Surveillance & Society

Book Review

Review of Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs.

704 pp. Hardcover. US $38.00. ISBN: 9781610395694.

Kirstie Ball

University of St. Andrews, UK
Kirstie.Ball@st-andrews.ac.uk

In 2006, when I worked for the Open University (OU), one of my many teaching assignments was to write a study unit on the controversies of corporate power. The unit was to be the final element of a level-one module called *Introduction to Business*. The module was studied by thousands of people in diverse occupations, from submariners to ballerinas, soldiers to aid workers, cleaners to prisoners, and everything in between.

I have always been an advocate of incorporating critical perspectives into business teaching, a teaching philosophy I have followed to the present day. As I had to convince an army of OU tutors that this was a worthwhile task, I decided to approach the topic of corporate power through the use of a film—a 2006 documentary entitled *Google: Behind the Screen*[1] by Dutch director Ijsbrand van Veelen. This documentary features Google execs who paint a picture of a primary-coloured employment utopia that is committed to the society-corporate win-win of end-user satisfaction in search. Its scientific recruitment techniques and the superior working conditions in "The Plex" were lauded. Marissa Meyer, who at the time was Google's vice president, explains the company's commitment to its motto "Don't be evil," and Vint Cerf (captioned as Vice President and Chief Internet Evangelist) explains the superior basis for their search-ranking algorithm. Both talk with an unblinking enthusiasm, reminiscent of scientology recruiters, as they characteristically deny any question of the company's motives. Meyer counters the question "Are you a big brother company?" with a giggle, saying, "I'm sorry, that's just not my view." Cerf, when considering the question as to whether users should trust the content displayed in a google search, turns the question on van Veelen, himself, asking the viewer to consider whether his account of the company should be trusted. Attack is the best form of defence. Ian Brown (then at the Open Rights Group) summarised concerns about monopolistic surveillant behaviours. Others were concerned with some of the unpleasant pages being unearthed by various searches—holocaust denial, for example—for which, in a now familiar move, the company abrogated all responsibility. This was fertile ground for teaching corporate power.

Looking back over my tutorial notes is oddly reassuring. I note that the organization characterises itself as "childlike," which "sharply contrasts with its massive economic power and its core mission to organize the world's information." I direct tutors to question Meyer's neoliberal inflection that it is important for the user

[1] https://www.singularityweblog.com/google-behind-the-screen-full-documentary/ [accessed 20 November 2018].

Ball, Kirstie. 2019. Review of Zuboff's *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. *Surveillance & Society* 17(1/2): 252-256.
http://library.queensu.ca/ojs/index.php/surveillance-and-society/index | ISSN: 1477-7487

to be critical when viewing search results as "absolving Google of any responsibility in terms of the way its search engine works." According to *The Age of Surveillance Capitalism*, at the time the film was made the organization was ramping up its exploitation of the behavioural surplus and leaving its competitors in the dust. The corporate motto "Don't be evil," so emphasised in the film, is simultaneously a smoke screen and an acknowledgement of the temptations inherent in what was then a newly emerging business model.

Reading *The Age of Surveillance Capitalism* is also oddly reassuring. For me, it contained very few surprises. The phenomena detailed within its pages have been a concern of surveillance scholars for the last twenty years. I would even go so far as to say it is not a work of surveillance scholarship at all. For reasons known only to the author, it sidesteps many of the contributions of surveillance studies and duplicates their core arguments. I have written both theoretical and empirical pieces that delve into many of the observations of surveillance studies, concerning, for example, enrolment in surveillance assemblages (Ball 2002), the surveilled body (Ball 2005), the political economy of interiority (Ball 2009; Di Domenico and Ball 2011), brandscapes and the smart city (Murakami Wood and Ball 2013), public-private boundaries and national security (Ball et al. 2015), normativity, the surveillant other (Ball, Di Domenico, and Nunan, 2016), and so on. Cohen's (2012) concept of "semantic discontinuity"—spaces in information infrastructures where unpredictable activity occurs—appears to be very similar to Zuboff's "right to the future tense." Other surveillance scholars will no doubt find the same. If you were looking for a comprehensive treatment of surveillance scholarship, you won't find it in this book.

