Original Research Article

BIG DATA & SOCIETY

Big Data & Society
January–June 2018: 1–15

DOI: 10.1177/2053951717751551
journals.sagepub.com/home/bds
SAGE

Data doxa: The affective consequences of data practices

Gavin JD Smith

Abstract

This paper explores the embedding of data producing technologies in people's everyday lives and practices. It traces how repeated encounters with digital data operate to naturalise these entities, while often blindsiding their agentive properties and the ways they get implicated in processes of exploitation and governance. I propose and develop the notion of 'data doxa' to conceptualise the way in which digital data – and the devices and platforms that stage data – have come to be perceived in Western societies as normal, necessary and enabling. The 'data doxa' concept also accentuates the enculturation of many individuals into a data sharing habitus which frames digital technologies in simplistic terms as (a) panaceas for the problems associated with contemporary life, (b) figures of progress and convenience, and (c) mediums of knowledge, pleasure and identity. I suggest that three types of data-based relations contribute to the formation of this doxic sensibility: fetishisation, habit and enchantment. Each of these relations come to mediate public understandings of digital devices and the data they generate, obscuring the multifaceted nature and hidden depths of data and their propensity to double up as technologies of exposure and discipline. As a result of this situation, imaginative educational programs and revamped regulatory frameworks are urgently needed to inform individuals about the contribution of data to the leveraging of value and power in today's digital economies, but also to protect them from experiencing data-based harms.

Keywords

Public understandings of data, surveillance, data doxa, governance, habit, data sharing

This article is a part of special theme on Data Associations. To see a full list of all articles in this special theme, please click here: http://journals.sagepub.com/page/bds/collections/data-associations.

Introduction

> The datafication paradigm thus performs a profound ideological role at the intersection of sociality, research, and commerce – an inextricable knot of functions that has been conspicuously under-examined (van Dijck, 2014: 201).

> '[E]nquiries into how publics engage with, configure, respond to and use big data require new ways of thinking . . .' (Michael and Lupton, 2016: 110).

This paper explores the embedding of data producing technologies in people's everyday lives and practices. It traces how repeated encounters with digital data operate to naturalise these entities, while often blindsiding their agentive properties and the ways they get implicated in processes of exploitation and governance. Notwithstanding the fact that the mass proliferation of internet-enabled digital devices has markedly transformed the social practices of actors and agencies, and contributed to the emergence of

School of Sociology, Australian National University, Australia

Corresponding author:
Gavin JD Smith, School of Sociology, Research School of Social Sciences, Australian National University, Haydon-Allen Building, Acton 2601, Australia.
Email: gavin.smith@anu.edu.au

'digital modernity' (Lyon, 2017) and 'infoglut' (Andrejevic, 2013), we still have limited concepts with which to explicate how individuals interface with, experience and make sense of what Pink et al. (2017) call 'mundane data'. In particular, few studies reflect on the affective capacities of digital data and specifically the types of subjectivation they peform in terms of enacting meanings and mentalities (Ruckenstein, 2014; Smith, 2016)[1]. Responding to this lacunae, I seek to outline an account of how digitech and data practices work to mediate relationships between body, self and society, specifically by focusing on how data get under the skin as a means of sensing and experiencing the exernal world and as biographical and reflective resources. More specifically, I am interested in theorising how the subjective experience of 'becoming with' (Haraway, 2008) digital devices and data inflects on impressions of these technologies: specifically, their increasing legitimacy, primacy and taken for grantedness.[2] I argue that the routinisation of digital devices and data use, coupled with the generalised faith and reliance that is invested in these technologies as mediums of the social, places certain constraints on users being able to engage with their complex ontologies in a critical manner. This situation is problematic in that power and capital increasingly transfer through data and yet people generally possess only a limited awareness of how data exercise influence over their lives in important, if often opaque and unseen, ways (Beer, 2017).

I wish to illustrate how digital devices and data are often utilised in ways that (a) facilitate the performance of 'social analytics' (Couldry et al., 2016) and (b) enchant the data sharing referent or analyst, progressively fixing her/his attentiveness on 'data performativity' (Matzner, 2016) in a way that obscures data-generated risks and prioritises data-based gratification. I propose and develop the notion of 'data doxa' to conceptualise the way in which digital data – and the devices and platforms that stage data – have come to be perceived in Western societies as normal, necessary and enabling. The 'data doxa' concept also accentuates the enculturation of many individuals into a data sharing habitus which frames digital technologies in simplistic terms as (a) panaceas for the problems associated with contemporary life, (b) figures of progress and convenience, and (c) mediums of knowledge, pleasure and identity.[3] Even though data sharing infrastructures evidently play a significant role in helping individuals adapt to and manage intricate events, circumstances and demands, as well as providing a means of connectivity, companionship and cognisance, a doxic relationship to them nevertheless entails the backgrounding of important systemic processes: specifically, how they are implicated in the extraction of value and the production of state, corporate and social power. It means increasing the visibility of the body/self via technologically mediated practices of self-monitoring and self-exposure as well as the prevalence of mediated voyeurism/witnessing (Andrejevic, 2004), while lessening awareness of how data, as technologies of government, structure social experiences from life chances to sentiments as a consequence of how they appear and are arranged in the building of profiles. Crucially, a doxic relationship to data also entails an obfuscation of the fact that data exist and grow independently of the subject creating, witnessing or being represented by them (Smith, 2016). Although individuals both involuntarily/voluntarily and subconsciously/consciously generate a multiplicity of digital data flows as they go about their lives, they typically wield only limited control over how those flows are generated, circulated and coded.

Drawing selectively on conceptual ideas from Georg Simmel and Pierre Bourdieu, I argue that the emergence of digital societies and the concomitant socialisation of many people into a 'datalogical' doctrine (Thornham and Cruz, 2016)[4] and data sharing habitus by organisational and cultural imperatives, has shaped the understandings they duly attribute to the data accessed and emitted from their bodies via networked devices. This doxic disposition mediates and orientates their relationalities with digital data, particularly by imbuing a relatively reductionist, utilitarian perspective of what they are and mean in terms of their being understood one dimensionally as mere artefacts to prosume. Although I acknowledge that individuals engage with digital devices and data in different ways and contexts, I nevertheless wish to suggest that the cumulative effect of data interfacing practices is the production of a doxic sensibility, whereby individuals develop a dependence on the affordances of digitech and a narrow understanding of the political economies in which data circulate as core assets (Michael and Lupton, 2016). I suggest that three types of data-based relations contribute to the formation of this doxic sensibility: *fetishisation*, *habit* and *enchantment*. Each of these relations come to mediate public understandings of digital devices and data, obscuring the multifaceted nature and hidden depths of data and their propensity to double up as technologies of exposure and discipline. As a result of this situation, imaginative educational programs and revamped regulatory frameworks are urgently needed to inform individuals about the contribution of data to the leveraging of value and power in today's digital economies, but also to protect them from experiencing data-based harms.

