Surveillance & Society

Article | Social Injustice in Surveillance Capitalism

Jonathan Cinnamon

University of Exeter, UK
j.cinnamon@exeter.ac.uk

Abstract

A rapidly accelerating phase of capitalism based on asymmetrical personal data accumulation poses significant concerns for democratic societies, yet the concepts used to understand and challenge practices of dataveillance are insufficient or poorly elaborated. Against a backdrop of growing corporate power enabled by legal lethargy and the secrecy of the personal data industry, this paper makes explicit how the practices inherent to what Shoshana Zuboff calls 'surveillance capitalism' are threats to social justice, based on the normative principle that they prevent parity of participation in social life. This paper draws on Nancy Fraser's theory of 'abnormal justice' to characterize the separation of people from their personal data and its accumulation by corporations as an economic injustice of maldistribution. This initial injustice is also the key mechanism by which further opaque but significant forms of injustice are enabled in surveillance capitalism—sociocultural misrecognition which occurs when personal data are algorithmically processed and subject to categorization, and political misrepresentation which renders people democratically voiceless, unable to challenge misuses of their data. In situating corporate dataveillance practices as a threat to social justice, this paper calls for more explicit conceptual development of the social harms of asymmetrical personal data accumulation and analytics, and more hopefully, attention to the requirements needed to recast personal data as an agent of equality rather than oppression.

Introduction

> The most precious commodity we have now is the few years of lead-time before this problem grows beyond our capacity for control. If we act now, and act wisely, we can balance the conflicting demands in the area of data surveillance in [the] tradition of democratic, rational solutions. (Westin 1967: 537)

> Surveillance capitalists have skillfully exploited a lag in social evolution as the rapid development of their abilities to surveil for profit outrun public understanding and the eventual development of law and regulation that it produces. (Zuboff 2015: 83)

The contemporary digital platforms of the Web, retail and e-commerce, mobile telecommunications, and smart infrastructure systems produce vast amounts of detailed data about users—their preferences as consumers, their spatial and temporal patterns and behaviours, their hopes, beliefs, and desires. Huge economic value is generated for the corporations that control these digital architectures since the data are produced without financial compensation to users, but even more so because these data enable competitive advantage and can also be sold on to the rapidly growing personal data marketplace. The use of personal data in advertising, strategic marketing, and client management is nothing new (see Curry 1997; Gandy

Cinnamon, Jonathan. 2017. Social Injustice in Surveillance Capitalism. *Surveillance & Society* 15(5): 609-625.
http://library.queensu.ca/ojs/index.php/surveillance-and-society/index | ISSN: 1477-7487

1993), however a new era of personal data analytics is upon us, defined by a new logic of accumulation that Shoshana Zuboff (2015) has called *surveillance capitalism* which marks a sharp divergence from neoliberal ideas about the market as inherently unknowable. Indeed, perhaps the foremost principle of big data analytics is that every actor, event, and transaction can be made visible and calculable. Knowability and visibility in surveillance capitalism is wildly asymmetrical however; power is sharply concentrated in the hands of the small number of Web companies, retailers, and data brokers "built on the economics of personal data" (World Economic Forum 2011: 7) who undertake "*unexpected and illegible mechanisms of extraction and control that exile persons from their own behavior*" (Zuboff 2015: 85, italics added). The unanticipated acceleration of personal data analytics as a core economic strategy does however belie the significant longstanding concern about increasing processes of 'dataveillance' (Clarke 1988), long recognized by surveillance scholars as a primary mechanism for social manipulation and control in the information age. Yet, as the opening quote couplet illustrates, early warnings about the harms of dataveillance at the dawn of the information age have thus far failed to result in sufficient public awareness or the development of satisfactory laws and regulations to counter the threats posed by a new era of capitalism fuelled by personal data. Contributing to this failure has been the inadequate development of conceptual frameworks with which to understand corporate dataveillance practices. This paper draws on normative political theory to demonstrate how these practices are specifically threats to social justice, towards an expanded conceptual vocabulary for challenging the range of potential harms that can occur when people and their data are separated.[1]

The rapid acceleration of surveillance capitalism has been enabled by exploitative agreements between data subjects and controllers—what Peacock (2014) has called 'unconscionable contracts'—in which the data subjects have no ability to negotiate the terms of the agreement and often insufficient knowledge of the full extent or legalities of personal data collection and use (Degli Esposti 2014; van Dijck 2014; Hoofnagle et al. 2010). Yet, the ability for surveillance capitalists to accumulate and profit from personal data is well-defined in a legal sense, enacted via cryptically written end user license agreements and hard-to-find 'data privacy' and 'data protection' policies typically designed to do just the opposite—provide a legal basis for separating users from their personal data (Nissenbaum 2010; Tene and Polonetsky 2012). The user action of ticking a box is taken as consent for the company to do what it wants with personal data, which generally means stockpiling and selling it on to data brokers, the shadowy and under-regulated third party (Crawford 2014) characterized in a report by the United States Senate as a "multi-billion dollar industry that largely operates hidden from consumer view" (2013: i).

Public knowledge and concern about threats to privacy and data security are growing however. In the US, due to the Snowden revelations of domestic state surveillance by the National Security Agency (NSA) in particular, and compounded by high profile online data breaches at banks, websites, retailers, and health insurance companies, a recent report found that the public "have exceedingly low levels of confidence in the privacy and security of the records that are maintained by a variety of institutions in the digital age" (Madden and Rainie 2015: 3). Growing public concern was further confirmed by another recent study in the US which identified a 'privacy tradeoff fallacy' that runs counter to the widely cited claim that people are happy to give up their personal data in exchange for perceived benefits, when in reality there is deep concern about the erosion of privacy (Turow et al. 2015). Privacy is an internationally protected human right, providing a foundation for freedoms such as speech and association, and is thus a unifying narrative

[1] The term 'separated' is used here following the work of Andrejevic (2014) and others, despite not being strictly accurate. At least in principle, digital data are a non-excludable, non-rivalrous good that anyone could potentially profit from and which can be copied and shared without actually 'separating' it from anyone else. Under conditions of surveillance capitalism however, the ability to restrict data subjects from ever coming into contact with the data they produce and to control who accesses it in the data marketplace does effectively render personal data as an excludable good, one which is increasingly conceptualized as having a tangible materiality, following Kitchin (2014), Wilson (2011), and others, as well as the interpretation of section 215 of the US Patriot Act, which justified collection of personal telephone records as 'tangible things' (Madden and Rainie 2015).

in democratic societies and a key concept invoked to challenge escalating practices of dataveillance. And while being subject to state surveillance or a victim of identity theft are clearly threats to privacy, a growing consensus is emerging in both Surveillance Studies and big data studies—characterizing dataveillance practices in terms of privacy infringements is insufficient, and it provides a distraction from other serious social harms that can occur when people and their data are separated (see Newman 2015; Lyon 2003a; Crawford 2014; Stalder 2002; Lyon 2007; Zuboff 2016; Dwork and Mulligan 2013; Andrejevic 2014; Matzner 2014).

As Zuboff (2016: 2) articulates:

> We've entered virgin territory here. The assault on behavioral data is so sweeping that it can no longer be circumscribed by the concept of privacy and its contests. This is a different kind of challenge now, one that threatens the existential and political canon of the modern liberal order defined by principles of self-determination that have been centuries, even millennia, in the making. I am thinking of matters that include, but are not limited to, the sanctity of the individual and the ideals of social equality; the development of identity, autonomy, and moral reasoning; the integrity of contract, the freedom that accrues to the making and fulfilling of promises; norms and rules of collective agreement; the functions of market democracy; the political integrity of societies; and the future of democratic sovereignty.