But this book was not written for us. It is intended as a wake-up call for the educated business reader to recognize the massive power of the tech platforms. The book deploys the term surveillance in its popular form as a sensitising device. It has been written by someone who has spent their working life at an elite business school, and it reflects both the US business context and the form of critique that arises in the vernacular of the US business school. In terms of genre, if I were to compare it to anything, then it would be George Ritzer's *McDonaldisation of Society* if only for the simple (but not only) reason that it displays a similar and welcome level of rancour. This essay reflects on the book in two ways. First, it offers my view on its major claims; then, it dwells on one of its aspects that I feel merits consideration: its continued use of a security lexicon. I claim that this lexicon betrays the insecurities that lie at the heart of the surveillance capitalist story.

The Age of Surveillance Capitalism is a work that constructs—at times in a poetic and elegant way—the history of two major corporations from documentary research and interviews of key informants. It forms a grand narrative of a new capitalist epoch, with terms to match, such as Instrumentarianism, Utopianism, and Big Other (the latter two being derived from B.F. Skinner's novel, *Walden Two*). It features a light, at times implicit smattering of the classical social-theory cannon. The ghosts of Marx, Durkheim, and Weber haunt the text as false consciousness, anomie, and the iron cage of rationality are implied throughout part one. Throughout the text, inferences could also be made about other ghostly theoretical figures, such as Haraway's God-Trick (1997), Foucault's docile subject (1977), and Levinas' Face (1969), but they are left un-interpellated. These glancing ricochets steer the narrative toward the main pillar of critique, based on Skinnerian behaviourism, and it is in part two that the main contribution is made. In the long-forgotten novel *Walden Two*, Skinner describes the utopia of living alongside a large-scale behavioural technology that drives decision making and overcomes what he saw as human limitations: free will and autonomy. The most convincing element of this book is its claim that Google has operationalised the large-scale behavioural technology Skinner envisaged. The exploitation of what Zuboff terms "the behavioural surplus" by the surveillance capitalists is an attempt at behaviourism on a massive scale. It is a story of dominance premised on the quest for behavioural certainty: even this, however, has already been discussed in this journal by von Otterlo (2014).

Pressing on, one is left in no doubt that this is the philosophy that drives the tech platform empires. Zuboff argues that the practices of surveillance capitalism move toward Skinner's mass behavioural technology by rendering consumers both predictive and addictive. The practices of surveillance capitalists seem to undermine the critiques of behaviourism that arose in Skinner's time. Then, critics argued that behaviourism

could not account for language development and memory. Behaviourism was also criticized as adopting an impoverished view of the human being as a mere product of its environment. The presence of an inner world was understood to be beyond the behaviourist explanation. Zuboff argues that the power and scale of analytics now render this interior world legible and open to manipulation and exploitation: a phenomenon I described as "The Political Economy of Interiority" in 2009. The corporate strategies involved are supported by intentionally unassailable governance structures and cultish corporate speech acts that exoticise Google employees as a chosen few. Using super-voter privileges, a level of dominance around corporate governance is revealed that closes down any questions about responsible and fair information practices, even from the shareholders themselves.

The critique, however, does not go far enough. At the end of part two, Zuboff draws on Karl Polanyi to argue that "if industrial civilization flourished at the expense of nature and now threatens to cost us the Earth, an information civilization shaped by surveillance capitalism will thrive at the expense of human nature and threatens to cost us our humanity" (2019: 347). After such a strong statement, I was looking forward to the book's final pages as being a treatise on the enduring relevance of autonomy, possibilities for new commons, privacy beyond the individual, perhaps a cross-cultural comparison that relativized surveillance capitalism and prised open new ways of thinking. How is this to be addressed at scale? Unfortunately no such analysis materialised. Predictably, artistic critique was considered as resistance and further coverage was given to the impact of social media on the mental health of young people. Both of these are important, but a much stronger conclusion was required and I felt the book lost its way in part 3.

