiley and Sons.

Slade S and Prinsloo P (2013) Learning analytics: Ethical issues and dilemmas. *American Behavioral Scientist* 57(10): 1509–1528.

Stanton JM and Weiss EM (2000) Electronic monitoring in their own words: An exploratory study of employees' experience with new types of surveillance. *Computers in Human Behaviour* 16: 423–440.

Thrift NJ (2008) Pass it on: The political economy of propensity. *Emotion, Space and Society* 1(2): 83–96

Waldby C (2000) *The Visible Human Project: Informatic Bodies and Posthuman Medicine*. London: Routledge.

Kirstie Ball is Professor of Organization at the Open University Business School. Her research interests focus on surveillance in and around organizations and in society at large. In particular, she is interested in subjectivity and the experience of surveillance. She has published in leading management journals including *Organization*; *Work, Employment and Society* and *New Technology, Work and Employment*, as well as in monographs and edited collections, including the *Routledge Handbook of Surveillance Studies*. She is director of the Centre for Research into Information, Surveillance and Privacy (CRISP) at the Open University.

MariaLaura Di Domenico is Professor of Entrepreneurship, Work and Organization, Director of Research and Deputy Head of Surrey Business School, University of Surrey. Her areas of expertise centre on the following: entrepreneurship and small businesses, particularly in relation to lifestyle, privacy, mobility and the home/work interface; social enterprise and social entrepreneurship; discourse and identity. She has published in leading management journals including *Human Relations*; *Organization Studies*; *British Journal of Management*; *Organization*; *Entrepreneurship, Theory and Practice*; *New Technology, Work and Employment*; as well as in books and monographs.

Daniel Nunan is Assistant Professor in Marketing at Henley Business School, University of Reading. His research interests are big data, digital marketing, market research, research ethics and in particular the impact of technology on society. He has published widely in these areas in journals such as the *International Journal of Market Research*; *International Journal of Retail & Distribution Management* and *New Technology, Work and Employment*.