Data power: Governing by, with and through data

> 'Someone has my dental records. Someone has my financial records. Someone knows just about everything

> about me. You have no privacy. Get over it.' (Scott McNealy, former CEO of Sun Microsystems).[5]

A burgeoning trans-disciplinary literature now explores the manifold ways in which data-driven cultures exert growing influence over organisational decision-making and contribute to consequent processes of algorithmic governance (Beer, 2017). Critical research has examined how processes of datafication and Big Data analytics are infusing and transforming policy, professional and commercial fields such as city planning and design (e.g. Kitchin, 2014; Williamson, 2017), law enforcement, warfare and security (e.g. Chan and Bennet Moses, 2017; Harcourt, 2007, 2014; Smith and O'Malley, 2017), health (e.g. Didžiokaitė et al., 2017; Lupton, 2013; Ruckenstein and Pantzar, 2017), education and research (e.g. Procter et al., 2013; Ruppert, 2013; Williamson, 2016), marketing, journalism and consumption (e.g. Andrejevic, 2004; Lewis and Westlund, 2015; Savage and Burrows, 2007). These studies show how the increasing digital mediation and dataveillance of social relations and prominence of the 'dataism' paradigm is fundamentally reshaping how actors and agencies conduct their everyday business, ensuring that progressively more social experiences and events are now recorded, shareable, measurable, auditable and analysable as digitised texts. Dataism is becoming a widespread ideological belief – and faith – where the enlightening, emancipatory and optimising properties of digital technologies are accentuated, and where greater supply and accumulation of information is thought to reveal/refine truths relating to the operativity of the natural and social worlds (see Clough et al., 2014; Kennedy and Moss, 2015; Thornham and Cruz, 2016). As an ideology, 'Dataism presumes *trust* in the objectivity of quantified methods as well as in the *independence* and *integrity* of institutions deploying these methods – whether corporate platforms, government agencies, or academic researchers' (van Dijck, 2014: 204). A key dogma animating and warranting the mass collection and monitoring of Big Data is that 'large data sets offer a higher form of intelligence and knowledge that can generate insights that were previously impossible, with the aura of truth, objectivity, and accuracy' (boyd and Crawford, 2012: 663). Data are often framed as representational artefacts which, at scale, provide insight about the essence of diverse phenomena. They are prosumed by individuals and organisations in manifold ways both to excavate and learn about subterranean dynamics, be those bodily or social, and to manufacture and performatively express personas which guide how each is perceived. As Cheney-Lippold (2011: 167) puts it, data flows generated from techno-mediated interactivity get 'embedded and integrated within a social system whose logic, rules, and explicit functioning work to determine the new conditions of possibilities of users' lives.' This process enables powerful data orchestrators to 'conduct a constant algorithmic diagnostics of patterns of human life, and to use the insights gained from those data to derive new models, classifications and theories of both individual and social behaviours.' (Williamson, 2016: 404)

The primary (although not exclusive) instigators and beneficiaries of data-driven environments are security and profit orientated organisations, be they state agencies or businesses. Such public–private duopolies provide each of the 'invisible hands' which steer this market and shape its surrounding infrastructure and meaning. In today's knowledge economies, personal information assemblages are valuable commodities. They make 'data barons' and 'data coders' – that is, those owning and administering the socio-technical systems – such as Mark Zuckerberg not only extraordinarily wealthy but also exceptionally influential. As Joris Toonders notably put it in *Wired* magazine: 'Data in the 21st Century is like Oil in the 18th Century: an immensely, untapped valuable asset. Like oil, for those who see Data's fundamental value and learn to extract and use it there will be huge rewards.'[6] Yet, as Mark Andrejevic notes, notwithstanding the primacy that is placed by state agencies and corporate firms in data scraping and mining, and in establishing correlative patterns for making predictions and optimising processes of governing and marketing: 'we [the general public] have very little access to the forms of information collection and circulation that are taking place "behind the scenes"' (2009: 57). In this way, data afford those who retain and process them exceptional capabilities to construct and define reality, to engineer social experience in ways that evade consciousness and that bypass proper regulation:

> Every click, every like, every comment and every connection is used to build up a rich profile of each user … Facebook already uses artificial intelligence to personalise your newsfeed, identify you in photos and translate your posts … The ultimate aim is to develop algorithms that can understand the nuances of people's physical interactions.[7]

Andrejevic (2009: 47, 57) introduces the idea of the 'digital enclosure' to describe how the corporate owners of these mediums/platforms strategically convert user content into surplus value: 'This feedback becomes the property of private companies that can store, aggregate, sort and, in many cases, sell the information in the form of a database or cybernetic commodity to others'. He illustrates the ways in which data sharers become unremunerated 'feedback devices' for marketing agencies that exploit 'their free [value-generating] participation … as

a form of productive labour [that is] captured by capital' (2009, 59). In this way, the meanings and actions of individuals are reduced to the economic opportunities they afford for market colonisation and the accumulation of capital.

But it is not just the exploitive dimensions of data-driven relations that are of concern. Advertisers, law enforcers, actuaries and public servants are also engaged in widespread practices of dataveillance, scraping and intercepting information from loyalty card, fitbit, app and credit card usage without the data subject being aware, wielding such intel to target-market services and manage risks (economic, political and security). Being able to run sophisticated machinic algorithms, which both aggregate and sort vast quantities of personalised content, enables understanding of historical and 'live' social trends to occur at scale. It sets up a salient power differential between those being watched and those watching: those being subjected and reduced to an objectifying gaze and those engaged in systematic observational practices for the purposes of knowledge production and the flexing of authority (Smith, 2015). This relational asymmetry between service user and provider is epitomised in Google's advanced dataveillance system:

> Google was not simply scanning people's emails for advertising keywords, but had developed underlying technology to compile sophisticated dossiers of everyone who came through its email system. All communication was subject to deep linguistic analysis; conversations were parsed for keywords, meaning and even tone; individuals were matched to real identities using contact information stored in a user's Gmail address book; attached documents were scraped for intel – that info was then cross-referenced with previous email interactions and combined with stuff gleamed from other Google services, as well as third-party sources. (cited from Harcourt, 2014: 4)

The 'digital knowledge' culled and assembled permits 'governments, transnational corporations and everyday businesses, employers, salesmen, advertisers, the police and parole workers to track individuals' physical movements, follow their internet browsing, know what they read, what they like, what they wear, whom they communicate with, where and on what they spend their money.' (Harcourt, 2014: 7)

The leaky and liquid nature of digital traces (Bauman and Lyon, 2012), when coupled with the manifold tracking technologies which make Web traffic legible, impinge on critically contested democratic tropes such as privacy and anonymity, but also on notions like informational autonomy and self-determination. As Stalder (2002: 120) explains:

> Our physical bodies are being shadowed by an increasingly comprehensive 'data body'. However, this shadow body does more than follow us. It does also precede us. Before we arrive somewhere, we have already been measured and classified. Thus, upon arrival, we're treated according to whatever criteria have been connected to the profile that represents us.

Evidently, as individuals – qua the datafied impressions they recurrently expel as they interact with and through digital technologies – are categorically sorted in accordance with their ascribed 'risk/value' or 'waste/target' categorisation (Turow, 2011), there is ample potential for data-based, if culturally mediated, stereotyping, bias and discrimination to eventuate, but in ways that are neither obvious nor accountable (Gandy, 2006). Yet, it is not simply the unidirectional and extractive nature of the monitory process that is the problem in terms of how persons are governed through data. Indeed, in today's era of 'knowing capitalism' (Thrift, 2005), private enterprise is as much in the business of knowing as it is in the arts of persuasion, where the modulation of desire is the start and end point of affective neuromarketers. There is ample evidence which reveals how commercial actors not only capture intelligence from the 'inmates' of the digital enclosures they operate, but also exert their architectural imaginaries and powers to purposefully arrange online spaces and experiences with content designed to stimulate specific consumption practices. Platforms like Google, Amazon and Facebook have a history of successfully crafting in real time exactly what it is users see, feel and know – and thereby what it is they come to want – as they engage these markets from particular addresses, subtlety directing some to predefined materials (consider here the function of 'autocomplete') while excluding others on the basis of how each data subject has been algorithmically constituted:

> These insidious manipulations – both by Google and by third parties trying to game the system – impact how users of the search engine perceive the world, even influencing the way they vote… Then there's the secret recipe of factors that feed into the algorithm Google uses to determine a web page's importance – embedded with the biases of the humans who programmed it.[8]

This way of constructing reality, of course, is an elemental part of Google's future business plan and model: to eventually know the user – and refine the system – to the point that the requirement for the former to actually conduct content searches, or even to make choices between differing options and courses of action, is lessened.[9] This is an idealised form of orientation where

the 'smart' algorithm comes to learn and model a user's habits from historical, locative and aggregate information to the point where probable futures are mapped and customised to perceived/ascribed desires and needs.