In addition to privacy harms, corporate personal data practices also threaten a diverse range of intersecting values and rights including autonomy, fairness, equality, democratic sovereignty, due process, and property (Barocas and Nissenbaum 2014; Zuboff 2016), and so an expanded conceptual terrain may prove to be useful for understanding and challenging these practices.[2] Dwork and Mulligan (2013: 38) ask, "[i]f privacy and transparency are not the panacea to the risks posed by big data, what is?" Framing the social harms using the concepts and grammars of social justice may be particularly valuable, as the unequal, oppressive, and discriminatory impacts of surveillance capitalism become apparent (e.g., Andrejevic 2014; Barocas 2014). Surprisingly, however, there has been little attention to the extensive and evolving body of justice theory from moral and political philosophy and how it might be instructive in this context. When the language of social justice is invoked, the concept is typically taken for granted—the specific mechanisms and forms of injustice are not clearly articulated, which weakens the claims being made about the social harms of dataveillance.

Against a backdrop of accelerating surveillance capitalism and inadequate conceptual frameworks to understand and challenge it, this article considers corporate personal data practices within a normative theory of justice. Nancy Fraser's theory of 'abnormal justice' (2008, 2009, 2010) is used here to make explicit how three core data practices fundamental to the project of surveillance capitalism can be considered unjust, based on the normative principle that they impair *parity of participation in social life*. After first introducing Fraser's framework, the paper traces how personal data accumulation by surveillance capitalists is not only an economic injustice of maldistribution, it is also the key mechanism by which two further, more opaque forms of injustice are made possible. The initial injustice of personal data maldistribution can lead to sociocultural misrecognition, which occurs when personal data are subject

[2] See Bennett (2011) for a 'defence of privacy'. He provides a useful review of advancements in academic privacy theory since Warren and Brandeis' (1890) formulation 'the right to be let alone', a conceptualization that has strongly influenced the public's perception of privacy, as well as those of legal systems which tend to more easily recognize 'traditional' privacy concerns such as spatial intrusions, disclosure of secrets, and distortion (spread of misinformation about a person) (Solove 2006). In particular, Solove's (2006) hierarchical taxonomy of privacy harms and Nissenbaum's (2010) concept of 'contextual integrity' may prove to strengthen the relevance of privacy as a concept in this context as these ideas filter down into public and legal discourses.

to algorithmic processing and classification, as well as political misrepresentation, which renders people voiceless to challenge any misuse of their personal data. In identifying the injustices of specific practices inherent to the current mode of capital accumulation, the paper calls for more explicit conceptual development of the social impacts of dataveillance, and briefly attends to the requirements needed to intervene in these practices, which could help to reconfigure personal data as an agent of social equality rather than oppression.

From distributive justice to abnormal justice

Although varied in aim and approach, social justice struggles fundamentally seek to achieve social equality by overturning social oppression, which occurs when a social group exploits another for its own gain, whether consciously or not (Bonnycastle 2011). Many social divides exist in society; social justice is about identifying and redressing those that are oppressive—and therefore unjust—through democratic action aimed at achieving social equality. In the continual efforts to challenge unjust divisions between individuals and groups in society, the concept of *distribution* is central to the construction of social justice claims—indeed, social justice and distributive justice are terms that are often used interchangeably, as illustrated by the United Nation's assertion that "social justice [is] the equivalent of distributive justice" (UN Department of Social and Economic Affairs 2006: 13). The characterization of distribution as a core concern of social justice is common in political philosophy, the social sciences, and society more generally, notably influenced in recent decades by John Rawls' (1971) *A Theory of Justice.* Distributive justice centres on the allocation of what Rawls calls 'primary goods' in society including wealth, resources, rights, and liberties. According to this utilitarian perspective, justice will be achieved when the worst off in society are the greatest beneficiaries of distributive reparations, whether that is the allocation of rights, freedoms, or economic resources. In practice however, recognized material goods with obvious social and economic value—especially privately held goods such as money or commodities—are more probable targets of distributive justice struggles than esoteric or abstract 'goods' (Miller 1999; Bonnycastle 2011). There is no undisputed list of what is considered a primary good, but rather, there is a "moveable boundary between justice-relevant and justice-irrelevant goods," which varies depending on—amongst other things—"the degree of consensus that can be reached about the value of particular goods" (Miller 1999: 11). Distributive justice struggles, then, are likely to change over time as society values, revalues, and devalues various goods in accordance with broader social and economic shifts.

In the new era of surveillance capitalism, the challenge of considering data as an economic and social good and therefore a potential target of distributive social justice redress is relatively uncomplicated, especially given the big claims about big data. Described as the 'industrial revolution of data', the 'new oil', or the 'new raw material of the information age', data are becoming firmly ensconced alongside other resources within structures of capital accumulation. As Mayer-Schönberger and Cukier (2013: 15-16) put it, data are "becoming a significant corporate asset, a vital economic input, and the foundation of new business models. … Though data is rarely recorded on corporate balance sheets, this is probably just a question of time." A small amount of attention has been paid to personal data from the specific standpoint of justice theory, focusing primarily on questions of access and distribution from a Rawlsian perspective (see Van den Hoven and Rooksby 2008; Duff 2006; Britz 2004; Nagenborg 2009), however a narrow focus on data redistribution runs the risk of crowding out other harmful effects of dataveillance that are ontologically different from questions of distribution across the social spectrum.

I argue here that Nancy Fraser's recently extended theory of 'abnormal justice' provides a particularly useful set of conceptual tools for thinking about corporate personal data practices as a topic of social justice, because it is based on but also expands beyond the issue of access and distribution. Borrowing from Kuhn (1962) and Rorty (1979), Fraser (2008, 2009, 2010) argues that we are now living in a time of 'abnormal justice' in which the 'what', the 'who', and the 'how' of justice are deeply contested. This is contrasted with conditions of 'normal justice', a state of general agreement amongst all parties about the

basic ontological structure and assumptions of justice. Under conditions of normal justice, disputants have shared presuppositions about the substantive questions of justice, a common terminology and grammar, and an equivalent understanding of how a justice process might proceed. Under the current conditions of abnormal justice, as Fraser (2008: 395) describes, "[t]oday's disputants often lack any shared understanding" of what justice claimants can look like (individuals or groups, fellow citizens or all human beings), the substantive focus of justice claims (economic redistribution only, or other ontologically different forms of redress), which social divides possess injustice (e.g., nationality, ethnicity, class, gender, sexuality), and the agencies and scales of arbitration and redress (state or non-state actors, territorial or supraterritorial bodies).

Under these circumstances, a conceptual framework that could 'do justice' to conditions of abnormal justice may seem improbable, since, as Fraser argues, familiar theories "fail to provide the conceptual resources" to do so (2008: 396-397). As the first step in constructing such a theory, Fraser starts by embracing both the positive and negative sides of abnormal justice. Although it may be difficult to see anything positive to be taken from the seemingly dysfunctional climate of justice sketched above, the upshot of this ontological instability is the provision of a foundation for an expanded and diversified field of contestation. Fraser suggests that decentring the erstwhile 'what' of justice—redistribution—enables non-economic forms of injustice to be rendered visible, providing the possibility of broader, multivalent understandings of justice. The problem with abnormal justice, however, is that a stable framework is required to enable diverse justice claims to be recognized and addressed, but when the 'what', 'who' and 'how' are in dispute, overcoming injustice is immensely more challenging compared to conditions of normal justice. Her suggestion here is to submit all justice claims to the normative principle of *parity of participation*, based on the basic idea that "*justice requires social arrangements that permit all to participate as peers in social life*" (2008: 405, italics added). 'Embracing the normative' is a necessary move here in order to be able to identify what a socially just world would actually look like (Olson and Sayer 2009). This understanding of justice provides the basis for recognizing heterogeneous justice claims and the means to overcome injustice through the identification and removal of the obstacles that prevent some individuals and groups from participating as equals in social life. In short, any justice claims that promote parity of participation can be morally justified.

Fraser considers three obstacles to parity of participation that can serve as focal points for social justice struggle. The first obstacle, *maldistribution*, is the familiar issue of class inequality and distributive injustice that deny some people the ability to participate equally in social life due to lack of resources. The second obstacle, *misrecognition*, occurs when institutionalized hierarchies afford some citizens or groups a higher status in society at the expense of others, which results in inequality and an inability to shape one's own identity. The third obstacle, *misrepresentation*, occurs when political subjects are not able to control their own representation or when the political constitution of society is arranged in such a way as to produce voiceless subjects unable to access democratic institutions or the means of social redress in an equitable way. These three types of obstacles to parity of participation are key components of Fraser's theory of abnormal justice and are a useful set of concepts for characterizing an emerging issue of justice in abnormal times: the accumulation and analysis of personal data by corporations.

