Critical Perspectives on Accounting 90 (2023) 102396

Contents lists available at ScienceDirect

Critical Perspectives on Accounting

journal homepage: www.elsevier.com/locate/cpa

# Data breaches in the age of surveillance capitalism: Do disclosures have a new role to play?

Jane Andrew *, Max Baker, Casey Huang

*The University of Sydney Business School, Sydney, NSW 2006, Australia*

ARTICLE INFO

*Keywords:*
Surveillance Capitalism
Instrumentarian Power
Data Breach
Data Security
Disclosure Framework
Accountability

ABSTRACT

The rise of big data has led to profound changes to the dynamics of accumulation and profiteering. Today, data is captured, produced, and reproduced with such regularity that its collection, utility, and value can go largely unnoticed, giving rise to "surveillance capitalism" (Zuboff, 2019a). This paper explores emerging forms of exploitation within the data economy, including the rise of "instrumentarian power" (Zuboff, 2019a), opacity surrounding data collection and use, and the impact of data breaches on our capacity to function within the information economy. We consider whether new forms of extended responsibility reporting may help to disrupt the trajectory of surveillance capitalism and democratise participation in the digital economy (Crawford, 2021). We draw on the accounting literature on organisational disclosures to consider whether the disclosure of data breaches might enhance accountability by making aspects of the surveillance economy knowable to us. Empirically, our analysis considers the various rules currently governing the disclosure of data breaches in Australia, the US, the EU, and Canada, and the application of these rules in practice. While regulation of the digital economy is developing, laws governing the disclosure of data breaches are highly dependent on an organisation's judgement. As a consequence, the nature, scale, and timeliness of these disclosures vary significantly, and the lack of clear routines makes it difficult for stakeholders to assess data risks. In response, we consider whether a mandatory disclosure framework might contribute usefully to the public "naming and taming" of surveillance capitalism (Zuboff, 2019a) and the democratisation of our digital future.

## 1. Introduction

While most of us are aware that our digital lives have become the means to commercial ends, to what extent are we aware of the exploitation of the human experience as free raw material that can be recruited for hidden commercial purposes (Zuboff, 2019a)? The use of technology, digitisation, and big data for profit-making has grown exponentially over the last ten years. Simultaneously, the methods employed to extract surplus value from the "digitisation of everything" are changing rapidly, while the source of surplus value derived from this data is nebulous and opaque. Zuboff (2019a, p. 10) argues that this has changed the nature of profit-making, giving rise to a new era of surveillance capitalism:

* Corresponding author.
*E-mail addresses:* jane.andrew@sydney.edu.au (J. Andrew), max.baker@sydney.edu.au (M. Baker), casey.huang@sydney.edu.au (C. Huang).

https://doi.org/10.1016/j.cpa.2021.102396
Received 22 March 2020; Received in revised form 20 October 2021; Accepted 21 October 2021
Available online 7 December 2021

> Instead of claiming work (or land, or wealth) for the market dynamic as industrial capitalism once did, surveillance capitalism audaciously lays claim to private experience for translation into fungible commodities that are rapidly swept up into the exhilarating life of the market.

In pursuing her thesis, Zuboff (2015, 2019a) offers a painstakingly detailed analysis of the economic logic underpinning this new form of capitalism, the methods used to bring it to life, and the challenges it presents to our futures. We are told that big data's value lies in its ability to offer a "penetrating gaze into consumers' and service users' lives" (Ball & Webster, 2020, p. 2) so that the human experience is shaped to help *ensure* returns to capital. Effective mobilisation of data and technology erases much of the risk associated with profit-seeking activities, enabling the potential of surveillance capitalism to extract wealth from "every aspect of every human's experience" (Zuboff, 2019a, p. 9). That is, we have become participants in a highly lucrative and almost completely opaque new market for "behavioural futures data" (Zuboff, 2019a, p. 93), in which big data is a valuable and tradeable source of information mobilised to influence behaviours, to shape thinking, and to make a profit.

It is easy to feel helpless in the face of behavioural data markets. We routinely give away information about ourselves to a wide range of organisations and we have little sense of how we might reclaim that data. It is almost impossible to navigate the digital world knowing and consenting to the data trail of our choosing; nor is it possible to access wants and needs outside of the totalising surrounds of digitisation. And once we have given that information away, we have no means of retrieving it. We lose track of where, when, and to whom we have provided data about some of our most sensitive identifiers, such as our names, dates of birth, addresses, marital status, medical conditions, and creditworthiness. We also leave behind a trail of "data fumes" (Thatcher, 2014, p. 1765) *donated,* often without our knowledge or consent, to surveillance capitalists, with every search, click, and like, with every tap of our credit card, every search of our map, and every trip to the shops. These "fumes" are collected and collated in astonishing detail, right down to the amount of time we spend reading an article online or the font we prefer when we use Microsoft Word – a process that has led to what Fourcade and Kluttz (2020, p. 1) refer to as "accumulation by gift". According to Peacock (2014, p. 1), this has left more and more of us feeling like "used users" because of the "unseen and unauthorised extraction, storage, analysing, selling, buying and auctioning of personal data". Compounding this, most of us lack the time to consider the implications of our digital choices, and when we do, the choices we make are highly individualised, leaving us feeling as if enrolment is inevitable, if not compulsory. Hull (2015) argues that the choice model of privacy self-management is a form of neoliberal responsibilisation, ensuring that individual privacy protection fails in ways that benefit big data companies. This form of individualisation, atomisation, and dependence is by design, as are the levels of opacity – because, as Zuboff (2019b, p. 25) says, "there can be no exit from processes that bypass individual awareness and on which we must depend on for effective daily life".

Unimpeded, the trajectory is bleak. But awareness of the exploitative and disempowering shape of surveillance capitalism is growing, regulators are slowly responding, and effective contest is possible. The complexity of the terrain warrants wide experimentation with modes of resistance, and it demands a multi-faceted network of disruptive socio-political responses from both within our current institutions, such as the law, and beyond them through new forms of cyber-activism (Cardullo, 2015). These might include projects that demand a democratisation of data related decision making, others that might insist the benefits of big data are collectivised and made a social good, and still others that help render some of the hidden dimensions of surveillance capitalism visible so that acts of resistance may reclaim our digital future. On their own, these forms of resistance are unlikely to derail surveillance capitalism's trajectory but combined they will be essential in the fight against digital exploitation. As Zuboff (2019a, p. 21) argues, if we are to make the digital future "*our home"* then *"it is we who must make it so*".

In a somewhat pragmatic response to Zuboff's (2019a) call to remake the digital future, this essay considers what role, if any, progressive forms of accounting, such as extended responsibility reporting, might play in contesting surveillance capitalism's claims on our digital future. Accounting is a complex and adaptive technology that has been an effective handmaiden to capitalism, playing a powerful role in the reproduction of exploitation through the many choices made about what to represent and how (Craig & Amernic, 2004). Fortunately, activists and scholars challenge accounting's role within capitalism, some working hard to describe and analyse the changing terrain of capitalist exploitation (Ejiogu et al., 2018), others exploring how accounting can counter forms of exploitation (Perkiss et al., 2020), and still others working to reimagine accounting as a highly charged and politically potent tool in the fight for representation, public debate, and social and environmental justice (Brown & Tregidga, 2017). Their efforts may be imperfect, but together they produce a matrix of resistance that offers a very important challenge to the unidirectionality of the kind of financial power driving inequality and exploitation as means to surplus accumulation. Within this, we explore whether accounting, through extended forms of disclosure, might offer a means to enhanced accountability in the information economy (Andrew & Baker, 2020a, 2019; Gumb, 2007; Roberts, 2018, 2009). Given critical research in accounting has debated the efficacy of disclosures as a tool for social justice, we seek to avoid making a totalising case for additional "subjects" of disclosure as if this is the salve needed to manage the intersectional nature of contemporary capitalist exploitation. Instead, we consider the conceptual distinction between disclosures of issues *we are aware of* (such as environmental pollution and labour exploitation) and disclosures that relate to issues *we are not aware of* (such as the market for our "behavioural surplus" data), and the impact this has on their potency. Extending this slightly further, it is our intention to explore whether information about the very immediate and often highly individualised nature of the risks associated with data breaches in the digital economy might make disclosures both highly potent sources of information and opportunities to expand wider public discourse.

Given this, we start with the assumption that Zuboff's (2019a) thesis offers a reasonably accurate appraisal of the new dynamics of capitalism. In particular, we agree that the value of big data lies in its capacity to alter our behaviour fundamentally and, perhaps most importantly, that the economic logics underlying surveillance capitalism are designed "to be *unknowable to us*" (Zuboff, 2019a, p. 11). Within this theoretical frame, we ask whether accounting might offer a way to make aspects of these logics *knowable* and, by extension, whether a form of extended responsibility reporting might help disrupt the trajectory of surveillance capitalism. There is no doubt that

accounting, even in its most progressive form, has significant limitations, but in attempting to expose the unprecedented asymmetries of knowledge and power that bolster surveillance capitalism, it may go some way to unsettling the opacity on which surveillance relies.

The remainder of this paper is organised as follows. We begin with a discussion of surveillance capitalism, paying particular attention to the idea of "instrumentarian power" developed by Zuboff (2015, 2019a). We then consider the accounting literature on disclosures, including arguments that suggest the limits of the disclosure project, to make the case that mandatory disclosures must be a feature of the information economy. To anchor our discussion empirically, we consider the various rules that currently govern security-related disclosures in Australia, the US, the EU, and Canada. We then explore the application of these rules in practice, taking a few key examples to highlight their uneven application and the disclosure gaps that continue to exist – particularly as organisations are still able to self-assess risks associated with data breaches and to self-govern their decision whether to disclose and to whom. Given this, we make a case for developing a mandatory disclosure framework designed to unsettle the opacity upon which surveillance capitalists rely. And while we acknowledge our proposal is imperfect, given that "bewildering the public" (Zuboff, 2019a, p. 15) appears core to the success of surveillance capital, we see value in disclosures as a means to turn responsibility back onto organisations in relation to how they handle our data. Indeed, such a framework could become a mechanism to make visible, at least partially, what is currently invisible in terms of the collection, storage, and trading of our data within the information economy.