Not only do search engines and social media platforms possess capacities for selectively filtering what is seen and known, they also function as conduits for the dissemination of what has been dubbed: 'fake news'. This capability and issue has sparked widespread fears about the vulnerability of political processes, the corruptability of knowledge, and the generalised erosion of institutional and relational trust. Key to the concern is the susceptibility of individuals to be unintentionally/intentionally conditioned and affected by what they witness online, in terms of the orientation of their beliefs, ideas, desires, emotions, and habits. Facebook, for instance, has already successfully experimented with strategies for modulating user emotions.[10] Of course, it is not simply the administrators of these sites that are engaged in processes of orchestration, a number of moral panics have also arisen in recent times with respect to a range of deviant groups – extremists, hackers and paedophiles – attempting to exploit these networked mediums to radicalise, deceive, sexualise, and victimise susceptible populations.

Aside from the weighty economic imperatives of mass dataveillance and their implications for autonomy, the 2013 Edward Snowden revelations about the National Security Agency (NSA) PRISM program drew global public attention to the political and security dimensions of state monitoring, in many ways illustrating how the three concerns effectively bleed into one another. Launched in 2007, PRISM 'allows officials to collect material including search history, the content of emails, file transfers and live chats . . . [it permits] the intelligence services direct access to the companies' servers . . . [it also] allows the NSA, the world's largest surveillance organisation, to obtain targeted communications without having to request them from the service providers and without having to obtain individual court orders.'[11] Moreover, the NSA's flagship snooping tool, XKeyscore, intercepts 'nearly everything a typical user does on the internet' in real time, including the content of emails, websites visited and searches, as well as her/his metadata. Motivated by national security and prosperity, state-sponsored dragnet apparatuses like these indiscriminately target users and mediums of the Web, effectively rendering the former into suspects and the latter into informants. Snowden highlighted the ubiquitous availability of metadata, the exceptional and discretionary nature of the powers available to security operatives, and the extent of collusion between state and corporate actors in data brokering. He accentuated the susceptibility of individuals to being profiled, hacked and harmed by corporations, states and cybercriminals as they connect to and browse the Web via digital devices, and his claims put paid to any naively held utopias of the Web as being a space that is free, anonymous and private. Perhaps even more starkly, Snowden revealed the contemporary precedence placed on hoovering up and analysing mundane data flows for the purposes of enacting government.

It is clear from this brief review that digital data have become not simply the new oil of liquid capitalism, but also the pre-eminent currency of power in today's online economies, especially as they are melded to align with particular narratives, desires and interests. Data performatively shape horizons at multiple levels and scales, from the personal to the political, and are infused with contradictory meanings as they circulate and percolate between networked performers and audiences (Smith, 2016). This takes me to the problem that I will spend the remainder of the paper addressing. Given all these ways in which data progressively figure as 'technologies of government' (in the Foucauldian sense) and are generative of manifold risks, harms and discernible power dynamics (i.e. in terms of data-based profiling, predation, exploitation, estrangement, dispossession and misrepresentation), and in light of Snowden's salient disclosures, it seems surprising that neither widespread boycotts of data sharing technologies and infrastructures have materialised nor more significant uptake of VPNs and the darknet.[12] Countless surveys indicate people generally continue to actively engage in data sharing practices on a mass scale,[13] bypassing terms and conditions sections (studies show 73% of people admit to not reading all the fine print)[14] and predominantly disregarding or misconstruing how their data flows are being put to use (Kang et al., 2015; Kennedy and Moss, 2015; Ostherr et al., 2017; Park, 2011). Indeed, recent reforms to data retention and tracking powers in Australia – where laws around data accessibility have been significantly relaxed for state agencies – have met with only very limited public opposition. Moreover, estimates by IT giant IBM suggest that 'every day, we create 2.5 quintillion bytes of data – so much that 90% of the data in the world today [have] been created in the last two years alone'.[15] van Dijck's (2014: 205) reading of this situation affords a clue that informs the subsequent analysis: 'it turns out to be very hard to escape from the rules and practices set by the dominant players in the system.' I argue that several factors explain why many people simultaneously misunderstand and depend on data in a way that cultivates what I call, 'data doxa', a sensibility that limits critical engagement with data beyond the immediate ends they serve (see Barnes, 2006; Michael and Lupton, 2016; Zureik et al., 2010). This misunderstanding of data is

epitomised in what has been termed the 'privacy paradox', where although individuals claim to value and desire privacy and anonymity, they are equally comfortable sharing personal information to garner services, rewards and what has been termed, 'attention capital' (see Andrejevic, 2009: 52). As Woo (2006: 950) notes, 'In surveys regarding privacy, most respondents answer that they are very or somewhat concerned about privacy on the internet . . . Ultimately, however, many of them are willing to sacrifice privacy on the network if they receive some material compensation for revealing their personal information, such as sample products or discount coupons.' A politics of data power needs to address these factors in nuanced and creative ways if more refined understandings and practices are to be developed and sustained.

Data doxa: Being and becoming with data

> *Digital knowledge* produces and reproduces consuming subjects who wittingly or unwittingly allow themselves to be watched, tracked, linked and predicted in a blurred amalgam of commercial and government projects. (Harcourt, 2014: 7)

The diffusion of always-on, portable, networked digital devices – like the sensor-clad smartphone – into the weave of daily relations has dramatically increased both the *connectivity* and *visibility* of their users. These datafying mediums have afforded new opportunities for individuals to interact in real/virtual time with a globally dispersed audience (of 'familiars' and 'strangers') and to access and share information about social experiences and events. It is evident that users form tactile and intimate relations with the digital devices they bear (constantly checking phones out of habit or sleeping with them under pillows), the data produced mediating performatively how the body and wider social field are consequently approached and understood. As Lupton (2016: 2) describes:

> Humans move around in data-saturated environments and can wear personalised data-generating devices on their bodies; including not only their smartphones but objects such as sensor-embedded wristbands, clothing or watches. The devices that we carry with us literally are our companions: in the case of smartphones regularly touched, fiddled with and looked at throughout the day.

In an era characterised by uncertainty, complexity, insecurity and reflexivity, where we have come to doubt the veracity of what we see, hear and feel, data perform a corroborative and evidential role, they verify and validate who and what we are, but also act as proxies on which other individuals and institutions formulate decisions. We have become utterly entangled in data, they both stimulate and embody social experiences in mediated interactions. In today's digital culture, we, to borrow Donna Haraway's (2008: 3) perceptive phrase, 'become with' data in what are relational interplays: we make them, just as they make us. Our relationship with data, therefore, is symbiont and ambiguous in character. I purposefully employ the term ambiguous, as it appears that those using digital media devices avidly participate in data sharing practices and personal/social analytics while often overlooking how, as windows onto interiority, data are appropriated by others for the acquisition of political, social and economic advantage (Andrejevic, 2009; Madden, 2014).

But from where has this popular desire for – and addictiveness to – data emerged and how might it explain public indifference to data asymmetries? Ideas sourced from Georg Simmel and Pierre Bourdieu are useful in this respect, for they provide constructive frameworks for making sense of data sharing ambiguities. Each thinker seeks to explain how external structures, be they a city street or a cultural artefact, produce internal affects in terms of their transferring logics and imprinting perspectives on those who engage them. Both Simmel and Bourdieu accentuate how spaces and objects condition people to view the world through a prism which reifies and reproduces distinctive power relations that privilege the agendas of some over others. Rather than attempt to summarise the nuances of their respective contributions, I will instead selectively apply several of their ideas to explain the seduction of agentive data generally, before analysing some of the many cultural and organisational vectors in which a doxic sensibility is enacted and perpetuated.