Personal data and parity of participation

In some contexts, as Fraser (2008) argues, "public debates about justice assume the guise of normal discourse. However fiercely they disagree about what exactly justice requires in a given case, the contestants share some underlying presuppositions about what an intelligible justice claim looks like" (393). Given the rapid and unexpected rise and the opacity surrounding its implications for individuals and society, any talk of social justice in the context of surveillance capitalism is unlikely to be one of those situations. Considering justice within Fraser's tripartite framework under the overarching principle of parity of participation opens the door towards a broader, more detailed understanding of the range of

injustices that can occur under conditions of surveillance capitalism. Against a backdrop of abnormal discourse surrounding personal data, the remainder of this section outlines the processes and mechanisms by which the initial injustice of personal data maldistribution provides the basis for further social injustices of misrecognition and misrepresentation to take place.

Maldistribution and personal data: Asymmetrical accumulation

Beyond the growing concerns about state surveillance or the loss of sensitive personal details in data breaches, the inability of data subjects to access their personal data creates significant injustices of maldistribution in which corporations are able to accumulate vast stockpiles of economically valuable personal data, enabled by strategies of dispossession which obfuscate the digital realm's materiality (see Kinsley 2014). Web companies have crafted the internet 'cloud' imaginary as a liminal space between the user and the website, a gap between the real and the virtual (Hu 2015), which has encouraged both confusion and public apathy towards the accumulation of personal data by private companies. Personal data are actually diverted to very earthly data centres—massive, industrial-sized operations not unlike the NSA's data storage facilities (Lyon 2014). Contra the 'cloud', Andrejevic (2007) has proposed an alternative spatial imaginary, the 'digital enclosure', which can be applied here to illustrate how preventing people from accessing their personal data through processes of accumulation by dispossession (Harvey 2003) parallels the primitive accumulation of the land enclosure movements that separated the producers from the means of production (see also Thatcher et al. 2016).

What, then, is the economic value of personal data that users are giving up? Critiquing Fuchs' (2010) analysis of user exploitation online, Arvidsson and Colleoni (2012) claim that value creation on social media cannot be considered according to the classic Marxist theory of labour because the value produced by users is purely 'affective' (i.e., users create content for platforms they are interested in, based on things such as buzz, brand recognition, and reputation) and because it is realized on financial rather than commodity markets. Yet what this assessment overlooks is the enormous economic value of data produced by users and sold on by the platforms to the personal data market. This is perhaps a paradigmatic example of alienation in the Marxian sense of labourers not being able to enjoy the fruits of their labours (Andrejevic 2015)—in this case, one's own data about who they are, what they do and like, and where they live, work, and play. Unfortunately, the secrecy of the personal data industry has thus far prevented any detailed analysis of the economic value of personal data, however a sense of what is at stake can be inferred. Attempting to estimate the value to an individual of all of their personal data is particularly challenging, although the example of Facebook's initial public offering (IPO) provides a hint. As Mayer-Schönberger and Cukier describe (2013), Facebook's market valuation at the time of their IPO in 2012 was $104 billion, yet they claimed assets of just $6.3 billion. Facebook had not put a value on their 2.1 trillion pieces of monetizable content—personal data produced by their users—and if we attribute this disparity to these unlisted data assets, the value of this content is about 5 cents per data point or around $100 per user (although certainly some of this disparity between valuation and earnings must also be attributed to Facebook's affective value). If one were to extrapolate this figure to all of their social media activity, retail purchasing, and Web surfing, the significant economic value of their personal data resources would grow substantially. Average Revenue Per User (ARPU), a metric used to assess how well a platform monetizes its users, also provides a hint at the value of personal data to the user; Google for example regularly obtains an ARPU value over $40 per financial quarter (Garner 2015). Datacoup, one of a number of startups that are attempting to develop a business model that pays people directly for their personal data, offered each user up to $8 per person per month in 2014 (Simonite 2014). This is certainly a rough estimation as to what one's personal data might be worth to data brokers, but the future reuse value of the data is not accounted for—i.e., what the data brokers then receive for aggregating and (re)selling it to the marketers, credit lenders, and insurance companies. Again, calculating the value of a person's data to data brokers is impeded by the secrecy of the industry—indeed some data brokers have outright refused to comply with government requests for information on data practices (United States Senate 2013)—however aggregate figures are insightful. The US data broker industry was estimated to generate over

$150 billion in revenues in 2012, and Acxiom, a major player which claims to have an average of 1500 data points for each of the 700 million people worldwide in its database, made a profit of $1.1 billion in 2013 (see Roderick 2014).

In any case, the economic value of personal data is largely realized in the aggregate—patterns and future potential become visible when data points are linked together through data analytics and algorithmic processing (Thatcher et al. 2016). Here, Fraser's claim that the 'who' of justice—e.g., individuals or groups—is also disputed in abnormal times is clearly relevant to the special case of personal data; surveillance capitalism feeds on individuals but its target is automatically-generated groupings of people based on behavioural attributes and propensities. Personal data analytics produces virtual representations of us—what Haggerty and Ericson (2000) have called 'data doubles'—yet as Cohen (2017: 14) describes, its "purpose is to make human behaviors and preferences calculable, predictable, and profitable *in aggregate*." The separation of people from their data—the dominant situation in the new landscape of personal data in which one's data is unlikely to ever have been in one's possession (President's Council of Advisors on Science and Technology 2014)—is a clear obstacle to parity of participation and therefore an injustice. Yet, as the following section explains, the corporate dataveillance practices that result in personal data maldistribution are also the key mechanism by which a further form of social injustice is made possible: misrecognition, or status inequality.

Misrecognition and personal data: Algorithmic subjectivities

Fraser describes how injustices of misrecognition are manifest in sociocultural hierarchies that privilege some individuals and groups over others, preventing some from attaining full parity of participation in society. Maldistribution and misrecognition are thus closely entwined (Carmalt 2011); uneven access to economic and social goods contributes to the production of unjust status inequalities. In the case of personal data, the division of society into three 'data-classes'; those who create data, those who collect data, and those who can analyze data (Manovich 2012; Andrejevic 2014), has serious implications that go beyond economic injustices of maldistribution. Comprising the third data-class is a very select group with the technical expertise to engage in personal data analysis. Although computer coding and data analytics have always been rarefied domains, the rapid rise of big data along with the development of new tools and algorithms to handle massive unstructured datasets has shrunk it drastically (see Davenport and Patil 2012). However, the data-class status hierarchy has more serious societal consequences than just the ability to access data and benefit from data analytics—relinquishing access to our data also gives up a degree of control over our lives as we are increasingly subject to classification and profiling (Ohm 2014). These activities threaten our ability to realize an 'undistorted identity' (Zurn 2003), leading to injustices of misrecognition.