## 2. Surveillance capitalism and instrumentarian power

Somewhat shockingly, according to Zuboff (2019a, p. 8), we have become subject to a new and more sinister incarnation of capitalism in which *all* human experience can be claimed "as free raw material for translation into behavioural data", available for extraction and exploitation in ways previously unimaginable. This new "surveillance" form of capitalism first claims all of the "*behavioural surplus*" data we create as we navigate our increasingly digitised lives, then collates and curates this surplus into "*prediction products*" that can then be securitised and traded on "*behavioural futures markets*" (Zuboff, 2019a, p. 8). Organisations use this data to "nudge, coax, tune and herd behaviour toward profitable outcomes" (Zuboff, 2019a, p. 8). Over the last 15 years or so, the scope of these products has grown exponentially as firms seek to turn all aspects of our lives – our voices, interests, habits, and even our emotions – into the "most predictive behavioural data" possible (Zuboff, 2019a, p. 8). While both the conceptualisation and implementation of the surveillance economy was pioneered at Google and later Facebook (Zuboff, 2019a; Crawford, 2021), it is now embedded everywhere, such that supermarkets, financial institutions, journalists, universities, policymakers, and health care providers all use data they have collected or acquired about us in this way. For Lyon (2014, p. 4) this has rendered "ordinary everyday lives increasingly transparent to large organizations". There is little doubt that it not only has a profound impact on the way we consume, but it can also influence the way we live, the way we conceptualise issues, the way we determine what matters to us as individuals or as a society, and, perhaps most worryingly, the way we vote.

The extent of surveillance made possible because of the digitisation and datafication of everything is quite extraordinary. Objects we buy are duplicitous, functioning both as a consumer good and as productive capital, collecting surplus value from our everyday activities to be traded in the market for future behaviour. Our bodily functions, private moments, our leisure time are all "recast as legible inputs for profit driven algorithms" and sold to "firms seeking to predict and control our futures" (Malmgren, 2019, p. 44). The "customers" in this new economy are the other enterprises that trade in these behavioural futures markets, with value emerging from both the effective mobilisation of data and from the trading of data as an asset in and of itself. Ultimately, surveillance capitalists are not content with simply knowing our behaviour, they want to *shape* it, and they want to shape it at scale because the purpose is not to simply "automate information flows *about us*" but to "automate *us*" (Zuboff, 2019a, p. 8). Aho and Duffield (2020, p. 190) summarise this intersection between the information economy, profit, and the human experience by saying that "big data provides the capacity, shareholder value provides the desire, powerful firms provide the determination to act on that desire, and an unwitting or indifferent populace provides the levelled social terrain on which to build".

This capacity to "shape human behaviour towards another's ends", gives rise to what Zuboff calls "instrumentarian power" (2019a, p. 8). This is not dissimilar to forms of governmentality described by Foucault and explored by accounting scholars (Viale et al., 2017), but its goal is not just the "conduct of conduct" (Rose, 1993, p. 3); rather it is to turn people themselves into highly predictable instruments of political or material consumption. In this sense "the principles and practices of surveillance capitalism embody the spectral logic of an algorithmic governmentality, which abstracts from life and channels us into the economic circulation" (Weiskopf, 2019, p. 977). Zuboff (2019a) sees this as a new form of power enacted through a "diffuse network of machines, that observe, catalogue, and translate human behaviour into shadow text" (Malmgren, 2019, p. 45) and, importantly, it is a form of power that arises in companies, not states. In coupling the idea of instruments with notions of power, Zuboff (2019a) offers dual insight into the role technology plays in contemporary capitalism, describing at once the instrumentation of the digital milieu that is being used to tune, herd, coach, and modify our behaviour, and the ways we are being instrumentalised towards some commercial or political end. Zuboff (2019a) describes instrumentarian power as the "whole digital surround that is now the instrumented medium that is producing the knowledge that creates the opportunity for the power to modify your behavior" – "your dishwasher, and your television set, and your car and the telematics, and your phone" (Kulwin, 2019). It is ubiquitous, sensate, computational, and global and it is designed so that *all* human activity, from the most banal to the boldest, can be monitored, measured, and modified for the purposes of surveillance capitalism. In effect, it replaces the neoliberal imperative to engineer *souls*, with a surveillance imperative to engineer *behaviour* (Zuboff, 2019b, p. 20).

In this way, surveillance capitalists are thought to be "radically indifferent" to what we like, what we do, and what we care about – or as Venkatesh (2021, p. 371) notes, "they do not care whether what happens on their platforms is good or bad, whether messages are true or false … they care only about the volume of data that can be harvested from it". It is, according to Zuboff (2019b, p. 21), "a form

of observation without witness". Technology firms and associated data harvesters are radically indifferent to our personhood, our politics, and our ethics, viewing us all as fragments of surplus data waiting to be aggregated, analysed, and sold to organisations seeking to influence us to act, buy, and vote in certain ways (Zuboff, 2019a, p. 377). Unlike the violence associated with totalitarian forms of power, instrumentarian power operates through behavioural modification, made possible because of the opacity built into the technologies of surveillance capitalism – and these technologies are quite literally built into material objects that enable the collection of data we do not even know we create (Malmgren, 2019, p. 45). These technologies are also woven into the social and economic systems that shape the nature of the data collected, the way it is stored, how it is created, how it is used and, perhaps most importantly, what we are able to *know* about it.

Part of the success of surveillance capitalism lies in its capacity to mobilise this "instrumentarian" form of power (Zuboff, 2019a, p. 8) to create levels of opacity not possible within industrial capitalism. It is coercive in nature, but not violent or obvious. It is stealthy, ensuring the only way to maintain a socially and economically viable digital life is to remain enrolled. Our collusion can feel consensual and where it does not, it can feel essential, inevitable, and useful. Instrumentarian power makes it possible to proliferate technologies and data collection regimes that form the social and economic basis of surveillance capitalism – guiding our behaviour with a new-found certainty and predictability, producing data assets of untold value. The rise of surveillance capitalism, and its associated instrumentarian form of power, have emerged at such speed that surveillance capitalists have been "protected by the inherent illegibility of the automated processes that they rule, the ignorance that these processes breed, and the sense of inevitability they foster" (Zuboff, 2019a, p. 10). Opacity, it seems, has been hard-wired into surveillance capitalism.

## 3. Disclosure and effective resistance

In fetishising technologically enabled freedoms, the architects of this new form of capitalism have been able to create digital spaces for accumulation at such speed and with such complexity that regulators have struggled to keep up. In most jurisdictions, the practice of harvesting our surplus data was well established before regulators began to explore how to break the opacity established by surveillance capitalists. As might be expected, one such strategy has been to insist on certain data rights, and to draw data related matters into view through greater disclosures such as those embedded in Europe's General Data Protection Regulation (GDPR) of 2018 (Andrew & Baker, 2019). Around the same time, a proliferation of domestic rules and laws emerged across the globe, directing organisations to disclose information related to data security and, in some circumstances, to breaches of personal data in their care (Aho & Duffield, 2020). Much of this regulatory activity was triggered in response to both market concerns about data related material risks and to consumer advocates' demands that organisations do more to protect personal data. While this recognises the limitations of "privacy self-management" that, by default, is the *modus operandi* of the digital economy (Lehtiniemi & Kortesniemi, 2017), it has been difficult to conceptualise behavioural data in ways that make these regimes an effective check on instrumentarian power. That said, rules and laws that focus on data security and privacy issues present an opportunity to begin to expand regulation such that we regain control over the collection and use of the surplus behaviour data driven by the reigning logic of accumulation within surveillance capitalism.

These emerging legal frameworks deserve our attention. Despite their imperfections, laws that insist on data related disclosures hold out the possibility that structural dynamics responsibilising the individual, can be reconfigured to ensure organisations and regulators take responsibility for protecting data security. We need first to understand what the laws currently offer, before we can advocate for laws that "shift from making individuals responsible for understanding the data market to making national and international authorities accountable for data governance" (Taylor, 2017, p. 12). As we have slowly become aware that "surveillance capitalists know everything *about us*" (Zuboff, 2019a, p. 11 emphasis in original), we have also begun to realise that we know very little *about them*. Thus, interest in some form of *mandated* disclosure regime addressing the opacity of data collection, trading, and utilisation is growing (the GDPR in Europe is a good example).

Unlike other forms of extended responsibility disclosures, such as emissions levels, data related phenomena are not easily observable. Thus, data related disclosures will need to provide insights into the coupling of "personal necessity with economic extraction" that are currently "unknown and unknowable" to us (Zuboff, 2019a, p. 25). The fact that the technologies that fuel surveillance capitalism are designed to be opaque makes their transparency important if we are to be able to participate in the production of a democratically determined future. Transparency of this kind is not the end game, nor is it imagined as a perfectly accurate reflection of the complex interwoven dynamics of the digital economy. Indeed, there is little doubt that calls for greater transparency and new forms of disclosure are in themselves ideological acts of worldmaking that are inevitably both enabling and constraining. Yet sharing information and insights are essential to debate, and while it is true that the debate can be framed by the disclosure itself, scope for dispute and conflict and critical interrogation becomes possible. Given this, as part of a wider democratising project, insisting on greater transparency within the digital economy can help shed some light on surveillance capitalism's "material architectures, contextual environments, and prevailing politics" (Crawford, 2021, p. 12). This is particularly important given so many organisations are reliant on the datafication of everything with only very tenuous connections to the norms of consent. Mouffe (2018, p, 42) sees the production of a wide variety of discourses about power as essential to democracy, describing these as a "discursive 'exterior'" from which "the discourse of subordination can be disrupted". Indeed, disclosures enable new forms of discourse, and while always emergent and imperfect, through discourse, participants in the data economy can start to understand the value and risks of shared data. This is essential if citizens and stakeholders are to reshape the digital economy data in ways that hold powerful organisations to account. For Mouffe (2018, p. 4), all forms of discourse that offer an opportunity to re-politicise democracy support the restoration of the "political frontier" that is essential to challenging the totalising logics of capital, and particularly, surveillance capital.

Brown (2019, p. 27) argues that, in combination with the digitisation of everything, neoliberal forms of capitalism have effectively

de-platformed "the social", obscuring our capacity to come together in ways that enable political enfranchisement and opportunities to redress, at least partially, historically produced inequalities. The opacity that surrounds the harvesting and commercialising of our data footprint ensures a "significant power asymmetry" making it impossible to "*not* collaborate with algorithmic systems" (Crawford, 2021, p. 58). According to Crawford (2021), when the technologies of surveillance "are truly hidden", people are kept "unaware of why or how they received forms of advantage or disadvantage" and this requires a "collective political response … even as it becomes more difficult" (2021, p. 149). Without at least some insight into the scope and scale of the data economy, the possibility that we might "harness the digital" to support activities that are "genuinely productive of effective life and compatible with a democratic social order" will remain impossible (Zuboff, 2019a, p. 395). Drawing from Brown and Tregidga (2017), we see our task as critical researchers in accounting is to "restore the (ant)agonisms needed for progressive politics" (p. 17) because ""the people" appear where *political* disputes are conducted" (p. 4). Indeed, the possibility of accountability relies on the production of discourses and arenas through which various accounts can clash. In this sense, disclosures of all kinds, but particularly those that relate to matters deliberately concealed, make it possible to enjoy "one of the privileges of democracy", which "is to disagree and to participate in the related power struggles and conflict" (Dillard & Vinnari, 2017, p. 100).