A key linking thread in the work of Simmel and Bourdieu is the analysis of how physical space and material culture have *embodying* qualities that permeate subjectivity in terms of the construction of identity and desire. As primary agents of socialisation, these ecologies – and all the discourses, objects, cues, and scripts they exhibit (what might be termed, 'codes') – impact on the mentalities and practices of those exposed to them. As Bourdieu (1990: 14) puts it, 'the analysis of objective structures . . . is inseparable from the analysis of the genesis, within biological individuals, of the mental structures which are to some extent the product of the incorporation of social structures'. Over time, and as a consequence of privileged elites possessing the communicative means to define the symbolic realm in accordance with their own interests and values, dominant codes become not only objectively, but also subjectively, normalised. This

process – where individuals are socialised by ideologies that teach them to misrecognise their situational interests, and to populate a belief system that reflects the interests of others – is what Bourdieu termed, 'doxa' (Bourdieu and Eagleton, 1992). Doxa refers to the taken for granted wisdoms which support the legitimacy of the status quo and render invisible or natural corresponding power dynamics/imbalances. As subjects relationally engage in fields of practice they begin to unconsciously internalise the rules and expectations to which they are exposed and then exhibit these via the patterns of activity they repeatedly perform. These practices are driven by what Bourdieu calls the 'habitus'. This is the complex set of values, beliefs, interests and tastes embodied from experiences in the surrounding historical, symbolic and material world. It is 'the way society becomes deposited in persons in the form of lasting dispositions, or trained capacities and structured propensities to think, feel and act in determinant ways, which then guide them' (Wacquant, 2005: 316).

A complementary approach to understanding the psychological effects of social space is taken up in Georg Simmel's (2010) influential essay, 'The Metropolis and Mental Life'. Simmel (2010: 103–104) contends that the ambience of the stimulus-rich city is progressively reflected in the psyches of its occupants. The fleeting impersonality of the modern city, the instrumentality of its design and money economy, and the sheer overload of sensory stimuli it accommodates functions to instil in urbanites a *blasé outlook*. This is the progressive incapacity to reflect critically on what is witnessed and experienced, and a mindset that reduces the wider sum or 'many-membered organism' of the city to the utilitarian pursuit of individual ends. As Simmel (2010: 106) puts it, 'The essence of the blasé attitude is an indifference toward the distinctions between things.' Importantly, he argues that self-seeking and sensorially-overloaded city dwellers become gradually unresponsive to the particulars of their environment, especially the experiences and suffering of others. They attune themselves to selectively blocking things out. They practice unconscious distancing and impassiveness. They embody a state of indifference as they transfer through space. That is to say, they become predominantly unquestioning and absorbed in themselves, with the implication that deeper constitutive forces/processes are necessarily backgrounded. So, how might these conceptual ideas contribute to our understanding of everyday data practices and the meanings attributed to digital technologies?

It is clear that digital technologies play a prominent social role in the lives of netizens, just as they – via their voluntary and involuntary data sharing practices – are contributing to the rapidly expanding data economy. And yet, despite the cultural fascination with and dependence on data, in the form of digitised texts, images and signals, people appear to be generally uninformed about: what data are; how they are made; what value and impacts they have; where they transfer; and how (and when) they exert influence. Similar to how the surfeit of foregrounded stimuli in the metropolis occupied and exhausted the minds of inhabitants and suppressed critical/communitarian engagement with background structural forces, the emerging 'datapolis' hardwires a blasé outlook with respect to data ontologies and processing politics. The glut of data-based media to which individuals are routinely exposed desensitises them to practices, meanings and consequences of data sharing qua Simmel, and it diverts their attention away from interrogating the power asymmetries and relations structuring the 'digital enclosure' (Andrejevic, 2009), especially in terms of how data are mined and configured as capital in accordance with commercial and political motives. In fact, I want to suggest qua Bourdieu that the field of data-driven visibility in which today's netizens participate as audiences and performers (as contributors to 'data capital') has embodying effects, fostering a participatory habitus that is predisposed to the practice of watching and the experience of being watched. Not only do people become habituated into revealing personal information as part of bureaucratic repertoires, and reliant on the data generated by digital devices to know, optimise and orientate the self, but they have also become familiar with, and attached to, data in a way that makes inquisition of them – and the wider circuitries disseminating them – difficult: in terms of how they operate and what they do. It is important to register the ways in which this data doxa, and the related data sharing habitus it animates, keeps data subjects simultaneously in the limelight (in terms of their presence) and in the dark (in terms of their understanding).

A doxic relation to data eventuates when data sharers develop a pragmatic orientation to the data they prosume, and when the holistic powers and complexities of data (as prisms that construct and distort reality) are reduced as a result of familiarity, dependency and seduction. It is where individuals learn to treat and utilise data in parochial and instrumental ways, as simply 'means to ends' (be they educational, entertainment, convenience) rather than as vital artefacts that also agentively construct and structure social experiences and environments. I will consider three principal types of data-based relations that contribute to the formation and maintenance of this sensibility: *fetishisation*, *habit* and *enchantment*. My contention is that, collectively, these relations come to entrench particular expectations of digital devices/data and orientations to data sharing.

Hynoptic data

There are many factors that account for data doxa, but few of these can be dealt with here. Instead, I will highlight some of the key social spaces, practices and experiences responsible for cultivating a generalised relation to data that is largely pragmatic and heuristic in orientation: where data are perceived as technologies of affordance rather than as technologies of government. When interpreted through the conceptual frameworks outlined above, we can begin to understand why a lack of focus is placed on the historical significance of data beyond the immediate stimulation and convenience they afford. The socialisation of 'datapolitans' (those who live with and through data) into a data-driven culture, where exposing and exposure to intimate moments and events is entirely normal and celebrated, produces a 'data inattentiveness' to amend Erving Goffman's famous portrayal of interaction rituals. This is where subjects approach and relate to data with a 'thin', as opposed to 'thick', awareness, utilising them associatively for pleasure or expediency while simultaneously learning to 'unsee' the broader *depths of data* in terms of how they operate to construct/structure the social field and thus are exploited for political and economic gain. Mutual processes of data familiarity and obliviousness occur in various organisational and cultural contexts. It is within these intersecting fields of practice, where data are used to protect, administer and stimulate persons, that digital device wielding publics are inculcated into a participatory habitus that regards data sharing, and data-based visibility, as required and desired. Collectively, they imbue a subjectivity that is congenial, and not hostile, to repertoires of watching and being watched.

Fetishisation: Inflating data

> 'If you want to replace the vagaries of intuition with something more reliable, you first need to gather data.'[16]

A key way in which data have come to be so accepted, if not valorised, is via claims that they afford a higher level of insight than human intutition, epitomised in the grandiose statement above by Quantified Self co-founder, Gary Wolf. These assertions contend that answers to historical and futurological problems lie within the data. This is particularly the case in the fields of law enforcement and national security. Indeed, the prevalent perception of rising crime rates and terror threats is a primary contributor to the data doxa. Because locally occurring events are increasingly mediated as glocal spectacles, they give rise to a cosmopolitan consciousness that is imbued with apprehension about the growing instability of the social world and order (Bauman, 2006). Daily media reports depicting in graphic detail both calculated and spontaneous acts of politically/ethnically motivated violence and detailing foiled terror plots[17] has facilitated widespread unease. Moreover, such isolated incidents – and the hysteria their amplified coverage prompts – are strategically appropriated as political opportunities for state officials to pitch vindications of need for additional powers in what is recursively presented as 'a time of crisis' (Hall et al., 2013). Publics are continuously and dramatically informed that the 'threat landscape' is increasing, exemplified here in former Australian Prime Minister Tony Abbot's 2015 national security address:

> The terrorist threat is rising at home and abroad – and it's becoming harder to combat. By any measure, the threat to Australia is worsening. The number of foreign fighters is up. The number of known sympathisers and supporters of extremism is up. The number of potential home grown terrorists is rising. The number of serious investigations continues to increase . . . Today's terrorism requires little more than a camera-phone, a knife and a victim . . . This new terrorist environment is uniquely shaped by the way that extremist ideologies can now spread online. Every single day, the Islam-ist death cult and its supporters churn out up to 100,000 social media messages in a variety of languages . . . That's the contagion that's infecting people, grooming them for terrorism.[18]

Data are portrayed by authority figures in ambiguous ways, as the motor of transnational crime and terror, but also, conversely, as the solution to these problems. The capture and analysis of data is described as being critical for safeguarding national interests and security from the imminent, kinetic and dislocated menace of radical Islamists, splintered criminal cells and paedophile rings. An example of this perspective is manifest in a 2003 US joint Senate and Congress inquiry which concluded that 'on September 11, enough relevant data was resident in existing databases' and that if 'dots had been connected' the events could have been 'exposed and stopped'. Similarly, providing evidence at a US Congressional hearing shortly after the World Trade Center attacks, IBM's federal business manager testified that 'in this war, our enemies are hiding in open and available information across a spectrum of databases.'[19]

Through these dataphilic and preemptive discourses, and those more spectacularly propagated in popular cultural shows like *CSI: Crime Scene Investigation*, data are framed as a moral and technical borderland where powerful agencies assent and coalesce, create

binary discourses of 'us' and 'them', and enact their commitment to defending sovereign borders from lurking perils through monitoring and information processing practices. A perception is duly cultivated and reified that mass dataveillance is necessary and desirable, and that as a vital source of real-time intelligence, striated data derivatives – when artfully reassembled by smart softwares – play an imperative role in minimising risks, preventing harms and saving lives. Data, in other words, are fetishised by those possessing symbolic capital and are rendered into a life or death issue: indiscriminate acquisition and analysis of personal information will serve humane and progressive ends, while letting it escape detection and inspection will spell certain catastrophe. Faced with the framing of this stark dichotomy, it is perhaps little wonder that publics, Australian in this case, are so tolerant of amendments to legislation that deregulates how data is retained and used.

This kind of political posturing is particularly observable in the hyperbolic space of counter-terrorism discourse. A deliberately exaggerated account of the 'unprecedented threats' confronting society, as we saw above, is crafted for maximum effect, at a time when the prospect of considered deliberation about proportionality and collateralism apropos data processing practices is least likely. Inflammatory language is purposefully selected and inserted into the public arena so as to ignite fervour and accrue approbation. It is no coincidence that Tony Abbott doggedly flagged the importance of Australian data retention reform in the immediate aftermath of the Sydney Lindt café siege when the public were experiencing profound shock and vulnerability:

> The cost of losing this data is an explosion in unsolved crime . . . if we want to combat crime, we need this legislation and if we don't get it, it will be a form of unilateral disarmament in the face of criminals and the price of that is very, very high indeed.[20]

Such incendiary and politically loaded statements are explicitly and strategically designed to convert discrete acts of criminality into hyper-moralised and nationalistic issues, in what Bauman (2006) calls fear-legitimation politics. They fabricate a perpetual state of emergency and atmosphere of insecurity which facilitates and legitimates consequent forms of state exceptionalism: especially in terms of power accumulation on the one hand and the reduction of civil liberties and accountability on the other. Strategies of manipulation, where facts get purposively warped and spectacular technological promises are made, are operationalised to exploit pubic sentiments of indignation, ignorance and impotency, and to render them into political capital. Emotively-charged language which accentuates an impending cataclysm at the hands of dangerous criminals is grossly distorted when one considers that the average Australian is, statistically, much more likely to experience harm on Australia's roads,[21] in Australia's homes[22] or via chronic health conditions like being overweight, than on its streets from what are comparatively rare incidents. This type of doctrinal commentary has the effect of shocking the public into compliance with what might, in other circumstances, be considered as excessive powers. At the same time as it valorises data for their postulated order maintaining virtues, it deflects attention away from state failings in foreign and national policy: their ineffectiveness at closing the gap in terms of indigenous injustices and inequality, for instance. It also diverts focus from questioning the role of society in creating the divisive conditions responsible for disaffecting, oppressing and marginalising sections of the community and prompting some to participate in acts of violence. And yet, the highly public, emotive and moralising nature of this violence makes it an easy medium to govern through: to create a climate of insecurity that justifies the appeal for more executive powers while simultaneously courting electoral favours for being seen to be tough on 'them'.

The assumed risk-reducing protections that data warehousing and dataveillence provide are presented as significantly outweighing any potential harms that might ensue from data being intentionally misused, inadvertently compromised/leaked or erroneously coded.[23] The politicised narratives that frame mass data retrieval – and deregulated access to netizenry data points (be they communication, social security, criminal or consumer records) – as being paramount to the success or otherwise of ongoing global wars on crime, terror and disease, also frame historic human rights as being secondary to the responsibilities of the state to ensure the integrity of borders in whatever way it deems most appropriate. Data are consistently represented in reductionist technical terms as the panacea for many of society's social ills. It is hard to overstate the power of these risk-accentuating governmentalities in orchestrating the meanings and hopes that publics attribute to data. They play a crucial part in citizens entrusting the state – and by virtue of this, private contractors – to manage their personal information and thereby the degree of exposure they are prepared to bear.

Habit: Repeating data

As more systems of observation become digitised and networked, so familiarity with performing visibility rituals increases. Data are used as mediums to share social experiences and construct identity but also to validate a person's credentials to distributed and 'absent present'

officials. The majority of us invite this kind of attention as we participate in modern life in ways that supplant the need for human co-presence and the presentation of cumbersome material documents. The doing of mundane tasks, like withdrawing money or logging into sites, is progressively contingent on digital interfaces and data associations which not only facilitate the action but also function as permanent virtual records of the transaction.

Thus, an ingrained conversancy with processes and experiences of data-driven visibility – as part of performing bureaucratic repertoires – is a key factor accounting for indifference to data-based governance. We organise our lives around (and through) digital devices/data, and by virtue of this proximity and the services supplied, we overlook/forget their multidimensional properties: their capacity to track and visualise us in varying ways. In ethnomethodological terms, the sheer ordinariness and utility of the data people freely transfer (although often unconsciously) render them unproblematic: they are simply a means for making (a) life feel more convenient and manageable and (b) netizens feel more connected and stimulated. As with most advanced liberal nations, the bureaucracy reigns supreme as the dominant mode of organisation in Australia. Living in this administrative ecology entails interfacing with various institutions that embrace bureaucratic values and that collate detailed informational files on our points of contact. We are continually asked to provide credentials that verify our identity, that corroborate our social stories, just as our activities are atomised and measured to establish (and audit) standards of performance and productivity. This process of supplying evidence to corroborate both a personalised and bureaucratic narrative of personhood is justified on the grounds that digital footprinting improves impartiality, transparency and efficacy in decision-making. Cumulatively, these, and many other institutional rituals taking place in educational and occupational settings, attune people to being monitored, instilling a perception that such attention is a custom that promotes procedural efficiency, increases fairness in service and delivers wellbeing.

Individuals become utterly accustomed to being seen, to *performing identity*, as they liaise with administrative organisations. They must continuously brandish identifiers in off/online spaces and have personal details recorded in a digital file that spares the requirement for lengthy processes of fact-finding and verification. This is epitomised in the arrangement of the clinic where health practitioners keep abbreviated notes on a patient's medical history, as much to accrete specialised knowledge and economise treatment practices, as to symbolically enact the impression of authority. Time-poor consumers of services are seduced by the convenience of supplying data derivatives for quicker responses and more customised products. But providing data is also made a condition of the service. One exchanges anonymity and invisibility for access to travel, education, credit and medical care. In the context of consumerism, customers are incentivised to join loyalty card schemes (which reveal their consumption preferences) in return for discounts. In this way, individuals are conditioned to reveal personal information and to display their datafied bodies at different moments and points in their day. This practice becomes part of a bureaucratically created habitus within a broader field of administrative visibility.