Significant public anxiety about identity theft, such as when credit card or personal health details are taken by hackers in data breaches, has thus far not been accompanied by a similar awareness or concern about analogous processes of misidentification and subjectification that occur when personal data are subject to automated analytics and classification, what might be referred to as *algorithmic identity theft*. Yet, personal data analytics could also threaten self-determination and identification, due to the narrowing of choice through the 'filter bubble' phenomenon, but perhaps more problematically through highly opaque practices of automated group classification, which can lead to sociocultural discrimination (Tene and Polonetsky 2012; Andrejevic 2014; boyd and Crawford 2012; Pasquale 2015). Big data algorithms and data mining are fundamentally about discrimination (see Barocas 2014); their purpose is to separate society into groups through identifying patterns of difference and sameness—or norms and deviations from them (Amoore 2009)—in vast datasets through processes of data reduction and categorization. These processes can simplify a complex world—or a complex data stream—however in doing so they also enact and constrain the world; they reduce difference and narrow possibilities for action (Bowker and Star 2000; Hacking 1982). Big data analytics also generally lack statistical certainty; correlations are the evidence of big data, but their value for decision making is highly suspect, as Zwitter (2014: 5) notes, "[b]ig data

makes random connectedness on the basis of random commonalities extremely likely. In fact, no connectedness at all would be the outlier." When personal data are algorithmically processed to predict future behaviours and events, the people represented by the data are therefore subjected to the material effects of discriminatory or inaccurate classification (Graham and Wood 2003; Lyon 2003b). This shapes "who we are before we make up our own minds" (Richards and King 2014: 396) and creates or further entrenches our sociocultural hierarchies (Tene and Polonetsky 2012). Yet, in the rulebook of surveillance capitalism, inaccuracies that might affect an individual are only problematic insofar as they are ineffective at accurately predicting patterns and behaviours. As Cohen (2017: 14) describes "[a]s long as [the] project is effective on its own terms—an outcome that can be measured in hit rates or revenue increments—partial (or even complete) misalignments at the individual level are irrelevant."

Data mining and automated analytics are problematic for data subjects because of poor design, bad data, and dubious inference, however algorithms are also *purposefully* developed to enable companies to engage in illegal forms of discrimination, by using proxy datasets to hide oppressive practices (Ohm 2014). For instance, while it is illegal to discriminate against potential property renters based on their racial background or socio-demographic characteristics, algorithms can be designed that intentionally avoid advertising on social media platforms to users from deemed undesirable backgrounds or statuses, which can be inferred from analysis of their Web activities, such as their 'likes' on Facebook (Crawford and Schultz 2014). A range of discriminatory practices are being conducted via algorithmic processing of personal data, including differential pricing by retailers, predatory lending to vulnerable groups, racial profiling, and higher life insurance rates for those suspected of having a disease (Rieke et al. 2015).

The emergence of a 'scored society' (Citron and Pasquale 2014) is a powerful example of how data maldistribution and its algorithmic processing can lead to further injustices of misrecognition. Credit scores shape our identity and status in society—they can determine our financial and material circumstances, however it is estimated that up to 25 per cent of credit scores have serious inaccuracies, including the misattribution of debts and the mixing up of files due to weak matching criteria that cannot distinguish between people with similar names or identity numbers (Wu 2009). As part of an emerging so-called 'alternative data' industry, new sources of personal data gleaned from online activities and social media are now used to calculate a form of credit score for the 'underbanked', however relying on the vagaries of one's online identity can produce serious inaccuracies that wrongly shape a person's creditworthiness (Yu et al. 2014). Automated approaches are now deployed to develop entirely new forms of personal scores, drawing on publicly available datasets combined with personal data held by retailers and data brokers. For instance Versium's LifeData® database, made up of over 800 billion personal attributes, is used to calculate a range of proprietary and bespoke predictive scores including the 'Fraud Score', ID Risk Score', and 'Churn Score' (Versium Analytics 2016) for clients wishing to further categorize people according to their predicted future behaviours and outcomes (Dixon and Gellman 2014). The data and calculation parameters used in these scores are opaque, and, unlike credit scores, they are largely unregulated and unknown to the public (Dixon and Gellman 2014). Inability to secure a loan, mortgage, job, or health insurance due to inaccurate placement in a 'risk' category is clearly unfair, however the accuracy of the classification is perhaps unimportant in the context of social justice—accurate or not, personal scoring systems 'make up people' (Hacking 1999); they produce new social categories of difference and restrict our ability to shape our own sense of self, a clear threat to parity of participation in social life.

While these new personal scores operate largely invisibly, the Chinese government is currently implementing an intentionally visible 'social credit system', which may act as a warning to policymakers about the potential threats to social justice from unfettered development of new personal data scoring or classification systems. By 2020 all Chinese citizens will have a personal score calculated from data not only related to financial standing but also a range of social and behavioural factors including criminal or political activities, driving records, and job evaluations (China Copyright and Media 2015; Hodson 2015).

The aim is to encourage positive economic and moral behaviours (Kshetri 2016), in order to "ensure that sincerity and trustworthiness become conscious norms of action among all the people" (China Copyright and Media 2015). In parallel, and with government backing, China's internet oligopoly is also developing scoring systems based on personal data produced online, including data from Alibaba's e-commerce sites, Baidu's search engine, and Tencent's communications and social media platforms. It is expected that these scoring systems will be fed into the state's social credit system for anyone to assess the 'sincerity and trustworthiness' of anyone else, such as potential job applicants, intimate partners, or neighbours (the initial version searchable by person or business name is now online at http://www.creditchina.gov.cn/) (Fan 2015). Moreover, it is expected that scores will be derived not only from one's own personal data but also those of people they associate with, online and offline, meaning that all the activities and behaviours that take place within one's family and social network deemed to be undesirable, such as extravagant spending or criticizing the Communist Party on social media, will count against their own score (see Kshetri 2016). Thus, Chinese citizens are facing a future in which their identity and social status will become increasingly externally shaped—through algorithmic processing of their own personal data and through the actions and behaviours of their friends and family—rather than intersubjectively through equitable social relations of recognition (Zurn 2003: 519).

Misrepresentation and personal data: Extraterritorial accumulation

As explained above, injustices of personal data maldistribution are enabling further, significant injustices of sociocultural misrecognition via algorithmic data processing, classification, and predictive analytics. The initial injustice of maldistribution is, however, also leading to further injustices of misrepresentation, described by Fraser as political voicelessness, which render some individuals and groups unable to engage as peers in democratic society. When this occurs within a jurisdictional frame, this can be referred to as 'ordinary-political misrepresentation' (Fraser 2008). In the case of data related injustices, this is exemplified by censuses and large scale surveys that typically undercount minorities, the socioeconomically marginalized, and the homeless, leading to inadequate political representation for these groups and further marginalization.

An important aspect of Fraser's third arm of her justice framework however, and the focus here, exposes *meta-political injustices* which "arise when a polity's boundaries are drawn in such a way as to wrongly exclude some people from the chance to participate *at all* in its authorized contests over justice" (Fraser 2010: 286, italics in original). With processes of globalization now deeply embedded, the demarcation of space according to jurisdictional boundaries inadequately reflects contemporary sociopolitical subjectivities and relations of governance. Contributing to this is the continued rise of the global internet, which is entrenching territorial mismatches between governance structures and subjects, preventing some citizens from accessing the democratic system. Under these conditions, the 'who' of justice becomes even more murky, leading to a particular type of socio-spatial misrepresentation Fraser calls *misframing*. This meta-level injustice prevents first-level injustices of maldistribution, misrecognition, and ordinary-political misrepresentation from being heard. As a concept, misframing enables political space itself to be interrogated from a justice standpoint (Fraser 2009).

In the age of surveillance capitalism, the accumulation of personal data is perhaps a definitive example of the injustice of misframing. The ability to challenge forces that oppress you through formal institutionalized processes is a fundamental condition of democracy, however the separation of people from their data is eroding that possibility. The territoriality of personal data accumulation means that if you live outside of the data centre's political jurisdiction, it is likely that a foreign entity is controlling your data, which means that you will be severely restricted from making a justice claim regarding access, the ways your data are used, or how it represents you.

Douez v. Facebook, Inc., a class-action lawsuit initiated in 2014 in British Columbia (BC), Canada, is illustrative. As Rose (2015) describes, the lawsuit was brought by a BC resident to the courts in that

jurisdiction to contest Facebook's 'Sponsored Stories', a feature that utilized the name and image of users to advertise products in their Facebook friends' newsfeeds. Fuelled by a successful challenge against Sponsored Stories in California in 2012 (Constine 2012), the lawsuit cited the *BC Privacy Act*, which prevents a person's name or likeness being used for advertising purposes without their consent. Although the case was initially cleared by the courts to go forward in 2015, Facebook appealed and it was quickly struck down because it "failed to give effect to the principle of territoriality" which states that "B.C. law applies only in B.C." (Court of Appeal for British Columbia 2015). Facebook's successful appeal rested on its carefully worded 'forum selection clause' in their terms of service, which stated that "[y]ou will resolve any claim, cause of action or dispute (claim) you have with us arising out of or relating to this Statement or Facebook exclusively in a state or federal court located in Santa Clara County, [California]," despite *s.4* of the BC Privacy Act stating that "[d]espite anything contained in another Act, an action under this Act must be heard and determined by the [BC] Supreme Court" (Court of Appeal for British Columbia 2015).