### *3.1. Accounting and the enduring hope of disclosure*

Given this, in our view, it is worth reconsidering the political potency of organisational disclosures as a means to rupture the trajectory of surveillance capitalism and the rise of instrumentarian power. We look to the work accounting researchers have undertaken over the last 30 years in a wide variety of settings and in enormously diverse contexts as guidance in considering how to meet the challenges presented by the data economy. There is no doubt we could also look to practice for this guidance, but we are focused on research to articulate the philosophical grounds for our thinking about the relationship between data and disclosures, and the implications this might have for a framework for data breach-related disclosures. The mainstream accounting literature on disclosure focuses primarily on market efficiencies that can be achieved when issues of information asymmetry are addressed through effective disclosure (Barron & Qu, 2014; Barth et al., 2003; Barth & Schipper, 2008), whereas the inter-disciplinary accounting literature explores the role disclosures play within a wider conceptualisation of organisational accountability, stretching well beyond the boundaries of responsibility established within capital markets (Gallhofer & Haslam, 2019; Haslam et al., 2019; Osman et al., 2021; Roberts, 2021). This interdisciplinary literature debates the role of disclosures in the production of relations of accountability between organisations and stakeholders, and there has been much discussion as to the form of transparency that might support, or indeed hinder, effective organisational scrutiny (Roberts, 2018, 2009).

The inter-disciplinary accounting community has had a sustained focus on disclosures because they are considered "essential to adjudication", allowing for an "evaluation of activities" (Bebbington et al., 2020, p. 2, drawing on the work of Miller and Power, 2013). Despite broad agreement on the importance of disclosures to accountability, the literature is replete with conflicting views about what disclosures matter (Bebbington et al., 2020); who should be responsible for producing disclosures – managers, or external experts, or stakeholders (Gray & Milne, 2018); whether they should be voluntary or mandatory (Leong & Hazelton 2019); the efficacy of disclosure frameworks (Andrew & Cortese, 2013, 2011); where and when and to whom disclosures should be made (Miles & Ringham, 2019); their content (Gumb, 2007); and their reliability (Khan et al., 2020; Michelon et al., 2015). In the context of surveillance capitalism, informing us about the relationship between our behaviours, the data we produce, and how that data might be stored and used, introduces the possibility of discussions that will expose the profiteering associated with behaviour data. Data related disclosures are likely to invite imperfect but still useful conversations about ethics, limits, consent, and value in the digital economy because, as Zuboff has argued (2019a, p. 249), discussions of both transparency and privacy "represent friction for surveillance capitalists".

Within both the accounting literature and research exploring the sociological implications of data, there is also a body of work that voices significant concerns about the effectiveness of disclosures, both in their ability to represent organisational realities, but also as a stimulus for political action in the face of pressing issues such as climate change and economic inequality (Andrew & Cortese, 2013; Bryer, 2014). These arguments are nuanced, but most point to the limits of all forms of language as a means of representation, be this textual, visual, or calculative (Mouritsen, 2011, p. 228). Others have argued that disclosures in and of themselves are unlikely to disrupt the structural power dynamics existing between reporters and audiences within capitalism (Ben-Amar et al., 2021; Lauwo et al., 2020); disclosures can be curated in the interests of power (Roberts, 2021); and perhaps most importantly, when organisations produce additional or improved disclosures, these can masquerade as progressive, responsive, and democratic, thereby muting the need for alternative and more radical political action (Andrew & Baker, 2020a; Mouffe, 2018; Spence, 2009). Perhaps the most evocative contribution to this debate comes from Roberts (2009, p. 962), who, drawing on the thinking of psychoanalysts such as Freud and Lacan, suggests the emphasis placed on transparency in the accounting literature promotes the view that the solution to all forms of organisational collusion and exploitation lies in "greater disclosure or new objects of disclosure" – as if we simply need to find a way "of seeing more sharply or more completely" (Roberts, 2009, p. 962).

For the most part, this latter set of arguments has oriented our thinking as critical researchers. We too have questioned the efficacy of disclosures as a mechanism for social change (Andrew & Baker, 2020a, 2020b). However, in light of surveillance capitalism and the information economy, we wonder if there might be a significant conceptual difference between disclosures relating to concerns we can experience materially and empirically, such as climate change, labour exploitation, and organisational diversity, and those that we cannot. Specifically, it seems to us that the ontological nature of behavioural data and digitised identities make them difficult to observe. In fact, they are designed to be empirically unobservable (Zuboff, 2019a; Crawford, 2021), buried within the technologies of power routinely mobilised to enrol us as suppliers of free data to surveillance capitalists. Ontologically and empirically, this means that surveillance capitalism has ensured data, *as a means to accumulation,* is impossible to conceptualise and interrogate in the same way we

do for exploitations that we can see and feel. The *un-discoverability* of the dynamics of data within the digital economy "are no accident", instrumental technologies are "built to see and intervene in the world in ways that primarily benefit the states, institutions, and corporations they serve" (Crawford, 2021, p. 211).

The public disclosure of objects that are difficult to access empirically might start to give these objects a shape and form that becomes actionable. Accepting that these disclosures will be imperfect, curated, and inadequate, they may yet provide a means by which to conceptualise surveillance capitalism. Disclosures hold out the possibility that we can show data to be the most profoundly impactful yet devastatingly invisible currency of our time. Despite concerns about disclosure as a driver for social change, disclosures can have a potency that animates dialogue in these circumstances. For us, disclosures can help make surveillance capitalism *known*.

Conversations about the trajectory of the information economy must be underpinned with knowledge of the object driving this new form of accumulation – our data – and to do this, we need to know how it is collected, what it is used for, how it is stored, who it is shared with, how it is sold, and what happens if the security of this data is breached. Without this, it is difficult to conceptualise the implications of surveillance capitalism for us as individuals, but more importantly, it will be impossible to assess its implications for our communities and the future of participatory democracy.

### 3.2. Mandatory disclosure and the information economy

In advocating for disclosures within the context of the surveillance economy, we acknowledge that the structural dynamics that drive exploitation and inequality within capitalism will still need to be addressed in a more material sense. But if we are to have any chance to transform the dynamics of exploitation, they must first be known, even if our knowledge is limited and partial. Given this, we believe disclosures, as an established practice within liberal democracies, can and will help to produce what Mouffe calls a "discursive 'exterior'" – a way of providing a language or discourse to interior, hidden practices. In essence, Mouffe is advocating for discursively turning power inside out so that the interior is exposed to external scrutiny. If, as we suggest, the ontology of behavioural data makes it empirically difficult to conceptualise, it is through the production of a discursive exterior that it becomes possible to "interrupt exploitation" (Mouffe, 2018, p. 39).

Following Mouffe's logic, disclosures might be usefully thought of as a strategy to map "the terrain of struggle" (Mouffe, 2018, p. 47). And it is in this vein we argue for mandatory disclosures to help produce the "discursive exterior" of surveillance capitalism, thereby making the data economy empirically knowable and resistance possible. To be clear, we make this argument, not as advocates for the kind of consensus-seeking deliberative democracy introduced to accounting through Habermas. As Godowski et al. (2020) argue, these rest too heavily on utopian ideals of perfect(able) transparent information that is intended to mute friction, orient debate, and sustain order. Instead, we see disclosure as part of the apparatus needed to ensure organisational accountability can be contested – a view more closely aligned to that of Mouffe (2018) and sympathetic critical accounting scholars (Andrew & Baker, 2020a; Brown, 2009; Brown & Dillard, 2013; Brown & Tredigda, 2017; Godowski et al., 2020). While we are arguing for mandatory disclosure regulations in this paper, we acknowledge that an agonistic form of democracy needs to be constituted by a suite of tools that encourage conflict, offering new knowledge while simultaneously exposing the limits of singular approaches to accountability. There is little doubt that any mandated regime will offer opportunities to both reveal and conceal information related to data breaches. However, mandating disclosure lays the groundwork for civil society to re-politicise the space for accountability. This is critical if we are to democratise our data rights and perhaps be kept safe from data related crimes. Importantly, we see shadow and counter accounts as an important complement to the arguments we make in this paper, because as many scholars have pointed out, these can be very effective at stimulating public debate (Andrew & Baker, 2020a; Perkiss et al., 2020; Uche & Khalid, 2021). Unlike the kinds of voluntary disclosures that dominate much of the discussion surrounding corporate social responsibility (Cho et al., 2012), mandatory disclosures are enforceable and rely on an external and independent regulator to design the basis upon which organisations must report.

While alternative forms of accounting, such as shadow accounting and counter accounting, address the shortcomings of regulation, they cannot operate in cases where there is no information. Instead, requiring new forms of regulation and reporting frameworks can assist in building a discourse around which other forms of resistance emerge as part of a matrix of political strategies. We understand regulators are constrained, and the model we propose has limitations, but given what we know about surveillance capitalism, we cannot leave organisations to guard themselves (Zuboff, 2019a). However imperfect, mandatory disclosures can provide the grounds for public debates about the data economy, offering the possibility of political resistance that "ruptures and confronts dominant economic interests" (Mouffe, 2018, p. 45). Transparency, according to Zuboff (2019a, p. 249) "represents friction for surveillance capitalism", and it is friction, or what Mouffe (2018, p. 57) calls "agonistic confrontations", that restores "the citizens' voice".

Following these arguments, the remainder of our paper considers the current requirements to disclose data breaches under the law. We have focused on data breaches primarily because there is growing pressure to ensure the security of data in the information economy, and these laws reflect this pressure. We accept that, in focusing on data breaches, we are only able to skim the surface of data related issues within surveillance capitalism. However, in focusing our empirical analysis here, we can develop what we consider to be a viable framework for disclosures in this space, and by extension, introduce a framework from which to expand the discussion about data rights. As we will see in the discussion that follows, on the surface, these laws appear to insist upon an appropriate level of transparency and accountability, but actually ensure that the empirical realities of data security risks are quarantined from wider public debate. At present, these laws appear to preclude discussion about compromised privacy, our rights to data security, and the level of responsibility that should be assigned to the organisation responsible for our data by ensuring any breaches to the security of our data do not have to be made *publicly* available under the law.

As accounting researchers, we focus on these disclosure laws because they connect to our wider disciplinary calls for improved

organisational accountability. We see them as having a role to play in the extended responsibility reporting obligations of powerful organisations (Amir et al., 2018). So far, the literature on corporate social responsibility has had little to say about data security and the importance of data breach disclosures despite arguments over a decade ago that "socially responsible corporate conduct necessitates strong information security" (Lending et al., 2018; Matwyshyn, 2009, p. 579). Given that much of the field has sought to challenge the more serious exploitative dynamics of corporate power, both as it affects the planet and people (Catchpowle et al., 2004; Cooper et al., 2005; Cousins & Sikka, 1993; Tregidga, 2017), it is understandable that data privacy, as a problem of privileged individuals in developed countries, has not been front of and within these debates. But as the collection of personal data grows in scale, the risks associated with data breaches have grown for all individuals. Indeed, data breaches are now a regular occurrence, yet we are mostly unaware of their scale, the organisations they affect, the nature of the data made available, or how organisations attempt to mitigate these risks. Significantly, for us as accounting researchers, the current rules governing the disclosure of data breaches and organisational practices in response to data breaches vary enormously, but none insist on the kind of *public* accountability that will inform and enrich a broader public debate about surveillance capitalism (Barocas & Nissenbaum, 2014; Cooper, 2005 et al.; Introna & Pouloudi, 1999; Madden, 2014).