Given that bureaucratic instruction begins from the moment of birth – when a newborn is registered and issued with certifying digits – and continues throughout the lifecourse, especially during the individual's formative years while enrolled in school (consider class registers, ID cards, fingerprinting and performance measurements), it is difficult for the average Australian to envisage an alternative existence or future that is not permeated by flows of data and subjective experiences of visibility. As Grosz (2013: 208, 219) puts it, 'habits are how environments impact and transform the forms of life they accommodate and are themselves impacted and transformed by these forms of life . . . [Habit] signals a milieu or environment that living beings must internalize in order to live in comfort and with minimal energy expenditure – a cohesion . . . between the living being's activities and its milieu.' People become so acquainted with data sharing, with creating and showing documentation in diverse milieu, that they experience such practices as second nature. The broader roles data perform in mediating and leveraging social relations are disregarded by a practical consciousness which registers only the immediate function they afford. Moreover, the lives of those now residing on the metropolis/datapolis borderland are so busy – and comparatively prosperous – that there is scant time or motivation to deliberate on each risk in depth. The hyperpoliticised maxim, 'if you have nothing to hide, then you have nothing to fear', is passively internalised as an ideology which reifies personal convictions that those doing the dataveillance are interested in 'them', not 'us'. Of course, the deeper connotation of this aphorism is the devaluing of privacy and secrecy, and the moral discrediting of those libertarians who feel there are interiorities and personal aspects of human experience that are worth concealing from prying profilers.

Enchantment: Seductive data

> 'Through the digital world, people can attain real power to speak beyond their own biological and geographical constrains' (Lam, 2012).

The routinisation of data sharing does not only pervade the organisational field. The cultural field is another vector that institutionalises blasé attitudes toward personal information and further develops the seductions of seeing and being seen. Indeed, an additional factor that accounts for the general obliviousness to data politics is our cultural preoccupation with scopophilia and exhibitionism (Koskela, 2004), especially in an age of networked social media and reality television (Andrejevic, 2004). It would not be amiss to talk of a deeply engrained enchantment people have with the data they and others prosume, both as a medium that embodies value and represents truths to diffuse onlookers and as a means to choreograph displays of self. Data, in this sense, have become both a feature and extension of subjectivity: they facilitate experiences of storytelling, spectatorship and companionship. As noted by Lam, there has been an astonishing growth in the amount of data being freely generated as a result of the Internet of things, and our concomitant use of online search engines and forums. In this way, digital devices get embedded in our daily routines (and even in our bodies) and are experienced phenomenologically as bodily prostheses: as extensions of the body and as portals to the bordering network.

Digital infrastructures encourage and normalise data sharing (for the purposes of knowledge production and profit-making) and they frame data flows as mediums of stimulation for the sharer and viewer alike. The very architecture of social media is engineered to ingrain in users an impulse to self-reveal and to voyeuristically spectate, so that the content of consequent newsfeeds and targeted advertising can be customised to suit the niche tastes of the user in accordance with their posting practices. Interfaces are purposively designed to ensure that sharing personal content from and between mobile devices, such as uploading smartphone images or user whereabouts, is very easy to accomplish: literally at the press of a button. The following advertising slogans and official mission statements taken from Facebook, and its founder Mark Zuckerberg, embody this ideal:

> 'Be Connected. Be Discovered. Be on Facebook';[24]
> '[Facebook seeks to give] everyone the power to share all of the things that they care about . . . [sharing makes] the world more understanding, it helps people stay closer to the people who they love'.[25]

In this way, social media begins to modulate our subjectivity, our view of social reality and relations, subtly determining how and what we see, how and what we think: and ergo how we consequently use digital devices and platforms.

As a consequence of their participation in online activity, netizens are turned into both agents and subjects of surveillance as they gaze upon the intimate lives of associates on social media and as they are exposed to the remote scrutiny of those virtual audiences to whom they are digitally bound. These media are explicitly used for titillation, exhibition, direction and meaning-making. The success of reality television shows like *Big Brother* and *I'm a Celebrity . . . Get Me Out of Here*! more than demonstrate the nation's fascination with asymmetrically witnessing through a screen the intimacies, banalities, adversities and idiosyncrasies of other people's lives. And the cultural obsession with celebrity further normalises the experience of witnessing and being observed as mediated spectator/performer. As Robert van Krieken (2012) has argued, an 'economics of attention' or the ability to captivate the gaze of fickle audiences has become an important form of capital in the celebrification of society. Sharing gossip, receiving validating feedback and appearing in enviable social situations, are desirable attributes in a 24/7 newsfeed economy. Indeed, the industry of celebrity has made the personal scrutiny of prominent figures a national pastime, in the process glamorising both practices of mediated voyeurism and acts of courting mediated recognition.

Moreover, it is not merely designated experts who now systematically monitor the physical and mental dimensions/functions of bodies. Today's world is awash with digital data: data that both structure and represent aspects of human experience, from birth and social relationships to self-identity and death. Formerly closed systems of knowledge are being unfurled via the digitisation/viralisation of information and related acts of 'technoscientific citizenship' (Michael, 2007), just as previously backstage spectacles are being increasingly transferred to frontstage scaffolds for public infotainment. A browse on YouTube, for example, registers approximately 302,000 childbirth videos, 51,600 abortion procedure videos, 540,000 autopsy videos, and 115,000 videos of people who are in the process of dying. Many of these films contain highly graphic and personal content and feature the mediated bodily exposure of people in contrasting states of epiphany, liminality and vulnerability. The connectedness of spaces and netizens to technological infrastructures has resulted in a de-centralisation, a de-institutionalisation in fact, of the means of hierarchical observation and a consequent upsurge in experiences of being watched, especially by unknown and unseen lay audiences. Of course, this process has contributed to enriched public understandings of all manner of embodied conditions and historical taboos while simultaneously desensitising the subjectivities of people to *practices of exposure* and *spectacles of suffering*. A key upshot from being situated within this socio-material infrastructure and visual culture, is that people are

structurally and socially conditioned into a habitus that desires and pivots on data-based visibility, in terms of viewing and contributing content.

Conclusion

This paper has utilised the ideas of Simmel and Bourdieu to explain the structures, practices and experiences through which people develop a doxic relationship to digitech and digital data. I have argued that the development of a habitus that is disposed to watching and being watched is no accident, but is instead the cumulative outcome of a person's subjection to various systems of visibility which are embedded in the arrangements of organisational and cultural fields. Datapolitans develop the utilitarian belief that practices of data sharing and dataveillance serve useful and noble ends and they come to depend on the services, conveniences and pleasures that data afford. In everyday interactions, they are habituated into displaying tokens of trust which perform their identity as they learn, travel, work, consume and browse the net. The same individuals are continuously exposed to mediated rhetoric and spectacles, which accentuate the risks of modern life and which justify the need for more data gathering to manage these threats. They are also encouraged to perform self/other tracking as part of their participation in digital sharing economies. Via apps and social media platforms, many individuals construct and present identity, chart and compare bodily processes and exchange stories with networked audiences. Data are reflective and generative of normativities just as normativities are used to create and frame data. Each field has, for different reasons, naturalised data sharing/viewing and the desirability/inevitability of visibility, and mass exposure to digital stimuli in the online economy has made people blasé about data power and politics. One upshot of this generalised disposition is that collective action to de-legitimise and prohibit dragnet dataveillance strategies seems highly improbable.