Privileging the forum selection clauses of a foreign entity over local laws thus provides a legal precedent for dismissing extraterritorial claims against personal data injustices. In the case of these claims in British Columbia, this ruling thus renders the BC Privacy Act unable to protect its citizens from uses of their personal data deemed illegal under local legislation, and the plaintiff would now have to attempt to challenge this injustice in a California court, a prospect unlikely to happen in this and many cases. For Facebook, this is a significant decision, as a vast majority of their approximately 1.8 billion monthly-active users do not reside in the United States (Facebook 2017), and therefore are effectively cut off from making claims against the company. The placement of Facebook's European headquarters in Ireland similarly acts as a barrier to democratic action against the company by users in other parts of that continent. Facebook has insisted that it is only subject to Irish jurisdiction rather than those of the European Union or its member states, which enables the company to avoid more stringent data protection in other jurisdictions—notably Germany—as part of the company's strategy to "resist local efforts to assert jurisdiction" (Chander 2012: 1836). If individuals are blocked from democratic action due to the extraterritorial accumulation of their personal data in a jurisdiction that they are not subject to nor have the resources to access, this is a meta-political injustice of misframing that presents a clear obstacle to parity of participation. An obstacle, it would seem, which is intentionally designed to render users politically voiceless and therefore unable to bring any data-related justice disputes—whether maldistribution, misrecognition, or ordinary-political misrepresentation—into recognized arenas of contestation.

Challenging the obstacles to parity of participation

To challenge political misframing, Fraser's suggestion is to ascertain the appropriate frame within which to contest injustices by applying the *all-subjected principle,* the notion that "all those who are subject to a given governance structure have moral standing as subjects of justice in relation to it" (2008: 411). This principle provides the basis for undertaking a process of *reframing*, to ensure all those subjected to a governance structure are accorded equal consideration regardless of nationality or geographic location. In the case of the personal data injustices of surveillance capitalism, a recognizable governance structure is evident in the accumulation activities of the Web companies that wield great power over their users, increasingly resembling sovereign nations in themselves (Chander 2012). A backlash against misframing concerning personal data is steadily growing, notably by Europeans contesting the misalignment between their subjection to the governance structures of Facebook, Google and others and their inability to access European data protection policies. Several recent rulings have made progress against this injustice, such as the 'right to be forgotten' legislation brought against Google (European Commission 2014), however these moments of opening are minor and fragmented; to advance towards moments of closure in which data injustices are widely understood and challenged will require supraterritorial, meta-democratic initiatives. As Fraser articulates in her discussion of the 'how' of abnormal justice, we must create "new institutions for staging and provisionally resolving such disputes democratically, in permanent dialogue

with transnational civil society" (2008: 416). A potential model for a global agreement is illustrated by the reform of data protection laws underway in the European Union. The EU has developed an update to their 1995 Data Protection Directive, the recently adopted General Data Protection Regulation (GDPR; to be implemented in 2018), which is designed to produce a clear legal framework for governing the flow of personal data between EU members and outside EU boundaries, and, importantly, to hold foreign companies accountable to these regulations (Council of the European Union 2015). The GDPR will also require the informed consent of data subjects for any initial uses as well as any reuse of their data, and the purposes for which the data are used must be made explicit in each case. Although a thorny issue for secondary use of data by researchers in particular—and some affordances will be built into the regulations for research purposes (Elias 2014)—the GDPR should empower European data subjects to control how their data are used. These reforms are fundamentally about reframing the scales of contestation and paving the way for Europeans to make justice claims against non-EU data accumulators.

The ability of these 'data localization' (Chander and Le 2014) and other forms of global regulatory 'soft law' approaches to advance social justice through parity of participation is certainly up for debate, however, in the face of strong resistance by the growing variety of powerful corporations with business models based on personal data accumulation, as well as opposition in various spheres to the balkanization of cyberspace and the free flow of research data (Elias 2014; Kuner et al. 2015; Borgman 2015), and more generalized failures to achieve consensus on various global policy issues. Irrespective of their actual capacity to address their aims, global data regulation and localization initiatives are fundamentally about *preventing* data driven oppression and injustice; however, there is as of yet little attention to a different question—how could personal data be more significantly reconfigured as an agent for *advancing* equality and social justice? In the stepwise fashion that data maldistribution lays the foundation for further data injustices of misrecognition and misrepresentation to take place, conceivably the reverse is also true; dismantling the digital enclosure of surveillance capitalism and placing control of personal data in the hands of data subjects could be a first step towards making further social justice advancements in the areas of socio-cultural recognition and political representation. This would require going a step beyond efforts such as those of the EU—from having the ability to limit how one's data are used, to promoting control and ownership of personal data by data subjects.

Some form of ownership could empower people to reap the value of personal data, economic or otherwise, yet considerably more attention from the legal domain is needed, to address the "lag in social evolution" that has been exploited by surveillance capitalists (Zuboff 2015: 83). A core perspective in democratic legal scholarship maintains that the development of norms, values, and expectations in a society in turn shape the development of its laws and regulations. In this view, law is shaped by society; it is a social construction always in flux (Schauer 2005: 498). In the case of surveillance capitalism however, the unjust social arrangements it produces are shaped by the crude application of out-dated laws and regulations that simply do not reflect contemporary life in digital and globalized societies. Mandatory privacy and data protection policies do fulfill the longstanding legal requirement of 'notice and consent', but to not consent effectively means exclusion from digital society (Cate and Mayer-Schönberger 2013). As such, the direction of travel is reversed—in these abnormal times, the 'norm' of personal data commodification has been shaped by laws instead of by societal expectations and values. In effect, what this means is personal data maldistribution, misrecognition, and misrepresentation are *legal constructions*. As legal scholar Julie Cohen (2017: 11) explains, social norms around personal data are being reorganized due to both a legal blindspot and the secrecy of the personal data industry:

> [a]ppropriation strategies based on contractually mandated secrecy are acts of *legal entrepreneurship* that both affirm and alter the legal status of collected information. Despite repeated efforts over the course of the twentieth century, data have proved powerfully resistant to formal, legislated propertization. The networks of secret agreements that characterize the emerging personal data industry step in where the map of

> formal legal entitlements ends, functioning simultaneously as self-interested programs for commercial advancement and assertions of normalizing authority. *They both consummate processes of extraction and appropriation and constitute those processes as foreordained*. [emphasis added]

Conferring ownership rights to data subjects would require updating laws in such areas as informed consent, property, and copyright. Despite surveillance capitalism being powered by personal data, it is largely when individuals are aggregated to groups based on predicted risk and behaviour that economic value as well as injustice are produced, and so a key consideration will be to weigh the relative merits of legally defining personal data as the private property of the data subject, the collective property of a defined group based on the all-subjected principle, or a common property resource for broader public benefit (see Schwartz 2004; Common Data Project 2011). If some form of collective public ownership of personal data is deemed appropriate, efforts to achieve this outcome might be encouraged by recent academic attention to how privacy infringements in personal data analytics not only affect individuals, but also operate at the group level due to big data's aggregative instincts. Advocates for a legal right to 'group privacy' thus argue that we must protect not only 'their' privacy (meaning individuals) but also 'its' privacy—the privacy rights of the algorithmically-defined group especially since they are often not recognized or protected groups in society, and the individuals that populate these groups are often unaware of their membership (see Taylor et al. 2017; Helm 2016). Although the present paper adds to the growing chorus of voices arguing that privacy is an insufficient concept to characterize the diverse social harms under conditions of surveillance capitalism, privacy does have the advantage of being an existing, widely recognized right protected in most legal systems. Perhaps then a leap to 'group privacy' may not be too far off from legal recognition, however it would likely only serve to prevent harms rather than advance equality and social justice through data control or ownership by data subjects.