## 4. Disclosure as a challenge to the opacity of surveillance capitalism

Given that data systems are "rife with relations of inequity, extraction, and exploitation" (Sadowski, 2019, p. 2), it is surprising that accounting researchers have been quiet about the role we might play in developing viable data-oriented forms of accountability. As we noted earlier, the accounting literature on accountability is diverse, but underpinning it is a shared recognition that powerful organisations owe the less powerful some form of account about how they behave in relation to a widening set of social expectations (Cousins & Sikka, 1993; Dillard & Vinnari, 2019; Pesci et al., 2020). We see the provision of *public* disclosures of data breaches as providing the conditions upon which accountability constituted through "talk, listening, and asking questions" (Roberts, 2009, p. 969, Roberts, 1991) can emerge. We do not conflate disclosures with accountability, but we do advocate for disclosures that may form the *basis of dialogue* about the surveillance economy, beginning with structured and enforceable reporting about data security issues.

Data breaches can take many forms, thereby exposing both the organisation and the individual (the data subject) to different types of risk. The GDPR (2018) is considered the gold standard on data regulation and its definition of personal data states that it includes:

> Information such as a name, an identification number, location data, an online identifier or information that relates to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person (Article 4, GDPR).

The GDPR's definition indicates that some data is more sensitive than others. For instance, genetic information is more sensitive than other personal information, such as one's name. This means that when personal data is made public without the consent or knowledge of the individual, it is important not only that the breach is disclosed but that the type of data and the level of sensitivity associated with that data is also made public. Further, since the data must be anonymised or pseudonymised using de-identification techniques (that can vary in efficacy), this can make it hard for the individual (the data subject) to know where that information is stored and how that information is used (Andrew & Baker, 2019). Without this information, our collective ability to construct a wider critique of the use of data and its effects on us as individuals and our communities more broadly is greatly impeded (Zuboff, 2019a).

When the data held by an organisation is breached, either as a result of leaking, hacking, or poor data management, there are two primary instruments currently used to insist on some form of disclosure – legislation and listing rules. Indeed, most jurisdictions and securities markets have requirements in place that ensure an organisation discloses data breaches, but as we will outline in the following discussion, both the law and the listing rules are limited in their ability to shed light on data security. When the law is triggered, in most circumstances, the organisation will be required to inform the regulator, and where certain thresholds are met, it will also be required to inform the individuals affected (Lake, 2017). Here the law provides ample scope for non-disclosure or aggregated forms of disclosure that leave data providers ill-informed. According to Ruppert et al. (2017, p. 2), the approach embedded in both the law and the listing rules is based on "the ontological premise of 'hyper-individualism' whereby persons, events and phenomena are treated as independent and 'atomistic' entities" – an assumption that is likely to impair our ability to develop a coherent analysis of surveillance capitalism. Indeed, rules that emerge to govern data breach disclosures within this context tend to reproduce the idea that it is up to individuals to protect themselves, and that the responsibility of the organisation can be effectively discharged if it has determined the risks to the individual are low, or where the individual (or a proxy for the individual, such as the regulator) has been informed. At present, in both scenarios, there is no obligation to provide a wider *public* set of disclosures, and this undermines our ability to assess risks and discuss rights as a community of data subjects, and correspondingly, it makes it impossible to construct an informed and collectivised view as to what we could or should expect from organisations we have entrusted with our data. In Zuboff's (2019a) terms, "friction" becomes all but impossible, muting the possibility of "antagonist confrontations" (Mouffe, 2018).

In keeping with the conceptual frame of this paper, for mandatory disclosures to be effective, they must first, document a wider set of data related security matters in order to begin to disrupt the ontological status of data as it is currently constructed in the surveillance economy, thereby making "data" empirically knowable. Second, mandatory disclosures need to insist on timely, routine, comparable, and most importantly, *public* disclosure of data related matters in order to begin to construct a "discursive exterior" for surveillance capitalism. It is through constructing this discursive exterior that future critical accounting research might construct a "new subject of collective action … capable of reconfiguring a social order experienced as unjust" (Mouffe, 2018, p. 11).

### 4.1. Disclosure laws and listing requirements?

Having laid out the conceptual and theoretical intent of this paper, in the discussion that follows we will try to draw out the importance of our arguments with reference to the rules and regulations that currently govern data breach-related disclosures.

In doing this, we pay particular attention to the legal similarities that exist across four jurisdictions, namely, Australia, the US, Canada, and the EU. While the nature and scope of these laws differ to some extent, all allow the organisation to determine whether the risks associated with a data breach are significant enough to warrant informing the individuals affected. Indeed, none require the organisations to make data breach disclosures *publicly* available and, perhaps even more problematically, if the organisation deems there is no evidence the breach has been acted upon illegally by some external party, it can decide not to disclose it at all. The evidential basis upon which an organisation can conclude a breach has not been "used" is entirely unclear, and this gives organisations considerable scope to avoid disclosures that might otherwise be deemed to be in the public interest. Given this, it is easy to see how the data economy continues to function on the basis of "concealment and obfuscation" (Zuboff, 2019a, p. 89).

Beginning with Australia, the law states that a "data breach happens when personal information is accessed or disclosed without authorisation or is lost", and until 2018, there was no clear reporting framework to govern an organisation's disclosures relating to these kinds of data breaches. This changed in February 2018 when the notifiable data breach scheme commenced, requiring an organisation or agency responsible for data according to the *Privacy Act 1988 (Cth)* to notify "affected individuals" and the Office of the Australian Information Commissioner (OAIC) if it is involved in a data breach that is "*likely to result in serious harm*" (OAIC, 2020). The OAIC produces aggregated and anonymised reports on data breaches that are made available to the public, but beyond this, there is no requirement that the organisation makes the wider public aware of the breach. This means that disclosure obligations are limited, and the scheme precludes a more direct form of accountability that might emerge if the firm was required to produce a public account of its data security performance.

In the US, every state and territory has a data breach notification statute that requires an organisation to notify affected individuals residing within that jurisdiction in the event of a data breach, but even this can be avoided if organisations find "no evidence" that the data breach has compromised the security of their clients or customers. In effect, this means that many data breaches go unreported, and most individuals are never notified (Neto et al., 2021). In addition to this disclosure requirement, in some limited situations where jurisdictionally determined risk thresholds are met, the organisation may also be required to notify the Attorney General of the state, state agencies (such as law enforcement), and credit reporting agencies. Beyond this, nowhere in the US is an organisation required to make a public disclosure of the breach under the law (Westerlind, 2019). Similarly, in Canada, there is no requirement under the Personal Information Protection and Electronic Documents Act (PIPEDA) to disclose data breaches to the public. Organisations experiencing a data breach are required to notify the individual if the breach is deemed to "create a real risk of significant harm to an individual" (Minister for Justice, 2020, p. 19 s 10.1); in addition, they need only report the breach to the Privacy Commissioner of Canada.

In the EU, the GDPR prioritises notification to the regulator over notification to the individual in the event of a data breach. The regulation also emphasises the importance of the timeliness of the notification in a way that is not reflected in the data breach disclosure rules currently operating in Australia, the US, and Canada. According to the regulation, data controllers are required to advise the relevant authority of a data breach within 72 h of becoming aware of the breach, and where the breach is considered high risk the data controller is required to notify the individual without undue delay (Article 34). While the GDPR (2018) is perhaps the most far-reaching and sophisticated of the laws governing data breaches, it still has its problems. The speed of reporting to the regulator enables the regulator to oversee the organisation's response, but the law lacks specificity in terms of individual notifications. Like in other jurisdictions, the individual only needs to be notified if "the personal data breach is likely to result in a high risk to the rights and freedoms of the individual" (GDPR Article 34, clause 1). But if the organisation has taken appropriate remedial steps or notifying an individual would involve "disproportionate effort", then the individual does not need to be identified (GDPR Article 34, clause 3). In addition, and in keeping with the norms established in Australia, the US, and Canada, the disclosure regime does not require the information to be made available publicly, thereby making it impossible to conceptualise the "various forms of obligatory reciprocity" to which we are entitled (Fourcade & Kluttz, 2020, p. 7).

Alongside these statutory obligations, the Listing Rules of some securities exchanges require that data breaches be disclosed to the market. For example, the Securities and Exchange Commission (SEC) in the US requires that "public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion" (SEC, 2018). In Australia, the ASX has

**Table 1**
Notifications required by data breaches in the EU, US, Australia, and Canada.

| Jurisdiction | Notify Regulator | Notify Individual | Notify Public |
|---|---|---|---|
| US | May be required in cases that meet various risk thresholds depending on the state jurisdiction. | All breaches, but only when the breach compromised an individual's security | None |
| EU | All breaches within 72 h of discovery | High risk breaches, but not if remedial interventions have been adopted, or if effort is deemed disproportionate to risk | None |
| Australia | All cases of unauthorised access or disclosure of personal information | Likely to result in serious harm | None |
| Canada | Where the breach creates a real risk of significant harm to an individual | Where the breach creates a real risk of significant harm to an individual | None |

reiterated that the principles underpinning a firm's continuous disclosure obligations under the *Corporations Act* and the ASX Listing Rules also apply to data breaches. As a rule, data breaches that would reasonably be expected to have a *material effect* on the price of a listed entity's securities would need to be disclosed immediately. The criteria for determining whether the breach constitutes market-sensitive information remains largely untested in Australia. There are similar requirements in place for the Canadian Securities Exchange and the London Stock Exchange, but until now, these disclosures have remained opaque with little uniformity around what constitutes a "material risk". There is no doubt that the listing rules in all four of these countries present an opportunity to provide information about data breaches to the public beyond those currently required under the law, but, in practice, the norms of data related disclosure to the market have not yet been established.

On the surface, these laws may seem adequate, but all allow for self-governance, and all individualise the disclosure relationship by creating communication pathways between the organisation and the individual, or the organisation and a government agency (see Table 1). While some of these agencies, like the OAIC, make aggregated reports about data breaches available to the public on a regular basis, none of the reports offer the kind of granular data that would make it possible to hold organisations to account and most make it difficult to stimulate the kinds of antagonisms needed to "reclaim the digital future as humanity's home" (Zuboff, 2019a, p. 525). Indeed, there remains a gaping void between the level of disclosure required under the respective laws and the significant (and lucrative) use of this data by surveillance capitalists – but as economists such as Thomas Piketty and Joseph Stiglitz have told us, even "'abnormal' dynamics of accumulation have been – and can again be – mitigated by democratic institutions that produce durable and effective countermeasures" (Zuboff, 2019a, p. 519).