Instead, the data doxa orientating contemporary social life in digital societies is only likely to be suspended at those points when a person's data representation comes to adversely impinge on her life: when an awareness of its liveliness is aroused, that is to say, its affective capacity to autonomously act on/against the data referent. There are numerous examples, but four immediately springing to mind are: being dismissed from employment as a result of an inadvertent and decontextualised social media post,[26] being refused travel as an outcome of appearing on a No Fly List,[27] being declined car insurance as a consequence of postal address,[28] being the victim of revenge porn where images of a sexual or intimate nature are distributed to an online forum without the referent's knowledge or consent.[29] These and other experiences might act as a catalyst for questioning ubiquitous data trails and better understanding the precise nature of the 'data-proxy': the disembodied figure that represents embodied subjects in the virtual/symbolic realm of the datapolis (Smith, 2016). But these epiphanies are predominantly individual and ephemeral in their character and effect. They are unlikely to break in any profound sense the deep enchantment that advanced liberal nations/subjects have with data, although more research focused on the subjective experience of data-based alienation and harm would be very beneficial.

Public acceptance of data capture does not stem from a devaluing or demise of privacy per se and nor does it derive from unreserved confidence in those doing the governing. It is more an effect of fear, habit, ignorance and seduction, where an increasing familiarity with and dependence on data obscures a capacity to perceive, let alone question, their broader history and probable trajectory from a critical perspective. Networked publics develop unconscious habits of data prosumption which domesticates digital surveillance devices, generating in the process a relatively uncritical and unimaginative understanding of how data might convert from asset to liability, and from text to circulation, at the behest of a pluralised audience of data brokers and inspectors. People's appetite for maintaining a virtual presence, for deriving meaning from data and for conducting their business through this medium, trumps any antithetical desire for disconnectedness and disappearance. But it is equally the case that people in today's digital societies have no choice other than to participate in the data sharing economy. We have become, to quote the CIA's Gus Hunt, 'walking sensor platforms', shedders of 'digital breadcrumbs' that attest who we are and that reveal our probable trajectories. In effect, our reliance on networked digital technologies and data flows has been determined by popular desire as much as it has been imposed by administrative design. This mutuality, and the data doxa it instigates, goes a long way in explaining public indifference to data politics. It appears that many people have a limited understanding of what data are, where and how they transfer, and how they get coded and utilised. More innovative research programs are needed to apprehend what is increasingly a multi-sited and multi-agent nodal process. But equally, greater research-based education of multiple publics is required to unsettle and decouple their doxic relationship with data, and to illustrate how their lives are structured and inscribed in multiplex ways as a result of the data they purposefully and inadvertently prosume. This extends to breaching the doxic relationship that policymakers and data scientists have with supposedly 'neutral' algorithms, by showing how

these actants often come to discriminate against specific social groups in unseen ways and leverage a determinative influence.

Declaration of conflicting interests

The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author received no financial support for the research, authorship, and/or publication of this article.

Notes

1. This focus builds on previous research by Smith and Vonthethoff (2017) which accentuates the 'addictiveness' of data prosumption in the context of self-tracking practices/cultures.
2. For the purposes of this paper, I conceptualise digital devices (like the smartphone or fitibit), infrastructures (such as Facebook, Google and the Web) and data flows (encompassing sensor-derived data, social media content and big datasets) as agentive technologies which contribute to the production of social relations and reality. That is to say, although discrete entities with their own distinct capacities and ontologies, they operate together as an assemblage, thus meanings of data are socially situated and contingent on the uses and circulations of the data. So, an individual sharing a social media feed may possess a different understanding of data to those administering the system on which that post appears, the former perceiving them as a means to connect and communicate and the latter construing them as a means to leverage insight and value. My argument is precisely that understandings of what data *are*, *mean* and *do* are contingent on where an individual is positioned, most merely experiencing the exterior façade of data as a performative technology that affords stimulation.
3. Of course, I by no means imply that data doxa is a universal, continuous or singular consciousness.
4. Given the abundance of digital data and the primacy to which they are accorded in contemporary social relations and organisation, Thornham and Cruz (2016) develop the notion of the 'datalogical' to describe the extent to which contemporary knowledges and practices are infused with data-based understandings.
5. Cited from: http://www.sfgate.com/business/onthereccord/article/On-the-Record-Scott-McNealy-2557428.php (accessed 11 May 2016).
6. Cited from: http://www.wired.com/insights/2014/07/data-new-oil-digital-economy/ (accessed 10 February 2016).
7. Cited from: https://www.theguardian.com/technology/2016/apr/23/facebook-global-takeover-f8-conference-messenger-chatbots (accessed 27 May 2016).
8. See: https://www.theguardian.com/technology/2016/dec/16/google-autocomplete-rightwing-bias-algorithm-political-propaganda (accessed 21 August 2017).
9. See: https://googleblog.blogspot.com.au/2012/08/building-search-engine-of-future-one.html (accessed 21 August 2017).
10. See: https://www.theguardian.com/technology/2014/jun/29/facebook-users-emotions-news-feeds (accessed 20 August 2017).
11. Cited from: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (accessed 24 April 2017).
12. https://metrics.torproject.org/userstats-relay-country.html/ (accessed 20 August 2017).
13. https://www.forbes.com/sites/bernardmarr/2015/09/30/big-data-20-mind-boggling-facts-everyone-must-read/ (accessed 20 August 2017).
14. http://www.bbc.com/news/business-27109000 (accessed 20 August 2017).
15. Cited from: http://www-01.ibm.com/software/data/bigdata/what-is-big-data.html (accessed 18 May 2016).
16. http://www.nytimes.com/2010/05/02/magazine/02self-measurement-t.html (accessed 13 March 2016).
17. BBC News (2015) Anzac Day terror plot: Blackburn boy sentenced to life. Available at: http://www.bbc.com/news/uk-34423984 (accessed 2 June 2016).
18. Cited from: http://www.smh.com.au/federal-politics/political-news/prime-minister-tony-abbotts-full-national-security-statement-20150223-13m2xu.html (accessed 10 August 2017).
19. Cited from: Intelligent Enterprise (2002) For Want of a Nail. 5(7): 8.
20. Cited from: https://pmtranscripts.dpmc.gov.au/release/transcript-24206 (accessed 20 August 2016).
21. https://bitre.gov.au/publications/ongoing/road_deaths_australia_annual_summaries.aspx (accessed 11 August 2016).
22. http://www.domesticviolence.com.au/pages/domestic-violence-statistics.php (accessed 11 August 2016).
23. See: https://www.theguardian.com/world/2015/mar/30/personal-details-of-world-leaders-accidentally-revealed-by-g20-organisers and https://techcrunch.com/2016/07/29/clinton-campaign-reportedly-breached-by-hackers/ (accessed 11 August 2017).
24. Cited from: https://prezi.com/6sdmahnvt6al/facebook-business-presentation/ (accessed 21 August 2016).
25. Cited from: http://www.dailymail.co.uk/news/article-3467123/The-key-world-peace-Sharing-Facebook-makes-world-understanding-says-Mark-Zuckerberg.html (accessed 21 August 2016).
26. See: http://www.huffingtonpost.com.au/entry/waitress-fired-facebook-kirsten-kelly_n_5552922 (accessed 16 August 2016).
27. See: https://www.theguardian.com/world/2014/jul/24/us-terrorism-watchlist-work-no-fly-list (accessed 20 August 2016).
28. See: http://www.dailymail.co.uk/news/article-1383317/Insurance-blacklists-The-addresses-insurers-wont-touch-disturbing-reasons-why.html (accessed 22 August 2016).
29. See: http://www.news.com.au/lifestyle/real-life/news-life/porn-sharing-site-targeting-aussie-schoolgirls-taken-down/news-story/ff7ff0b163d0311fcae6c5d8ebbdcef8 (accessed 22 August 2016).

References

Andrejevic M (2004) *Reality TV: The Work of Being Watched*. Oxford: Rowman and Littlefield.

Andrejevic M (2009) Privacy, exploitation, and the digital enclosure. *Amsterdam Law Forum* 1(4): 47–62.