It is, however, hard to imagine a new world of personal data in which data subjects acquire ownership or control, either personally or as part of a collective. But if such a landscape-shifting scenario were to occur, an equally problematic barrier is still apparent: the advanced data analytics skills necessary to enable parity of participation. Arguing that the question of agency, not just structures of oppression, should be central to any discussion about personal data, Kennedy et al. (2015: 6) ask "[c]an ordinary people do the same things with their data as corporations and organisations?" Similarly, Tene and Polonetsky (2012) contend that measures should be put into place to enable individuals and groups to gain *meaningful* access to personal data accumulated by big data companies, which could be realized through mandatory provision of user-friendly tools for data analysis and visualization. Such provisions—perhaps 'social media dashboards' that collate, aggregate, and correlate one's behaviours, activities, and preferences, coupled with data literacy initiatives, could empower people to engage in personal and collective analytics, a grassroots data science (see also Couldry and Powell 2014). Beyond access, participatory data projects such as *Our Data Ourselves* (Pybus et al. 2015) aim to redistribute personal data back to informed, capable data subjects. Data intermediaries are playing an important role in the data landscape more generally, from non-profit organizations that work with community groups to make the most of open data, to startups that undertake data analytics on behalf of NGOs. Data intermediaries could assist individuals and groups with the more sophisticated types of data mining required to overturn the algorithmic misrecognition that constrains their ability to self-identify. Democratizing data mining, as Kennedy and Moss (2015) describe, could enable groups to challenge injustices of misrecognition and misrepresentation, enabling 'knowing publics' based on self-identification and reflexivity rather than 'known publics' based on discrimination and subjectification.

Value in this paper has thus far focused on its economic interpretation, yet value in personal data for data subjects and groups is likely to be somewhat more nuanced than the pathological economic rationale underlying surveillance capitalism. The ability to extract insight at the individual level could lead to a better consumer experience, access to employment and other life opportunities, or improved health and

wellbeing, while the same at the collective scale might, for instance, empower groups towards a more informed bargaining position with state or corporate oppressors. Scholarship on the value of information (e.g., Lor and Britz 2005; Ponelis 2014) suggests various facets of value that might be accrued to individuals or collectives if people owned the personal data they produce (see Table 1). Accumulative and competitive value are the motivators of surveillance capitalism and might also motivate individuals and collectives, but a grassroots data science could also extract the instrumental, educational, cultural, and transcendental forms of value that these data can provide.

Accumulative Value	Lies in being used to build upon the contributions of others in order to create and generate new data	Surveillance capitalism
Competitive Value	Lies in possessing data that others do not (yet) have that can be exploited to gain a livelihood or competitive advantage	
Instrumental Value	Found in the application of data to improve the capacity of humankind to cope with the environment	Grassroots data science
Educational Value	Equipping successive generations of humans to improve the quality of their lives and the quality of their environment	
Cultural Value	Strengthening the cohesion of communities and societies/enhancing the quality of communal living	
Transcendental Value	Relates to satisfaction of aesthetic, religious, spiritual or higher needs, i.e., non-material quality of life	

Table 1: *Types of value that can be derived from personal data (adapted from Lor and Britz 2005; Ponelis 2014).*

The brief discussion here of how we might overcome the barriers to parity of participation in personal data analytics is a call not only for greater attention to the many and diverse threats to social justice in which surveillance capitalism is implicated, but also to the ways personal data might be reconfigured for advancing social equality. Attention from the legal sphere at national and global scales is needed, as well as evidence and frameworks for developing a grassroots data science that enables people and groups to accrue the various forms of value embedded in personal data.

Conclusion

A rapidly accelerating phase of capitalism based on asymmetrical personal data accumulation poses significant concerns for democratic societies. A diverse range of economic, social, political, and legal consequences must be more fully interrogated, yet the frameworks for conceptualizing and challenging practices of corporate dataveillance are underdeveloped. This paper has argued that the recent, surprising acceleration of surveillance capitalism situates these personal data practices as important threats to social justice. In the absence of detailed consideration of how political theories of justice might be useful in this context, this article draws on Nancy Fraser's theory of abnormal justice to make explicit how three core data practices inherent to surveillance capitalism should be viewed as threats to parity of participation in social life, and therefore targets of social justice reparations. This article illustrates how asymmetrical accumulation of personal data leads to injustices of maldistribution in which data subjects are dispossessed of an increasingly valuable material good, their personal data. This data maldistribution then lays the foundation for further injustices to take place—misrecognition due to status inequalities caused by algorithmic identification and categorization, and misrepresentation in the form of political misframing by

transnational surveillance capitalists, which creates a territorial mismatch and renders data subjects voiceless to challenge any illegal or inappropriate use of their data.

Any potential concept of justice must be relentlessly reviewed in the rapidly evolving era of surveillance capitalism, however I argue that the normative principle underlying the three dimensions of Fraser's framework, parity of participation, provides a useful tool for connecting diverse social harms to a common conceptual framework, whether that is economic losses associated with personal data dispossession, loss of employment due to algorithmic misidentification, or inability to take action against a foreign company that has illegally misused one's personal data. This paper focuses on three categories of social harm, however such a principle could potentially also enable further injustices not discussed here or not yet recognized to be brought under the framework. Overcoming any current or future injustices under the principle of parity of participation, if not in practice is at least conceptually straightforward—simply requiring a "dismantling [of] institutionalized obstacles that prevent some people from participating on a par with others, as full partners in social interaction" (Fraser 2008: 405).

Recognizing the focused nature of this account of social harms specific to corporate personal data practices, there is clearly a need for more conceptual development of the threats of dataveillance as well as empirical research that exposes further examples of unjust data practices occurring within the broader assemblage of state and corporate surveillance (Murakami Wood 2013). A focus on *data justice* is also of high priority—not only on the justness of data practices—due to the biases and inequalities baked directly into data. Recent critical attention is highlighting how data must no longer be afforded ontological privilege as neutral, objective representations of the world given the biases and subjectivities that influence their production, use, and reuse (Gitelman 2013; Bowker 2005), and so the potential for threats to parity of participation may also be directed at data production. While the present paper focuses on the grammars of justice, this approach would benefit from also interacting with other intersecting democratic values, ideals, rights, morals, and ethics in order to refine and advance the conceptual terrain used to understand dataveillance practices. More hopefully, research should also seek to ascertain the conditions necessary to recast personal data as a force for advancing social equality rather than injustice. A central objective here should be to provide data subjects with ownership or at least meaningful access to their data as a necessary first step towards addressing the lag in social evolution identified by Zuboff (2015), which has enabled the surveillance capitalists to normalize asymmetrical data accumulation and conduct further unjust data practices under cover of secrecy and under the protection of out-dated legal frameworks.

Acknowledgments

Thanks to the reviewers for their insightful comments and suggestions.

References

Amoore, Louise. 2009. Algorithmic war: Everyday geographies of the War on Terror. *Antipode* 41 (1): 49-69.

Andrejevic, Mark. 2007. Surveillance in the digital enclosure. *The Communication Review* 10 (4): 295-317.

Andrejevic, Mark. 2014. The Big Data Divide. *International Journal of Communication* 8: 1673-1689.

Andrejevic, Mark. 2015. Personal Data: Blind Spot of the "Affective Law of Value"? *The Information Society* 31 (1): 5-12.

Arvidsson, Adam, and Elanor Colleoni. 2012. Value in Informational Capitalism and on the Internet. *The Information Society* 28 (3): 135-150.

Barocas, Solon. 2014. Data Mining and the Discourse on Discrimination. Data Ethics Workshop, Conference on Knowledge Discovery and Data Mining, New York City.

Barocas, Solon, and Helen Nissenbaum. 2014. Big Data's End Run Around Anonymity and Consent. In *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, edited by Lane, J., V. Stodden, S. Bender and H. Nissenbaum, 44-75. New York: Cambridge University Press.