### 4.2. Who gets told what in practice?

Having established a rudimentary understanding of the legal landscape, we will now turn to a discussion of practice. It is one thing to require disclosures under the law, and another thing altogether to discharge this duty in practice. It seems useful to have a brief look at how these disclosure laws work in practice by using a few short examples. These are by no means comprehensive, but as exemplars they suggest what matters are relevant to stakeholders, legislators, policymakers, and researchers like us, interested in influencing "the social ordering in an information civilization" (Zuboff, 2019b, p. 521). Specifically, the examples we have chosen demonstrate that the nature of data that can be breached varies hugely and, as a consequence, these breaches can have very different effects on both the organisation and the individuals involved. The examples also demonstrate some of the strategies organisations can recruit to avoid disclosing data breaches to the public, while still, ostensibly, operating within the law. We could have chosen any number of examples to illustrate this diversity of practice – those we have selected are just a few examples to highlight some of the most significant problems with current practice. These examples both point to the importance of a comprehensive mandatory disclosure regime and provide us with indicators on the extent, scope, and shape the regime should take.

We begin with an example from 2014 in which a cyber-attack on JP Morgan Chase compromised the accounts of its clients, including 76 million households and 7 million small businesses. Despite the hackers gaining "the highest level of administrative privilege" (Weise, 2014) JP Morgan claimed that the hackers had only stolen the names, addresses, phone numbers, and emails of some of its top account holders. After an internal assessment, the bank determined there was no evidence that fraud had resulted from the breach and that "critical data", such as account information, passwords, and social security numbers, had not been stolen. It made the decision not to disclose the breach to the individuals affected because on its assessment no "sensitive customer information was involved" in the breach – despite personal information about its account holders having been stolen (Murphy, 2014). Based on JP Morgan's own assessment of itself, it was able to elect not to disclose this information to its customers, and in so doing, muted a wider discussion about the vulnerability of data in the financial services sector – an unfortunate turn of events given breaches of data in this industry carry enormous risks for data providers. The scale of the breach made it impossible for JP Morgan to ignore, but while it discussed the breach publicly, pressured in part because the media and the sector had become aware of the issues, it used the opportunity to mute concerns about the seriousness of the event. In this case, the media applied some pressure to JP Morgan, but still, it insisted that there was no need for wider transparency around these events. Instead, it seems, it elected to make a wider statement about data security-related risks in its 2016 SEC filing in an attempt to inform stakeholders about the potential consequences, on the company, of data breaches: "[a] breach in the security of JP Morgan Chase's systems, or those of other market participants, could disrupt the Firm's businesses, result in the disclosure of confidential information, damage the Firm's reputation and create significant financial and legal exposure for the Firm" (USSEC, 2017). Had the bank been required to disclose the details of the 2014 breach *publicly*, the bank's clients would have been in a position to ask questions about data security in regard to that specific issue, but more broadly, this would have provided an opportunity to advocate for improved disclosure.

In another high-profile case, in 2015 a third-party software developer, Cambridge Analytica, harvested millions of Facebook user profiles of US voters and used them to build a model that could predict and influence voting behaviour. Eventually, Cambridge Analytica amassed information on 50 million Facebook users and then used this information to produce targeted political advertising to influence the outcome of the 2016 US presidential election campaign. The harvesting of data was exposed by Christopher Wylie, an ex-employee of Cambridge Analytica during interviews with *The Guardian* and the *New York Times*. Despite knowing the data had been breached, Facebook made no effort to disclose this to the public, making only limited attempts to secure the data of the affected users (Cadwalladr & Graham-Harrison, 2018). The SEC took this as a breach of the company's duties to accurately disclose the material risks

to its business and fined the company $100,000[1]. After conducting an investigation into Facebook's disclosures as they related to Cambridge Analytica, the US SEC stated in a press release dated July 24, 2019 (emphasis added), that:

> Facebook's public disclosures presented the risk of misuse of user data as merely hypothetical when Facebook knew that a third-party developer had actually misused Facebook user data. Public companies must identify and consider the material risks to their business and have procedures designed to make disclosures that are accurate in all material respects, *including not continuing to describe a risk as hypothetical when it has in fact happened*.

Facebook's decision to obfuscate the truth related to Cambridge Analytica suggests the enormity of risk that technology firms believe is attached to failures to keep user data secure. As part of the regulator's effort to recognise the material risks associated with data breaches, the SEC has emphasised that firms must disclose "cyber information that is significant or material" wherein "a *reasonable* investor would need to know about it" (Faitelson, 2018). Importantly, the breaches associated with Facebook's user data were never disclosed to the individuals affected, there was a considerable time lag between the events and any form of disclosure, and when they were disclosed, the information provided lacked clarity and precision. Like JP Morgan, Facebook policed itself. In doing so, it deemed the data breaches "hypothetical" and therefore not sufficiently known to warrant disclosure.

The health care sector also stores significant and highly sensitive personal data and is vulnerable to data breaches. Breaches of health data held by government agencies present a different challenge, partly because these agencies are not subject to any secondary disclosure requirements enacted by the SEC, and partly because governments hold in trust the data of every single citizen. In an Australian case, a cyber security researcher discovered that the Medicare and Pharmaceutical Benefits Scheme history of over 2.5 million people, which had been made public in a de-identified form through the Government's Open Data[2] initiative (DTA, 2020), could be re-identified. When the data was re-identified using simple technology, the researchers were able to access these individual's entire medical history, including medications the person had purchased and all of the medical tests they had undergone (Teague et al., 2017). The researchers informed the Government, arguing that the Government's "de-identification" and "Open Data" strategy was "unlikely to work for rich datasets in the governments care, like census data, tax records, mental health records, penal information and Centrelink data" (Teague et al., 2017). Instead of informing those citizens affected and reconsidering its Open Data policy, the Australian Government sought to amend the *Privacy Act 1988 (Cth)* to make it a criminal offence to re-identify published government data (Farrell, 2016). In correspondence dated September 14, 2018, the Secretary of Health, indicated that notifying individuals affected by data breaches would be too difficult (Beauchamp, 2018). Unlike those organisations subject to the notifiable data breach clauses in the *Privacy Act*, who are required to disclose the breach to the individual impacted if it is deemed "significant", the Australian Government is not required to inform any of the individuals affected by the Medicare data breach. Setting aside the importance of *public* disclosure, it is critical that the development of a mandatory reporting regime covers *all* organisational forms, including government departments and agencies.

While these examples paint a bleak picture, not all organisations try to avoid or obstruct their data breach disclosure responsibilities. Take the case of the Australian National University (ANU). In 2018, the ANU's databases were hacked leading to the theft of 19 years' worth of highly sensitive personal data (Reuters, 2019). The Vice-Chancellor made a public announcement about the breach two weeks after it was discovered, undertaking to produce and release a comprehensive report on the incident. When, in 2019, that report was made available, the Vice-Chancellor reiterated his commitment to public disclosure as a mechanism to support the public interest saying he "made this report public because it contains valuable lessons not just for ANU, but for all Australian organisations who are increasingly likely to be the target of cyber-attacks … I hope this report will help them protect themselves, and their data and their communities" (ANU, 2019, page 1). The University's decision to discuss the breach publicly was a choice made within the organisation, but it signalled the power and importance of wider public disclosures of these events to trigger discussion about intensifying cyber-attacks and the growing importance of robust approaches to data security. That said, just as at JP Morgan, Facebook, and Medicare, the University decided not to notify the affected parties because it deemed that there was no "evidence their data has been misused" (ANU, 2019, p. 2).

In all of these examples, it is clear that self-governance of data breach-related disclosure continues, despite the existence of laws and listing rules. Indeed, the law has been ineffective. As these examples show, in self-assessing the impact of breaches, organisations have been able to avoid informing individuals, and in some cases, they have avoided informing the regulator and/or the market. Where there is disclosure, it appears to fail on two critical measures: specific disclosure that might notify an individual that their data had been stolen (even if the organisation itself did not believe the theft had led to the data being "compromised") is not undertaken, nor is the kind of wider disclosure that might meaningfully inform a public debate about the data security obligations of organisations. Given this, and what we now know about surveillance capitalism, in the following section we propose a mandatory framework for data breach disclosures that seeks to address both these limits in current practice.

[1] More recently, the US Federal Trade Commission approved a $5 billion settlement with Facebook after investigating the way the company handled user data in relation to the matters pertaining to Cambridge Analytica (Reuters, 2019).

[2] The Open Data initiative publishes information that is collected during the normal course of government because it is thought that "making data open has economic and social benefits" because according to the site, most often "the government agency publishing the data cannot foresee its future use, or how it might be combined with other data or displayed in a program, interface or tool". As would be expected, the information is supposed to be "anonymised prior to release" to "ensure the highest privacy standards are met, and security is not breached" (DTA, 2020).

## 5. A framework for data breach disclosures

Given the variability in rules and practices, we suggest that a systematic data breach disclosure framework for public and private sector organisations, will, at the very least, create *public* opportunities to discuss a wide set of data related issues. Primarily, a mandatory framework would need to insist on the public provision of data security-related information so that stakeholders, and more specifically the individuals who provide their data to an organisation, can start to form a picture of risk and relativities across the many organisations and sectors that hold our data in trust. In a very practical sense, a mandatory disclosure framework picks up on Zuboff's (2019a) insistence that we must name surveillance capitalism in order to tame it. In her words, we must mobilise a suite of tools that begin to make it possible to describe and discuss surveillance capitalism and instrumentarian power to "equip us to intercept these mechanisms of dispossession, reverse their action [and] produce urgently needed friction" (Zuboff, 2019a, p. 347). As we have established earlier, surveillance capitalism turns a huge variety of information about us – such as our birth dates, our song preferences, our typing speed – into data objects that are ontologically ambiguous, difficult to conceptualise, and, as a consequence, difficult to claim as our own. While we have acknowledged that disclosures should not *stand in for* organisational accountability, when mobilised to represent things that are designed to be occluded and unknowable, they are critical to the possibility of organisational accountability. On this basis, in making data breach-related information *publicly* available, disclosures might be usefully recruited to help establish the basis for a robust discussion about data, its uses, its value, and its security – naming it so we can start taming it (Beraldo & Milan, 2019).

In focusing on data breaches in the previous sections, we have shown how the rules that govern these disclosures allow for significant judgement and self-governance, and that this produces variability, inconsistency, and further opacity. This is a view supported by Alazab et al. (2021, p. 28) who argue that "proactive and timely notification of data breaches" is essential. While specific details might be explained away by jurisdictional issues, at present, even if the thresholds for disclosure are met, this only takes place between the organisation and the regulator, or the organisation and the individual – there are no requirements, anywhere, to make a *public* disclosure of any kind. We propose the following disclosure framework as a means to ensure the public availability of information that would help stimulate and democratise a wider debate about data (see Fig. 1).