Andrejevic M (2013) *Infoglut: How Too Much Information is Changing the Way We Think and Know*. Abingdon Oxon: Routledge.

Barnes SB (2006) A privacy paradox: Social networking in the United States. *First Monday* 11(9). Available at: http://first-monday.org/issues/issue11_9/barnes/index.html (accessed 20 August 2017).

Bauman Z (2006) *Liquid Fear*. Cambridge: Polity Press.

Bauman Z and Lyon D (2012) *Liquid Surveillance: A Conversation*. Cambridge: Polity Press.

Beer D (2017) The social power of algorithms. *Information, Communication & Society* 20(1): 1–13.

Bourdieu P (1990) *In Other Words: Essays Towards a Reflexive Sociology*. Redwood City, CA: Stanford University Press.

Bourdieu P and Eagleton T (1992) Doxa and common life. *New Left Review* 199: 111–121.

boyd d and Crawford K (2012) Critical questions for big data. Information, Communication & Society 15(5): 662–679.

Chan J and Bennett Moses L (2017) Making sense of Big Data For security. *British Journal of Criminolgy* 57(2): 299–319.

Cheney-Lippold J (2011) A new algorithmic identity. Soft biopolitics and the modulation of control. *Theory, Culture & Society* 28(6): 164–181.

Clough PT, Gregory K, Haber B, et al. (2014) The datalogical turn. In: Vannini P (ed.) *Non-Representational Methodologies: Re-Envisioning Research*. London: Routledge, pp. 146–164.

Couldry N, Fotopoulou A and Dickens L (2016) Real social analytics: A contribution towards a phenomenology of a digital world. *The British Journal of Sociology* 67(1): 118–137.

Didžiokaitė G, Saukko P and Greiffenhagen C (2017) The mundane experience of everyday calorie trackers: Beyond the metaphor of quantified self. *New Media & Society*. Online first publication (March 24, 2017): 1–18. DOI: 10.1177/1461444817698478 (accessed 15 August 2017).

Gandy OH (2006) Data mining, surveillance, and discrimination in the post-9/11 environment. In: Haggerty KD and Ericson RV (eds) *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press, pp. 363–384.

Grosz E (2013) Habit today: Ravaisson, Bergson, Deleuze and us. *Body & Society* 19(2/3): 217–239.

Hall S, Critcher C, Jefferson T, et al. (2013) *Policing the Crisis: Mugging, the State and Law and Order*. London: Palgrave.

Haraway D (2008) *When Species Meet*. Minneapolis, MN: University of Minnesota Press.

Harcourt BE (2007) *Against Prediction: Profiling, Policing and Punishing in an Actuarial Age*. Chicago, IL: University of Chicago Press.

Harcourt BE (2014) *Governing, exchanging, securing: Big Data and the production of digital knowledge*. Columbia Public Law Research Paper (14–390). Available at: https://ssrn.com/abstract=2443515 (accessed 23 April 2017).

Kang R, Dabbish L, Fruchter N, et al. (2015) "My Data Just Goes Everywhere:" User mental models of the internet and implications for privacy and security. In: *Symposium on Usable Privacy and Security* (SOUPS). Berkeley, CA: USENIX Association, pp. 39–52.

Kennedy H and Moss G (2015) Known or knowing publics? Social media data mining and the question of public agency. *Big Data & Society* 2(2): 1–11.

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

Koskela H (2004) Webcams, TV shows and mobile phones: Empowering exhibitionism. *Surveillance & Society* 2(2/3): 199–215.

Lam A (2012) From Arab spring to autumn rage: The dark power of social media. *The World Post*. Available at: http://www.huffingtonpost.com/andrew-lam/social-media-middle-east-protests-_b_1881827.html (accessed 20 August 2016).

Lewis SC and Westlund O (2015) Big Data and journalism. *Digital Journalism* 3(3): 447–466.

Lupton D (2013) Quantifying the body: monitoring and measuring health in the age of mHealth technologies. *Critical Public Health* 23(4): 393–403.

Lupton D (2016) Digital companion species and eating data: Implications for theorising digital data–human assemblages. *Big Data & Society* 3(1): 1–5.

Lyon D (2017) Surveillance culture: Engagement, exposure, and ethics in digital modernity. *International Journal of Communication* 11: 824–842.

Madden M (2014) Public perceptions of privacy and security in the Post-Snowden Era. Available at: http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ (accessed 19 August 2016).

Matzner T (2016) Beyond data as representation: The performativity of Big Data in surveillance. *Surveillance & Society* 14(2): 197–210.

Michael M (2007) *Technoscience and Everyday Life*. Maidenhead: Open University Press.

Michael M and Lupton D (2016) Toward a manifesto for the 'public understanding of big data'. *Public Understanding of Science* 25(1): 104–116.

Ostherr K, Borodina S, Conrad Bracken R, et al. (2017) Trust and privacy in the context of user-generated health data. *Big Data & Society* 4(1): 1–11.

Park YJ (2011) Digital literacy and privacy behavior online. *Communication Research* 40(2): 215–236.

Pink S, Sumartojo S, Lupton D and Heyes La Bond C (2017) Mundane data: The routines, contingencies and accomplishments of digital living. *Big Data & Society* 4(1): 1–12.

Procter R, Vis F and Voss A (2013) Reading the riots on Twitter: Methodological innovation for the analysis of big data. *International Journal of Social Research Methodology* 16(3): 197–214.

Ruckenstein M (2014) Visualized and interacted life: Personal analytics and engagements with data doubles. *Societies* 4(1): 68–84.

Ruckenstein M and Pantzar M (2017) Beyond the quantified self: Thematic exploration of a dataistic paradigm. *New Media & Society* 19(3): 401–418.

Ruppert E (2013) Rethinking empirical social sciences. *Dialogues in Human Geography* 3(3): 268–273.

Savage M and Burrows R (2007) The coming crisis of empirical sociology. *Sociology* 41(5): 885–899.

Simmel G (2010) The metropolis and mental life. In: Bridge G and Watson S (eds) *The Blackwell City Reader*, 2nd ed. Chichester: Blackwell, pp. 103–110.

Smith GJD (2015) *Opening the Black Box: The Work of Watching*. Abingdon Oxon: Routledge.

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

Smith GJD and O'Malley P (2017) Driving politics: Data-driven governance and resistance. *The British Journal of Criminology* 57(2): 275–298.

Smith GJD and Vonthethoff B (2017) Health by numbers? Exploring the practice and experience of datafied health. *Health Sociology Review* 26(1): 6–21.

Stalder F (2002) Opinion. privacy is not the antidote to surveillance. *Surveillance & Society* 1(1): 120–124.

Thornham H and Cruz EG (2016) Hackathons, data and discourse: Convolutions of the data (logical). *Big Data & Society* 3(2): 1–11.

Thrift N (2005) *Knowing Capitalism*. London: Sage.

Turow J (2011) *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth*. New Haven, CT: Yale University Press.

van Dijck J (2014) Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society* 12(2): 197–208.

van Krieken R (2012) *Celebrity Society*. London: Routledge.

Wacquant L (2005) Habitus. In: Becket J and Milan Z (eds) *International Encyclopedia of Economic Sociology*. London: Routledge.

Williamson B (2016) Coding the biodigital child: the biopolitics and pedagogic strategies of educational data science. *Pedagogy, Culture and Society* 24(3): 401–416.

Williamson B (2017) Computing brains: Learning algorithms and neurocomputation in the smart city. Information Communication and Soc*iety* 20(1): 81–99.

Woo J (2006) The right not to be identified: Privacy and anonymity in the interactive media environment. *New Media & Society* 8(6): 949–967.

Zureik E, Stalker LH, Smith E, et al. (2010) *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons*. Montreal and Kingston: McGill-Queen's University Press.