Bennett, Colin J. 2011. In Defence of Privacy: The concept and the regime. *Surveillance & Society* 8 (4): 485-496.

Bonnycastle, Colin R. 2011. Social Justice along a Continuum: A Relational Illustrative Model. *Social Service Review* 85 (2): 267-295.

Borgman, Christine L. 2015. *Big Data, Little Data, No Data: Scholarship in the Networked World*. Cambridge, MA: MIT Press.

Bowker, Geoffrey C. 2005. *Memory Practices in the Sciences*. Cambridge, MA: MIT Press.

Bowker, Geoffrey C, and Susan Leigh Star. 2000. *Sorting Things Out: Classification and its Consequences*. Cambridge, MA: MIT Press.

boyd, danah, and Kate Crawford. 2012. Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society* 15 (5): 662-679.

Britz, Johannes J. 2004. To Know or not to Know: A Moral Reflection on Information Poverty. *Journal of Information Science* 30 (3): 192-204.

Carmalt, Jean Connolly. 2011. Human Rights, Care Ethics and Situated Universal Norms. *Antipode* 43 (2): 296-325.

Cate, Fred H., and Viktor Mayer-Schönberger. 2013. Notice and consent in a world of Big Data. *International Data Privacy Law* 3 (2): 67-73.

Chander, Anupam. 2012. Facebookistan. *North Carolina Law Review* 90: 1807-1842.

Chander, Anupam, and Uyen P Le. 2014. Breaking the Web: Data Localization vs. the Global Internet. Davis, CA: California International Law Center.

China Copyright and Media. 2015. Planning Outline for the Construction of a Social Credit System (2014-2020). Available at https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/. (accessed 5 July 2016).

Citron, Danielle Keats, and Frank A Pasquale. 2014. The scored society: due process for automated predictions. *Washington Law Review* 89: 1-33.

Clarke, Roger. 1988. Information technology and dataveillance. *Communications of the ACM* 31 (5): 498-512.

Cohen, Julie E. 2017. The Biopolitical Public Domain: the Legal Construction of the Surveillance Economy. *Philosophy & Technology*: 1-21.

Common Data Project. 2011. The Common Data Project White Paper v.2. Available at http://www.commondataproject.org/. (accessed 12 Nov 2016).

Constine, Josh. 2012. Problems For Monetization: Lawsuit Forces Facebook To Let You Opt Out Of Sponsored Story Ads. Available at http://techcrunch.com/2012/06/21/sponsored-stories-lawsuit/. (accessed 5 August 2015).

Couldry, Nick, and Alison Powell. 2014. Big Data from the bottom up. *Big Data & Society* 1 (2): 1-5.

Council of the European Union. 2015. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Brussels: European Union.

Court of Appeal for British Columbia. 2015. Douez v. Facebook, Inc. In *2015 BCCA 279*.

Crawford, Kate. 2014. When Big Data Marketing Becomes Stalking: Data brokers cannot be trusted to regulate themselves. *Scientific American* Available at http://www.scientificamerican.com/article/when-big-data-marketing-becomes-stalking1/. (accessed 22 Nov 2016).

Crawford, Kate, and Jason Schultz. 2014. Big data and due process: Toward a framework to redress predictive privacy harms. *Boston College Law Review* 55 (1): 93-128.

Curry, Michael R. 1997. The digital individual and the private realm. *Annals of the Association of American Geographers* 87 (4): 681-699.

Davenport, Thomas H, and D.J. Patil. 2012. Data Scientist: The sexiest job of the 21st century. *Harvard Business Review* 90: 70-76.

Degli Esposti, Sara. 2014. When big data meets dataveillance: the hidden side of analytics. *Surveillance & Society* 12 (2): 209.

Dixon, Pam, and Robert Gellman. 2014. The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future. San Diego, CA: World Privacy Forum.

Duff, Alistair S. 2006. Neo-Rawlsian co-ordinates: Notes on a theory of justice for the information age. *International Review of Information Ethics* 6 (12): 17-22.

Dwork, Cynthia, and Deirdre K Mulligan. 2013. It's not privacy, and it's not fair. *Stanford Law Review Online* 66: 35.

Elias, Peter. 2014. A European Perspective on Research and Big Data Analysis. In *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, edited by Lane, J., V. Stodden, S. Bender and H. Nissenbaum, 173-191. New York: Cambridge University Press.

European Commission. 2014. Factsheet on the "Right to be Forgotten" Ruling (C-131/12). Brussels: European Commission.

Facebook. 2017. Company Info. Available at http://newsroom.fb.com/company-info/. (accessed 5 Jan 2017).

Fan, Jiayang. 2015. How China Wants to Rate its Citizens. *The New Yorker* Available at http://www.newyorker.com/news/daily-comment/how-china-wants-to-rate-its-citizens. (accessed 5 July 2016).

Fraser, Nancy. 2009. *Scales of Justice: Reimagining Political Space in a Globalizing World*. New York: Columbia University Press.

Fraser, Nancy. 2010. Who Counts? Dilemmas of Justice in a Postwestphalian World. *Antipode* 41: 281-297.

Fraser, Nancy 2008. Abnormal Justice. *Critical Inquiry* 34 (3): 393-422.

Fuchs, Christian. 2010. Labor in Informational Capitalism and on the Internet. *The Information Society* 26 (3): 179-196.

Gandy, Oscar H. 1993. *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview Press.

Garner, Patricia. 2015. Average revenue per user is an important growth driver. *Market Realist* Available at http://marketrealist.com/2015/02/average-revenue-per-user-is-an-important-growth-driver/. (accessed 19 July 2016).

Gitelman, Lisa, ed. 2013. *"Raw Data" is an Oxymoron*. Cambridge, MA: MIT Press.

Graham, Stephen, and David Wood. 2003. Digitizing surveillance: categorization, space, inequality. *Critical Social Policy* 23 (2): 227-248.