Within the "minimum data breach disclosure framework" (Fig. 1), the first five proposed disclosures have been developed in response to the limits of the law and practice outlined earlier, because, despite nearly two decades since the "invention of surveillance capitalism, existing law, largely centred on privacy and antitrust, have been insufficient to disrupt its growth" (Zuboff, 2019a, p. 344). In order to address these limitations, an organisation subject to the framework proposed here would, first, be required to inform the public as to the type of data that has been breached, and whether or not as a result of the breach individuals can be identified; second, it would be required to provide information about the level of sensitivity of the data involved, so that the public can start to form an independent assessment of the potential level of harm; third, the organisation would be required to be explicit about the cause of the breach, whether it occurred by accident or as a result of criminal activity; fourth, both the number of people affected by the breach and its overall size would need to be made clear, and fifth, in an effort to encourage the timely communication of information, the organisation would be required to provide the dates of each breach. The final two disclosures are intended to broaden the context, with the sixth requiring organisations to indicate how they have responded to their legal obligations as a means to expose current laws to wider critique and to animate discussions about the appropriate organisational response to a data breach; the seventh has been designed to encourage organisations to be explicit about the actions they have taken to assess data risks and to improve the security of data in their care. While we are fully aware the framework is more pragmatic than it is radical, the naming of these data issues through a formal and mandatory process would help curtail an organisation's ability to self-regulate and to use its own judgement to determine the appropriate disclosure pathway.

Without mandatory disclosures of this kind, disclosure is only required if an organisation has triggered a listing rule or a law, and even then, the organisation is able to self-assess the level of risks. And, as we have seen in the case of Facebook, in claiming that the breaches were "hypothetical" in nature it determined that the law had not been triggered; similarly, JP Morgan decided there was no evidence that the data breached had been "compromised", thereby avoiding disclosure; and the Australian Government intervened to

| Minimum Data Breach Disclosures |
|---|
| 1. **Type of data breached:** identified or de-identified |
| 2. **Sensitivity of data breached:** personal data or personal data likely to result in serious harm |
| 3. **Cause of data breach:** indicating human error or cyber-attack |
| 4. **Size of data breached:** number of individuals affected and total size of breach |
| 5. **Date of data breach:** data breach event; date of disclosure to affected individuals; method of disclosure |
| 6. **Indication of data disclosure laws triggered or potentially triggered by a data breach:** Law; Listing Rules |
| 7. **Data risk mitigation:** analysis undertaken; strategies adopted |

**Fig. 1.** Proposed minimum data breach disclosure framework.

ensure individuals would not be notified of the Medicare data breach, citing issues of scale and the commercial and public benefit of "open access" de-identified data. This is disappointing because, in practice, a well-designed legal framework can make it incumbent on the organisation to formally notify individuals, the regulator, and the public of a breach. In Europe, where the GDPR's definition of data subjects places individuals as the ultimate owners of their own information, data has been conceptualised within the law as an object relating to personhood. This makes it possible for individuals to foster a sense of proprietorship over their data in a similar way we might articulate the ownership of something material that is given, lent, or offered as collateral in exchange for some other good or service. When we begin to imagine the data that relates to a person *as the property of that person*, then a mandatory disclosure framework will be an important mechanism to ensure that property is being used and managed appropriately; it is also an important means through which data can be made discussable.

At its simplest, our proposed data breach disclosure framework encourages the production and communication of annual disclosures that are timely, comparable, and *publicly* available. Beyond this, it has the potential to broaden awareness of the risks borne by "data subjects". In bringing this information together in one place, stakeholders will have a foundation upon which to start to assess data security and to talk about data rights in ways that can begin to address the "wealth and power wielded by data capitalists" (Sadowski, 2019, p. 9).

## 6. Conclusion

If, as Sadowski (2019, p. 2) argues, "datafication takes shape as a political, economic regime driven by the logic of perpetual (data) capital accumulation and circulation", then it is imperative critical accounting scholarship tackles the many issues arising from big data. There is no doubt that a range of strategies need to be mobilised to exert control over our digital lives and reclaim the future from surveillance capitalists. But it seems to us that, within this wider project, disclosures, particularly when *mandated* and *public*, can challenge the rise of instrumentarian power and the accompanying lack of accountability. Disclosures seem particularly relevant here given that surveillance capitalism has "been crafted in secrecy and designed [to be] fundamentally illegible" (Zuboff 2019a, p. 344). Indeed, it is possible that disclosures, despite their limitations, might help make visible and legible the underlying economic logics and associated social consequences of this new form of capitalism. We agree with Crawford (2021, p. 227) that reclaiming the future will rely on "the growing justice movements that address the interconnectedness of capitalism, computation and control".

In taking this possibility seriously, we have tried to scope the political potency of disclosures within the context of surveillance capitalism and its accompanying "instrumentarian" form of power (Zuboff, 2019a, p. 8). In doing so, we have made the case for disclosures as an important, if not essential, tool in our efforts to ensure the ontological peculiarities of behavioural data become legible and discussable. Alongside the obvious inclusion of new "subjects" of disclosure, it seems to us that the real power of disclosure within the data economy will lie in our ability to make ontologically ambiguous objects *knowable*.

In making the case for disclosures as a means to combat the occluded nature of the data economy, we have proposed that there is an important conceptual distinction between the potency of disclosures that relate to issues *we are aware of* (such as environmental pollution and labour exploitation), from disclosures that relate to *issues of which we are not aware* (such as the market for our "behavioural surplus" data). With this as the conceptual frame, we have focused our paper on the role disclosures might play as a means to achieve some practical improvements to data security, but also, more ambitiously, as a means to encourage a wider public dialogue about data, its use, and our rights. We acknowledge that the challenges presented by surveillance capitalism extend well beyond security issues, but given it is increasingly difficult to engage with organisations without sharing personal data of some kind – even if it feels innocuous, like the provision of names and email addresses – we see data security issues as providing an appropriate anchor to the conceptual explorations posed in this paper. In showing how difficult it is for an individual to determine if the data they have provided an organisation has been breached, we have built on Zuboff's (2019a) work to argue that it is this sustained *un-discoverability* within the data economy that has made it so difficult to craft a coherent political response to the challenges posed by surveillance capitalism. In response, we have argued that the introduction of some form of mandatory disclosure regime offers an (albeit imperfect) means through which to conceptualise data as an object that *can and should be knowable and known*. In mandating these disclosures, data begins to take on an empirical shape that can be acted on to secure the interests of individuals and through which we may be able to reclaim our social and political futures.

In our effort to bring some of the dynamics of surveillance capitalism into view, we have mapped the current status of data breach-related rules, both as they pertain to the requirements inscribed in the law and the Listing Rules of stock exchanges; we have highlighted the diversity of practices, providing a number of examples of private and public sector organisational responses; and finally, we have proposed a framework for publicly available, uniform and timely data breach disclosures that could form the basis of future discussions within the literature on social accounting and extended responsibility reporting. Given that data breaches are increasingly common, most of us might expect that we would be informed if our sensitive personal data had been breached, and we have shown here that this is often not the case. It is also very unlikely that we would be made aware of data breaches that do not affect us directly, despite the importance of this information as part of the wider public debate about the data obligations of powerful private and public sector organisations. And while it is clear that regulators across the globe have been actively reshaping laws to encourage data breach-related disclosures, these disclosures are hugely variable and organisations retain considerable power to determine whether they report them and to whom. And even in cases where an organisation's self-assessment of risk leads it to disclose a breach to the regulator and/or individuals, there are no obligations for an organisation to disclose these data breaches *publicly*.

It is important to acknowledge that regulators are constrained by the ideological imposition of neoliberalism, turning socio-political matters of government into technical matters of governance. Most are unwilling to constrain capital, preferring instead to act as a collaborator working towards a mutually agreed consensus about what should and should not be subject to the law. Indeed, as

Morales et al. (2014, p. 426) point out, we are very much amidst a kind of third wave of neoliberalisation "in which members of central governments and public servants increasingly think and behave like entrepreneurs". Data regulation is new, and changing rapidly but, in keeping with the powerful influence of neoliberal ideas on the role of regulators, the asymmetries of concern between states, capital, and citizens are perhaps predictable. While data breaches pose material risks, in the context of third wave neoliberalisation, regulators have crafted data breach disclosure rules from the perspective of organisations, as if this will, in turn, serve the interests of citizens (Morales et al., 2014). As Jones and Hameiri (2021, p. 8) point out, the state's capacity "to secure desired policy outcomes has been severely hollowed out" under neoliberalism.

We agree with Jones and Hameiri's argument (2021, p. 21) that effective regulation of surveillance capitalism will take "a new democratic movement" that can "re-subordinate state institutions to the needs and wishes of citizens, establishing clear lines of responsibility, accountability and control". In response to this, we have proposed a minimum data breach disclosure framework that responds practically to these specific dilemmas, while also starting to make the hidden life of data discussable: after all, "taming surveillance capitalism must begin with careful naming" (Zuboff, 2019a, p. 61). Disclosures, like the ones we propose here, will never offer a full or complete representation of practice, nor should we think about the disclosure of data breaches as an end in and of itself. Instead, we see disclosures as an important catalyst for a widening public conversation about data rights, data security, and datafication more broadly. Given that "concerns about data use can be held in tandem with a desire for, acceptance of, or even resignation towards (corporate) data gathering practices" (Pridmore & Mols, 2020, p. 10), the more we understand how data is used and maintained, the more able we are to assess our willingness to provide data to public and private sector organisations. That said, disclosures without political will are unlikely to have much effect, but political will is impossible to mobilise without making some information publicly available. This double bind is difficult to overcome but, for now, given the legal and practical inconsistency associated with data breaches across the world, our proposed framework is an important step towards a more invigorated and richer public dialogue about data, its use, and our rights. All of this is imperfect, but if we have any chance of "reawakening our astonishment and sharing a sense of righteous indignity" (Zuboff, 2019a, p. 395), critical researchers in accounting must play a role. Initially, at least, accounting academics can help "establish our bearings", a call we take up in our choice to critique the legal arrangements that shape data breach disclosures in the emerging surveillance economy and to suggest an alternative that might "enthuse us" (Zizek, 2011, p. 237) into political actions designed to craft a genuinely human future from our digital life. While it is impossible to offer a completely comprehensive appraisal of current law and practice, in providing exemplars we have signalled the importance of further research into the data economy, a critical step if we are to destabilise instrumentarian forms of power that see our personal data extracted "with little regard for consent and compensation" (Sadowski, 2019, p. 1).