Nevertheless, *The Age of Surveillance Capitalism* provides glimpses into new avenues for critique. One particular feature that caught my eye was the use of a securitisation lexicon throughout. Two words that occur within this lexicon, exceptionalism and rendition, are frequently used. The term "state of exception" is used in security studies to describe the suspension of normal democratic rules and the use of coercive power in security-intense and war-like settings (Agamben 2005). In the book, exceptionalism arises in the emergence of Google's data-exploitation strategy. Borne of an existential threat to the corporation itself—i.e., of profound *in*security—the new strategy demanded a suspension of the normal modus operandi, an abandonment of information ethics, and an exploitation of so-called "lawlessness" in cyber space (although see Cohen [forthcoming] for a legal critique of this argument). Extraordinary rendition is a term used to describe the removal of a person to be interrogated in a country whose regulations for the treatment of prisoners is less rigorous. In *The Age of Surveillance Capitalism*, Zuboff uses the term "rendition" to describe an equivalent extraction of information from user data. She asserts that we should "Forget the cliché that 'if it's free, you are the product.' You are not the product; you are the abandoned carcass. The 'product' derives from the surplus that is ripped from your life" (2019: 377).

This aspect of the text caused me to reflect on how securitisation pervades the world of the surveillance capitalists, from everyday micro discourses to the most macro levels of the worlds of national and international policy. This lexicon is a reminder of what is at stake for the surveillance capitalists who invest heavily in hardware to monitor and extract data and make appeals to our own insecurities to ensure that we continue to engage. For example, the extraordinary levels of control over corporate governance exerted by the boards of both Google and Facebook, for me, betray a deep fragility that is suppressed by the use of brute power and a cultish corporate culture. In the fake news enquiry, the rhetoric deployed also betrays the exceptional politics that lies at the heart of the tech giants. On April 11, 2018, Mark Zuckerberg told US Senators that Facebook was in "an arms race" with Russian operators who were seeking to exploit the social network platform to international political ends.[2] One week later, Brittany Kaiser, former Director of Programme Development at Cambridge Analytica said on BBC Radio 4's programme "Today" that the firm had been engaged in "constructing enemies for the public to vote against" during the Trump election campaign.

[2] https://www.bbc.com/news/world-us-canada-43719784 [Accessed 12 April 2018].

For several years Iain Munro and I have been working on a set of ideas that explores the extreme politics of information networks as a war by other means. The work, which is still in development, argues that corporate communications networks reflect many military characteristics. We have researched multiple documentary sources and argue that the militarisation impetus comes from government and is readily transferred to the corporate world. But we see in *The Age of Surveillance Capitalism* how exceptionalism, rendition, and other war-like notions begin in the corporate arena just as readily.

The idea of politics as a war by other means is discussed by Foucault (1977, 2003) and is an inversion of military strategist von Clausewitz's (1832) observation that war is politics by other means. Foucault's concern was to address how military techniques had migrated from the military to the civilian realm, recoded as the police state to control revolutionary action and civil war. Von Clausewitz's work has also influenced recent scholarship on information warfare. Klimburg (2017), for example, argues that an inversion of von Clausewitz has been used in Russian military intelligence in order to categorise all information as a potential weapon. Some have downplayed the military presence in communications networks (e.g., Rid 2013), whereas others have noted that this has played a significant role both in the funding of hi-tech research and in the policing of networks (Powers and Jablonski 2015). Communications networks have been framed as being a "special kind of battlefield" (Terranova 2004), a site of "cyberwars" (Arquilla and Ronfeldt 1997), and as exemplifying a militarized "state of exception" (Jordan 2015; Lyon 2015). Even Castells (2005: 6), who emphasises the emancipatory potential of communications networks, concedes that "technological development is controlled by the military."

A key element of Foucault's take on von Clausewitz is the idea that militarization propagates between the state and society in a transversal rather than top-down manner. Iain and I argue that there are a number of mechanisms through which this transfer takes place in the surveillance and security context—the "other means" to which Foucault refers. Innovations in surveillance technologies are co-produced through the subcontracting of corporate services to the military. Corporations are also legally co-opted to provide data for national security purposes and, as Zuboff argues, there is a revolving door of expertise between the tech giants and the military. Whilst this network of alliances is at times unstable, there is no doubt that it is pervasive in a number of industrial sectors including that of the surveillance capitalists (Ball et al. 2015). Companies such as Amazon, Facebook, Google, and Microsoft all work closely with military and national security organizations. The extent of these collaborations and their influence urgently needs to be understood.