Hacking, Ian. 1982. Biopower and the avalanche of printed numbers. *Humanities in Society* 5 (3-4): 279-295.
Hacking, Ian. 1999. Making Up People. In *The Science Studies Reader*, edited by Biagioli, M., 161-171. London: Routledge.
Haggerty, Kevin D, and Richard V Ericson. 2000. The surveillant assemblage. *The British Journal of Sociology* 51 (4): 605-622.
Harvey, David. 2003. *The New Imperialism*. Oxford: Oxford University Press.
Helm, Paula. 2016. Group Privacy in Times of Big Data. A Literature Review. *Digital Culture & Society* 2 (2): 137-152.
Hodson, Hal. 2015. Inside China's Plan to Give Every Citizen a Character Score. *New Scientist* Available at https://www.newscientist.com/article/dn28314-inside-chinas-plan-to-give-every-citizen-a-character-score/. (accessed 5 July 2016).
Hoofnagle, Chris Jay, Jennifer King, Su Li, and Joseph Turow. 2010. How different are young adults from older adults when it comes to information privacy attitudes and policies? : Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864.
Hu, Tung-Hui. 2015. *A Prehistory of the Cloud*. Cambridge, MA: MIT Press.
Kennedy, Helen, and Giles Moss. 2015. Known or knowing publics? Social media data mining and the question of public agency. *Big Data & Society* 2 (2).
Kennedy, Helen, Thomas Poell, and Jose van Dijck. 2015. Data and agency. *Big Data & Society* 2 (2): 1-7.
Kinsley, Samuel. 2014. The matter of 'virtual' geographies. *Progress in Human Geography* 38 (3): 364-384.
Kitchin, Rob. 2014. *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences*. London: Sage.
Kshetri, Nir. 2016. Big data's role in expanding access to financial services in China. *International Journal of Information Management* 36 (3): 297-308.
Kuhn, Thomas S. 1962. *The Structure of Scientific Revolutions*. Chicago: University of Chicago Press.
Kuner, Christopher, Fred H. Cate, Christopher Millard, Dan Jerker B. Svantesson, and Orla Lynskey. 2015. Internet Balkanization gathers pace: is privacy the real driver? *International Data Privacy Law* 5 (1): 1-2.
Lor, Peter Johan, and Johannes Britz. 2005. Knowledge production from an African perspective: International information flows and intellectual property. *International Information & Library Review* 37 (2): 61-76.
Lyon, David. 2003a. Introduction. In *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*, edited by Lyon, D. London: Routledge.
Lyon, David, ed. 2003b. *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. London: Routledge.
Lyon, David. 2007. *Surveillance Studies: An Overview*. Cambridge, UK: Polity.
Lyon, David. 2014. Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society* 1 (2): 1-13.
Madden, Mary, and Lee Rainie. 2015. Americans' Attitudes About Privacy, Security and Surveillance. Pew Research Center. Available at: http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ (accessed 15 Jan 2017).
Manovich, Lev. 2012. Trending: The Promises and the Challenges of Big Social Data. In *Debates in the Digital Humanities*, edited by Gold, M. K., 460-475. Minneapolis: University of Minnesota Press.
Matzner, Tobias. 2014. Why privacy is not enough privacy in the context of "ubiquitous computing" and "big data". *Journal of Information, Communication and Ethics in Society* 12 (2): 93-106.
Mayer-Schönberger, Viktor, and Kenneth Cukier. 2013. *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. New York: Houghton Mifflin Harcourt.
Miller, David. 1999. *Principles of Social Justice*. Cambridge, MA: Harvard University Press.
Murakami Wood, David. 2013. What is global surveillance? Towards a relational political economy of the global surveillant assemblage. *Geoforum* 49: 317-326.
Nagenborg, Michael. 2009. Designing spheres of informational justice. *Ethics and Information Technology* 11 (3): 175-179.
Newman, Nathan. 2015. Data Justice: Taking on Big Data as an Economic Justice Issue. Data Justice. Available at: http://www.datajustice.org/blog/data-justice-report-taking-big-data-economic-justice-issue (accessed 11 May 2017).
Nissenbaum, Helen. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.
Ohm, Paul. 2014. Changing the Rules: General Principles for Data Use and Analysis. In *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, edited by Lane, J., V. Stodden, S. Bender and H. Nissenbaum, 96-111. New York: Cambridge University Press.
Olson, Elizabeth, and Andrew Sayer. 2009. Radical Geography and its Critical Standpoints: Embracing the Normative. *Antipode* 41 (1): 180-198.
Pasquale, Frank. 2015. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press.
Peacock, Sylvia E. 2014. How web tracking changes user agency in the age of Big Data: The used user. *Big Data & Society* 1 (2): 1-11.
Ponelis, Shana. 2014. Information as Economic Good: Its Origins, Characteristics, Pricing, and Associated Legal and Ethical Issues. In *Approaches and Processes for Managing the Economics of Information Systems*, edited by Tsiakis, T., 1-13. Hershey, PA: IGI Global.
President's Council of Advisors on Science and Technology. 2014. Report To The President - Big Data And Privacy: A Technological Perspective. Washington, DC: Executive Office of the President.
Pybus, Jennifer, Mark Coté, and Tobias Blanke. 2015. Hacking the social life of Big Data. *Big Data & Society* 2 (2): 1-10.
Rawls, John. 1971. *A Theory of Justice*. Cambridge, MA: Harvard University Press.

Richards, Neil M, and Jonathan H King. 2014. Big data ethics. *Wake Forest Law Review* 49: 393-432.
Rieke, Aaron, David Robinson, and Harlan Yu. 2015. Civil Rights, Big Data, and Our Algorithmic Future. Washington, DC: Upturn.
Roderick, Leanne. 2014. Discipline and Power in the Digital Age: The Case of the US Consumer Data Broker Industry. *Critical Sociology* 40 (5): 729-746.
Rorty, Richard. 1979. *Philosophy and the Mirror of Nature*. Cambridge, UK: Cambridge University Press.
Rose, Keith. 2015. BC Privacy Act Does Not Oust Facebook's Forum Selection Clause: BC Court of Appeal. Available at http://www.canadiancybersecuritylaw.com/2015/06/bc-privacy-act-does-not-oust-facebooks-forum-selection-clause-bc-court-of-appeal/. (accessed 5 Aug 2015).
Schauer, Frederick. 2005. The Social Construction of the Concept of Law: A Reply to Julie Dickson. *Oxford Journal of Legal Studies* 25 (3): 493-501.
Schwartz, Paul M. 2004. Property, Privacy, and Personal Data. *Harvard Law Review* 117 (7): 2056-2128.
Simonite, Tom. 2014. Sell Your Personal Data for $8 a Month. *MIT Technology Review* Available at https://www.technologyreview.com/s/524621/sell-your-personal-data-for-8-a-month/. (accessed 7 July 2016).
Solove, Daniel J. 2006. A taxonomy of privacy. *University of Pennsylvania Law Review* 154 (3): 477-564.
Stalder, Felix. 2002. Privacy is not the Antidote to Surveillance. *Surveillance & Society* 1 (1): 120-124.
Taylor, Linnet, Luciano Floridi, and Bart van der Sloot, eds. 2017. *Group Privacy: New Challenges of Data Technologies*. Dordrecht: Springer.
Tene, Omer, and Jules Polonetsky. 2012. Big data for all: Privacy and user control in the age of analytics. *Northwestern Journal of Technology and Intellectual Property* 11 (5): 239-273.
Thatcher, Jim , David O'Sullivan, and Dillon Mahmoudi. 2016. Data colonialism through accumulation by dispossession: New metaphors for daily data. *Environment and Planning D: Society and Space* 34 (6): 990-1006.
Turow, Joseph, Michael Hennessy, and Nora Draper. 2015. The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers And Opening Them Up to Exploitation. Philadelphia: Annenberg School for Communication, University of Pennsylvania.
UN Department of Social and Economic Affairs. 2006. Social Justice in an Open World: The Role of the United Nations. New York: United Nations.
United States Senate. 2013. A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes. Washington, DC: Committee On Commerce, Science, And Transportation.
Van den Hoven, Jeroen, and Emma Rooksby. 2008. Distributive justice and the value of information: A (broadly) Rawlsian approach. In *Information Technology and Moral Philosophy*, edited by Van den Hoven, J. and J. Weckert, 376-398. Cambridge, UK: University of Cambridge Press.
van Dijck, José. 2014. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society* 12 (2): 197-208.
Versium Analytics. 2016. Predictive Scores: Deriving meaningful intelligence from complex assortments of data. Available at http://versium.com/predictive-scores. (accessed 1 July 2016).
Warren, Samuel D., and Louis D. Brandeis. 1890. The Right to Privacy. *Harvard Law Review* 4 (5): 193-220.
Westin, Alan F. 1967. Legal safeguards to insure privacy in a computer society. *Communications of the ACM* 10 (9): 533-537.
Wilson, Matthew W. 2011. Data matter (s): legitimacy, coding, and qualifications-of-life. *Environment and Planning D: Society and Space* 29 (5): 857.
World Economic Forum. 2011. Personal Data: The Emergence of a New Asset Class. Geneva: World Economic Forum.
Wu, Chi Chi. 2009. Automated Injustice: How a Mechanized Dispute System Frustrates Consumers Seeking to Fix Errors in Their Credit Reports. Boston, MA: National Consumer Law Center.
Yu, Persis, Jillian McLaughlin, and Marina Levy. 2014. Big Data: A Big Disappointment for Scoring Consumer Credit Risk Boston, MA: National Consumer Law Center.
Zuboff, Shoshana. 2015. Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology* 30 (1): 75-89.
Zuboff, Shoshana. 2016. The Secrets of Surveillance Capitalism. *Frankfurter Algemaine Zeitung* Available at http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html. (accessed 22 December 2016).
Zurn, Christopher F. 2003. Identity or Status? Struggles over 'Recognition' in Fraser, Honneth, and Taylor. *Constellations* 10 (4): 519-537.
Zwitter, Andrej. 2014. Big Data ethics. *Big Data & Society* 1 (2): 1-6.