Critical accounting researchers have the potential to contribute to our understandings of big data as a means to extract value and direct behaviours and we can do this in a variety of ways across a wide range of settings. To begin, it might be worth building a picture of data related disclosures across a wide range of organisations and from a variety of perspectives so as to support further analysis. Beyond this, it will be important to understand the drivers of these disclosures from the perspective of the organisation and the regulators; the ways in which organisations conceptualise the scope of this kind of disclosure; the ways cultural or jurisdictional differences might influence the formulation of data disclosure laws and practices; and how well these disclosures are able to reflect actual practices, especially given the velocity of technological change. It will also be important to understand how individuals respond to these disclosures; whether disclosure provides a mechanism to responsibilise the individual for data management and/or the effects of the breach on them personally; it might also be useful to explore whether data related disclosures shift (or embed) particular views about the data economy; and beyond this, how we might start to account for all of the data that is offered up to surveillance capitalists for free.

We also encourage critical researchers to collaborate with stakeholders to bring together expertise that will help articulate new forms of regulation to shape the digital economy *for us* (Crawford, 2021). This is but one way to mould the data economy that serves us as a community, to restore the possibilities of democratically negotiated political and economic futures. Future research might look to new forms of activism that try to "jam" the collection of data; counter accounts of data collection that draw from activists and civil society; digitally enabled leaking and whistleblowing that exposes the data habits of organisations; and perhaps even examine the new data disclosure documents that are being maintained and produced for users of all kinds of online platforms such as Facebook, Twitter, and even Netflix and Spotify. No doubt there is more to do but given the profound changes to the dynamics of profiteering that have become possible because of the growth in big data, critical researchers in accounting are beginning to make sense of this new form of capitalism. If we can help make the surveillance economy *knowable*, there is a real chance we can help shape a future that socialises and democratises the many extraordinary possibilities of technology and data.

## Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## References

Aho, B., & Duffield, R. (2020). Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China. *Economy and Society, 49*(2), 187–212. https://doi.org/10.1080/03085147.2019.1690275

Alazab, M., Hong, S. H., & Ng, J. (2021). Louder bark with no bite: Privacy protection through the regulation of mandatory data breach notification in Australia. *Future Generation Computer Systems, 116*, 22–29. https://doi.org/10.1016/j.future.2020.10.017

Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies, 23*(3), 1177–1206. https://doi.org/10.1007/s11142-018-9452-4
Andrew, J., & Baker, M. (2019). The General Data Protection Regulation in the age of surveillance capitalism. *Journal of Business Ethics, 168*(3), 565–578. https://doi.org/10.1007/s10551-019-04239-z
Andrew, J., & Baker, M. (2020a). For emancipation: A Marxist critique of structure within critical realism. *Accounting, Auditing & Accountability Journal, 33*(3), 641–653. https://doi.org/10.1108/AAAJ-11-2019-4251
Andrew, J., & Baker, M. (2020b). The radical potential of leaks in the shadow accounting project: The case of US oil interests in Nigeria. *Accounting, Organizations and Society, 82*, 101101. https://doi.org/10.1016/j.aos.2019.101101
Andrew, J., & Cortese, C. (2011). Accounting for climate change and the self-regulation of carbon disclosures. *Accounting Forum, 35*(3), 130–138. https://doi.org/10.1016/j.accfor.2011.06.006
Andrew, J., & Cortese, C. (2013). Free market environmentalism and the neoliberal project: The case of the Climate Disclosure Standards Board. *Critical Perspectives on Accounting, 24*(6), 397–409. https://doi.org/10.1016/j.cpa.2013.05.010
ANU. (2019). *ANU incident report on the breach of the Australian National University's administrative systems*. https://apo.org.au/node/262171.
Ball, K., & Webster, W. (2020). Big data and surveillance: Hype, commercial logics and new intimate spheres, 205395172092585 *Big Data & Society, 7*(1). https://doi.org/10.1177/2053951720925853.
Barocas, S., & Nissenbaum, H. (2014). Big data's end run around procedural privacy protections. *Communications of the ACM, 57*(11), 31–33. https://doi.org/10.1145/2668897
Barron, O. E., & Qu, H. (2014). Information asymmetry and the ex ante impact of public disclosure quality on price efficiency and the cost of capital: Evidence from a laboratory market. *The Accounting Review, 89*(4), 1269–1297. https://doi.org/10.2308/accr-50715
Barth, M. E., Clinch, G., & Shibano, T. (2003). Market effects of recognition and disclosure. *Journal of Accounting Research, 41*(4), 581–609. https://doi.org/10.1111/1475-679x.00117
Barth, M. E., & Schipper, K. (2008). Financial reporting transparency. *Journal of Accounting, Auditing & Finance, 23*(2), 173–190. https://doi.org/10.1177/0148558x0802300203
G. Beauchamp Letter to Professor Glyn Davis AC 2018 https://www.righttoknow.org.au/request/6092/response/16930/attach/5/Document%201%20Letter%20to%20Professor%20Glyn%20Davis%20AC%2014%20September%202018%20FOI%201511.pdf.
Bebbington, J., Schneider, T., Stevenson, L., & Fox, A. (2020). Fossil fuel reserves and resources reporting and unburnable carbon: Investigating conflicting accounts. *Critical Perspectives on Accounting, 66*, 102083. https://doi.org/10.1016/j.cpa.2019.04.004
Ben-Amar, W., Bujaki, M., McConomy, B., & McIlkenny, P. (2021). Gendering merit: How the discourse of merit in diversity disclosures supports the gendered status quo on Canadian corporate boards. *Critical Perspectives on Accounting, 75*, 102170. https://doi.org/10.1016/j.cpa.2020.102170
Beraldo, D., & Milan, S. (2019). From data politics to the contentious politics of data, 205395171988596 *Big Data & Society, 6*(2). https://doi.org/10.1177/2053951719885967.
Brown, J. (2009). Democracy, sustainability and dialogic accounting technologies: Taking pluralism seriously. *Critical Perspectives on Accounting, 20*(3), 313–342. https://doi.org/10.1016/j.cpa.2008.08.002
Brown, J., & Dillard, J. (2013). Agonizing over engagement: SEA and the "death of environmentalism" debates. *Critical Perspectives on Accounting, 24*(1), 1–18. https://doi.org/10.1016/j.cpa.2012.09.001
Brown, J., & Tregidga, H. (2017). Re-politicizing social and environmental accounting through Rancière: On the value of dissensus. *Accounting, Organizations and Society, 61*, 1–21. https://doi.org/10.1016/j.aos.2017.08.002
Brown, W. (2019). *In the Ruins of Neoliberalism: The Rise of Antidemocratic Politics in the West (The Wellek Library Lectures)*. Columbia University Press.
Bryer, A. R. (2014). Participation in budgeting: A critical anthropological approach. *Accounting, Organizations and Society, 39*(7), 511–530. https://doi.org/10.1016/j.aos.2014.07.001
Cadwalladr, C., & Graham-Harrison, E. (2018). March 18). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.
Cardullo, P. (2015). Hacking multitude' and big data: Some insights from the Turkish 'digital coup, 205395171558059 *Big Data & Society, 2*(1). https://doi.org/10.1177/2053951715580599.
Catchpowle, L., Cooper, C., & Wright, A. (2004). Capitalism, states and ac-counting. *Critical Perspectives on Accounting, 15*(8), 1037–1058. https://doi.org/10.1016/s1045-2354(02)00214-9
Cho, C. H., Guidry, R. P., Hageman, A. M., & Patten, D. M. (2012). Do actions speak louder than words? An empirical investigation of corporate environmental reputation. *Accounting, Organizations and Society, 37*(1), 14–25. https://doi.org/10.1016/j.aos.2011.12.001
Cooper, C., Taylor, P., Smith, N., & Catchpowle, L. (2005). A discussion of the political potential of social accounting. *Critical Perspectives on Accounting, 16*(7), 951–974. https://doi.org/10.1016/j.cpa.2003.09.003
Cousins, J., & Sikka, P. (1993). Accounting for change: Facilitating power and accountability. *Critical Perspectives on Accounting, 4*(1), 53–72. https://doi.org/10.1006/cpac.1993.1003
Craig, R. J., & Amernic, J. H. (2004). Enron discourse: The rhetoric of a resilient capitalism. *Critical Perspectives on Accounting, 15*(6–7), 813–852. https://doi.org/10.1016/J.CPA.2002.12.001
Crawford, K. (2021). *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. Yale University Press.
Digital Transformation Agency (DTA). (2020). Open data. *Digital Transformation Agency*. https://www.dta.gov.au/help-and-advice/guides-and-tools/requirements-australian-government-websites/open-data.
Dillard, J., & Vinnari, E. (2017). A case study of critique: Critical perspectives on critical accounting. *Critical Perspectives on Accounting, 43*, 88–109. https://doi.org/10.1016/j.cpa.2016.09.004
Ejiogu, A., Ambituuni, A., & Ejiogu, C. (2021). Accounting for accounting's role in the neoliberalization processes of social housing in England: A Bourdieusian perspective. *Critical Perspectives on Accounting, 80*, 102053. https://doi.org/10.1016/j.cpa.2018.07.002
Faitelson, Y. (2018, August 13). SEC's new toughness on breach reporting and what it means for your it compliance. Forbes. https://www.forbes.com/sites/forbestechcouncil/2018/08/13/secs-new-toughness-on-breach-reporting-and-what-it-means-for-your-it-compliance/?sh=72e16c4ea67d.
Farrell, P. (2016). *September 29)*. The Guardian: Research work could be criminalised under George Brandis data changes. https://www.theguardian.com/world/2016/sep/29/george-brandis-to-criminalise-re-identifying-published-government-data.
Fourcade, M., & Kluttz, D. N. (2020). A Maussian bargain: Accumulation by gift in the digital economy, 205395171989709 *Big Data & Society, 7*(1). https://doi.org/10.1177/2053951719897092.
Gallhofer, S., & Haslam, J. (2019). Some reflections on the construct of emancipatory accounting: Shifting meaning and the possibilities of a new pragmatism. *Critical Perspectives on Accounting, 63*, 101975. https://doi.org/10.1016/j.cpa.2017.01.004
Godowski, C., Nègre, E., & Verdier, M. A. (2020). Toward dialogic accounting? Public accountants' assistance to works councils – A tool between hope and illusion. *Critical Perspectives on Accounting, 69*, Article 102095. https://doi.org/10.1016/j.cpa.2019.102095
Gray, R., & Milne, M. J. (2018). Perhaps the Dodo should have accounted for human beings? Accounts of humanity and (its) extinction. *Accounting, Auditing & Accountability Journal, 31*(3), 826–848. https://doi.org/10.1108/aaaj-03-2016-2483
Gumb, B. (2007). What is shown, what is hidden: Compulsory disclosure as a spectacle. *Critical Perspectives on Accounting, 18*(7), 807–828. https://doi.org/10.1016/j.cpa.2006.06.001
Haslam, J., Chabrak, N., & Kamla, R. (2019). Emancipatory accounting and corporate governance: Critical and interdisciplinary perspectives. *Critical Perspectives on Accounting, 63*, 102094. https://doi.org/10.1016/j.cpa.2019.102094
Hull, G. (2015). Successful failure: What Foucault can teach us about privacy self-management in a world of Facebook and big data. *Ethics and Information Technology, 17*(2), 89–101.