Considering the exceptional politics that seems to pervade so much of what the surveillance capitalists do, this war by other means is fought on many more different fronts than we have considered so far. Apart from active involvement in national security governance and the processes detailed in the previous paragraph, it is also reflected in the metaphors used in everyday interactions, the strategies of denial and defence in official communications and corporate governance, the cultural brainwashing of employees, and the addictive designs people are anxious to live without. Even if this book is more likely to be found in an airport bookshop than in a learned library, it has still provoked reflection on the insecurities that drive the path dependencies of mass surveillance in the corporate world. *The Age of Surveillance Capitalism* highlights that security and insecurity are at the heart of corporate power, especially in a dominant form of commerce that has mass surveillance as its core process.

References

Agamben, Giorgio. 2005. *The State of Exception*. London: Chicago University Press.

Arquilla, John, and David Ronfeldt, eds. 1997. In Athena's Camp: Preparing for Conflict in the Information Age. Washington, DC: RAND National Defense Research Institute.

Ball, Kirstie. 2009. Exposure: Exploring the Subject of Surveillance Information. *Communication and Society* 12 (5): 639-657.

Ball, Kirstie. 2005. Organization, Surveillance and the Body. *Organization* 12 (1): 89-08.

Ball, Kirstie. 2002. Elements of Surveillance: A New Framework and Future Directions. *Information, Communication and Society* 5 (4): 573-590.

Ball, Kirstie, MariaLaura DiDomenico, and Daniel Nunan. 2016. Big Data Surveillance and the Body-Subject. *Body & Society* 22 (2): 58-81.

Ball, Kirstie, Ana Canhoto, Elizabeth Daniel, Sally Dibb, Maureen Meadows, and Keith Spiller. 2015. *The Private Security State?: Surveillance, Consumer Data and the War on Terror*. Copenhagen: Copenhagen Business School Press.
Castells, Manuel. 2005. The Network Society: From Knowledge to Policy. In *The Network Society From Knowledge to Policy*, edited by Manuel Castells, and Gustavo Cardoso, pp. 3-23. Washington, DC: John Hopkins Center for Transatlantic Relations.
Cohen, Julie. Forthcoming. Surveillance Capitalism as Legal Entrepreneurship. *Surveillance & Society*.
Cohen, Julie. 2012. *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. London: Yale University Press.
Di Domenico, MariaLaura, and Kirstie Ball. 2011. A Hotel Inspector Calls: Exploring Surveillance at the Home-Work Interface. *Organization* 18 (5): 615-636.
Foucault, Michel. 1977. *Discipline and Punish: The Birth of the Prison*. London: Penguin Books.
Foucault, Michel. 2003. *Society Must Be Defended: Lectures at the College De France 1975–76*. London: Penguin Books.
Haraway, Donna J. 1997. *Modest Witness@Second Millenium.FemaleMan© Meets On coMouse™: Feminism and Technoscience.* New York and London: Routledge.
Jordan, Tim. 2015. *Information Politics: Liberation and Exploitation in the Digital Society.* London: Pluto Press.
Klimburg, Alexander. 2017. *The Darkening Web: The War for Cyberspace.* New York: Penguin Press.
Levinas, Emmanuel. 1969. *Totality and Infinity: An Essay on Exteriority.* Pittsburgh, Pennsylvania: Duquesne University Press.
Lyon, David. 2015. *Surveillance After Snowden.* Cambridge: Polity Press.
Murakami Wood, David, and Kirstie Ball. 2013. Brandscapes of Control: Subjects and Space in Late Capitalism. *Marketing Theory* 13 (2): 47-67.
Powers, Shawn M., and Michael Jablonski. 2015. *The Real Cyber War: The Political Economy of Internet Freedom.* Urbana, IL: University of Illinois Press.
Rid, Thomas. 2013. *Cyber War Will Not Take Place.* London: Hurst and Company.
Terranova, Tiziana. 2004. *Network Culture: Politics for the Information Age.* London: Pluto Press.
von Clausewitz, Carl. 1982. *On War.* London: Penguin Books.
von Otterlo, Martijn. 2014. *Automated Experimentation in Walden 3.0: The Next Step in Profiling, Predicting, Control and Surveillance.* Surveillance & Society 12 (2): 255-272.