Introna, L., & Pouloudi, A. (1999). Privacy in the information age: Stakeholders, interests and values. *Journal of Business Ethics, 22*, 27–38. https://doi.org/10.1023/A:1006151900807
Jones, L., & Hameiri, S. (2021). COVID-19 and the failure of the neoliberal regulatory state. *Review of International Political Economy, 1–25*. https://doi.org/10.1080/09692290.2021.1892798
Khan, H. Z., Bose, S., & Johns, R. (2020). Regulatory influences on CSR practices within banks in an emerging economy: Do banks merely comply? *Critical Perspectives on Accounting, 71*, 102096. https://doi.org/10.1016/j.cpa.2019.102096
Kulwin, N. (2019). *February 25)*. Intelligencer: Shoshana Zuboff on surveillance capitalism's threat to democracy. https://nymag.com/intelligencer/2019/02/shoshana-zuboff-q-and-a-the-age-of-surveillance-capital.html.
Lake, R. W. (2017). Big Data, urban governance, and the ontological politics of hyperindividualism, 205395171668253 *Big Data & Society, 4*(1). https://doi.org/10.1177/2053951716682537.
Lauwo, S., Kyriacou, O., & Julius Otusanya, O. (2020). When sorry is not an option: CSR reporting and 'face work' in a stigmatised industry – A case study of Barrick (Acacia) gold mine in Tanzania. *Critical Perspectives on Accounting, 71*, 102099. https://doi.org/10.1016/j.cpa.2019.102099
Lehtiniemi, T., & Kortesniemi, Y. (2017). Can the obstacles to privacy self-management be overcome? Exploring the consent intermediary approach, 2053951717721935 *Big Data & Society, 4*(2). https://doi.org/10.1177/2053951717721935.
Lending, C., Minnick, K., & Schorno, P. J. (2018). Corporate Governance, social responsibility, and data breaches. *Financial Review, 53*(2), 413–455. https://doi.org/10.1111/fire.2018.53.issue-210.1111/fire.12160
Leong, S., & Hazelton, J. (2019). Under what conditions is mandatory disclosure most likely to cause organisational change? *Accounting, Auditing & Accountability Journal, 32*(3), 811–835. https://doi.org/10.1108/aaaj-12-2015-2361
Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique, 2053951714541861 *Big Data & Society, 1*(2). https://doi.org/10.1177/2053951714541861.
Madden, M. (2014). November 12). *Public Perceptions of Privacy and Security in the Post-Snowden Era. Pew Research Center: Internet, Science & Tech.* https://www.pewresearch.org/internet/2014/11/12/public-privacy-perceptions/.
Malmgren, E. (2019). Resisting "big other": What will it take to defeat surveillance capitalism? *New Labor Forum, 28*(3), 42–50. https://doi.org/10.1177/1095796019864097
Matwyshyn, A. M. (2009). CSR and the corporate cyborg: Ethical corporate information security practices. *Journal of Business Ethics, 88*(S4), 579–594. https://doi.org/10.1007/s10551-009-0312-9
Michelon, G., Pilonato, S., & Ricceri, F. (2015). CSR reporting practices and the quality of disclosure: An empirical analysis. *Critical Perspectives on Accounting, 33*, 59–78. https://doi.org/10.1016/j.cpa.2014.10.003
Miles, S., & Ringham, K. (2019). The boundary of sustainability reporting: Evidence from the FTSE100. *Accounting, Auditing & Accountability Journal, 33*(2), 357–390. https://doi.org/10.1108/aaaj-05-2018-3478
Miller, P., & Power, M. (2013). Accounting, organizing, and economizing: Connecting accounting research and organization theory. *Academy of Management Annals, 7*(1), 557–605. https://doi.org/10.5465/19416520.2013.783668
Minister for Justice. (2020). The Personal Information Protection and Electronic Documents Act (PIPEDA). *Office of the Privacy Commissioner of Canada.* https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/.
Morales, J., Gendron, Y., & Guénin-Paracini, H. (2014). State privatization and the unrelenting expansion of neoliberalism: The case of the Greek financial crisis. *Critical Perspectives on Accounting, 25*(6), 423–445. https://doi.org/10.1016/j.cpa.2013.08.007
Mouffe, C. (2018). *For a Left Populism*. Verso.
Mouritsen, J. (2011). The operation of representation in accounting: A small addition to Dr. Macintosh's theory of accounting truths. *Critical Perspectives on Accounting, 22*(2), 228–235. https://doi.org/10.1016/j.cpa.2010.06.015
Murphy, M. M. (2014, October). *JPMorgan Data Breach Involves Information on 76 Million Households, 7 Million Small Businesses*. https://fas.org/sgp/crs/misc/breach.pdf.
Neto, N. N., Madnick, S., Paula, A. M. G. D., & Borges, N. M. (2021). Developing a global data breach database and the challenges encountered. *Journal of Data and Information Quality, 13*(1), 1–33. https://doi.org/10.1145/3439873
Office of the Australian Information Commissioner (OAIC). (2020). *Notifiable Data Breaches Report: July–December 2020*. OAIC. https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2020/.
Osman, M., Gallhofer, S., & Haslam, J. (2021). Contextualising and critically theorising corporate social responsibility reporting: Dynamics of the late Mubarak era in Egypt. *Critical Perspectives on Accounting, 74*, 102166. https://doi.org/10.1016/j.cpa.2020.102166
Peacock, S. E. (2014). How web tracking changes user agency in the age of big data: The used user, 205395171456422 *Big Data & Society, 1*(2). https://doi.org/10.1177/2053951714564228.
Perkiss, S., Bernardi, C., Dumay, J., & Haslam, J. (2020). A sticky chocolate problem: Impression management and counter accounts in the shaping of corporate image. *Critical Perspectives on Accounting*, 102229. https://doi.org/10.1016/j.cpa.2020.102229
Pesci, C., Costa, E., & Andreaus, M. (2020). Using accountability to shape the common good. *Critical Perspectives on Accounting, 67-68*, 102079. https://doi.org/10.1016/j.cpa.2019.03.001
Pridmore, J., & Mols, A. (2020). Personal choices and situated data: Privacy negotiations and the acceptance of household Intelligent Personal Assistants, 205395171989174 *Big Data & Society, 7*(1). https://doi.org/10.1177/2053951719891748.
Reuters. (2019, July 13). Facebook to be fined $US5 billion for Cambridge Analytica privacy violations, reports say. *ABC News*. https://www.abc.net.au/news/2019-07-13/facebook-5-billion-dollar-fine-cambridge-analytica-privacy/11306324.
Roberts, J. (1991). The possibilities of accountability. *Accounting, Organizations and Society, 16*(4), 355–368. https://doi.org/10.1016/0361-3682(91)90027-c
Roberts, J. (2009). No one is perfect: The limits of transparency and an ethic for 'intelligent' accountability. *Accounting, Organizations and Society, 34*(8), 957–970. https://doi.org/10.1016/j.aos.2009.04.005
Roberts, J. (2018). Managing only with transparency: The strategic functions of ignorance. *Critical Perspectives on Accounting, 55*, 53–60. https://doi.org/10.1016/j.cpa.2017.12.004
Roberts, J. (2021). The boundary of the 'economic': Financial accounting, corporate 'imaginaries' and human sentience. *Critical Perspectives on Accounting, 76*, 102203. https://doi.org/10.1016/j.cpa.2020.102203
Rose, N. (1993). Government, authority and expertise in advanced liberalism. *Economy and Society, 22*(3), 283–299. https://doi.org/10.1080/03085149300000019
Ruppert, E., Isin, E., & Bigo, D. (2017), 205395171771774 *Data politics. Big Data & Society, 4*(2). https://doi.org/10.1177/2053951717717749.
Sadowski, J. (2019). When data is capital: Datafication, accumulation, and extraction, 205395171882054 *Big Data & Society, 6*(1). https://doi.org/10.1177/2053951718820549.
Securities and Exchange Commission (SEC). (2018, February). *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*. https://www.sec.gov/rules/interp/2018/33-10459.pdf.
Spence, C. (2009). Social accounting's emancipatory potential: A Gramscian critique. *Critical Perspectives on Accounting, 20*(2), 205–227. https://doi.org/10.1016/j.cpa.2007.06.003
Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally, 205395171773633 *Big Data & Society, 4*(2). https://doi.org/10.1177/2053951717736335.
Teague, V., Culnane, C., & Rubinstein, B. (2017). *December)*. Pursuit: The simple process of re-identifying patients in public health records. https://pursuit.unimelb.edu.au/articles/the-simple-process-of-re-identifying-patients-in-public-health-records.
Thatcher, J. (2014). Big data, big questions| Living on fumes: Digital footprints, data fumes, and the limitations of spatial big data. *International Journal of Communication, 8*, 19.

Tregidga, H. (2017). "Speaking truth to power": Analysing shadow reporting as a form of shadow accounting. *Accounting, Auditing & Accountability Journal, 30*(3), 510–533. https://doi.org/10.1108/aaaj-01-2015-1942

Uche, C., & Khalid, S. (2021). Corporate reporting on conflict: A struggle over land. *Critical Perspectives on Accounting*, 102340. https://doi.org/10.1016/j.cpa.2021.102340

Securities and Exchange Commission (USSEC). (2017). J.P. Morgan Chase & Co. Form 10 K. https://sec.report/Document/0000019617-18-000057/.

Venkatesh, N. (2021). Surveillance capitalism: A Marx-inspired account. *Philosophy, 96*(3), 359–385. https://doi.org/10.1017/s0031819121000164

Viale, T., Gendron, Y., & Suddaby, R. (2017). From "mad men" to "math men": The rise of expertise in digital measurement and the shaping of online consumer freedom. *Accounting, Auditing & Accountability Journal, 30*(2), 270–305. https://doi.org/10.1108/aaaj-12-2014-1887

E. Weise October 3). JP Morgan reveals data breach affected 76 million households 2014 USA TODAY.

Weiskopf, R. (2019). Book review: *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*. *Organization, 27*(6), 975–978. https://doi.org/10.1177/1350508419842708

J. Westerlind Arent Fox 2019 Survey of Data Breach Notification Statutes 2019 https://www.jdsupra.com/post/contentViewerEmbed.aspx?fid=8b4cfbdc-fb2b-46aa-98d5-91e7689dd676.

Zizek, S. (2011). Did Somebody Say Totalitarianism?: 5 Interventions in the (Mis)Use of a Notion (The Essential Zizek) (Second Edition). Verso.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30*(1), 75–89. https://doi.org/10.1057/jit.2015.5

Zuboff, S. (2019a). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile Books.

Zuboff, S. (2019b). Surveillance capitalism and the challenge of collective action. *New Labor Forum, 28*(1), 10–29. https://doi.org/10.1177/1095796018819461