Book Review

Review of Birchall, Clare. 2017. *Shareveillance: The Dangers of Openly Sharing and Covertly Collecting Data*. Minneapolis, MN: University of Minnesota Press.

88 pp. Paperback. US \$7.95. ISBN: 9781517904258.

Kevin Walby

University of Winnipeg, Canada
k.walby@uwinnipeg.ca

Shareveillance builds on several important conceptual reflections and empirical inquiries into secrecy and transparency by cultural theorist Clare Birchall. In this book, Birchall sets out to theorize politics and subjectivity in an era when we voluntarily share more information about ourselves than ever before. Birchall begins with a bold claim: shareveillance, “a state in which we are always already sharing—indeed, in which any relationship with data is only made possible through a conditional idea of sharing—produces an antipoliticized public made up of shareveillant subjects caught between the affects and demands of different data projects” (2). The author explicitly uses the notion of antipoliticized rather than depolitized and goes on to elaborate why this is a more accurate rendering of political subjectivity today. Social media and web-based platforms encourage participation, but Birchall suggests shareveillance operates to foreclose forms of politics before they even emerge. *Shareveillance* is thus a radical critique of sharing in the digital world.

The notion of sharing is celebrated in our current entrepreneurial economy that offloads risk and responsibility onto data-constituted citizens. The internet is (or at least it was) celebrated as an open, utopian form of networking and learning. Forms of surveillance and control that are enabled by digital sharing cannot be avoided anymore, which means these information flows constitute the subject in ways not previously conceived or thought possible. What Birchall does is provide new terminology for understanding our relationship with data and the logic of data sharing in the 21st century.

The idea and practice of sharing that fascinates Birchall is “protocological” (16) in the sense that the rules and modes of sharing and participation are built-in to the process and the technology. The controls are immanent and there is little that can be done from the outside to “protect” users and those subject to data collections and flows. These flows are characterized by “openness and enclosure” (18). The subject is both monitoring and being monitored at all times. Openness and enclosure are relational (21), but Birchall highlights how covertly collected state data are different in kind. Closed government data are information that multiple publics have not had access to or knowledge of, such as national security decisions. There are also contradictions, such as the opacity of open data. The main claim here is that the logic of “sharing is not something we do after possessing data but is the basis on which having any relation with that data

Walby, Kevin. 2018. Review of Birchall's *Shareveillance: The Dangers of Openly Sharing and Covertly Collecting Data*. *Surveillance & Society* 16(2): 261-262.

<https://ojs.library.queensu.ca/index.php/surveillance-and-society/index> | ISSN: 1477-7487

© The author(s), 2018 | Licensed to the Surveillance Studies Network under a [Creative Commons Attribution Non-Commercial No Derivatives license](#).

can be possible at all” (23). This condition of permanent and constant data sharing works in the interest of state and commercial entities.

Given the proclivity toward data sharing, and state and corporate consumption of these data, Birchall argues “privacy is like the light we see from an already dead star. We cling to it even though we live in what our digital conjuncture has essentially rendered a postprivacy paradigm” (25). Appeals to privacy reduce collective politics and reduce political agency due to the individualized scope of privacy rights. The notion of privacy also fails to conceive of the mass form that surveillance takes today (think metadata) and fails to advance a radical politics since it remains ensconced in the rhetoric of individual rights. Birchall also advances a critique of open data and recent state transparency initiatives that rely on a disingenuous notion of openness. Although new “datapreneurs” have emerged to “harness the potential of [open] data to create value from raw data sets” (32), there is a corporate logic to open data projects which again represents a distraction from actual openness and collective politics. This transparency of the state (and of corporations) is a fiction. Citizens today must be “vigilant and veillant” (33) to derive benefit from citizenship and political rights, otherwise these can be washed away in swarms and flows of data. Citizens have accepted these conditions in a wholesale manner, this shareveillant assemblage.

Given the limits of privacy discourse and rights, Birchall looks to formulate a conceptualization of politics and resistance. She suggests, “I am not imagining a once fully agential political subject who has now been supplanted by this shareveillant version” (38). Birchall advances the notion of tactical cuts into or away from data. Cuts into data could include hacking, archiving, or even forms of data obfuscation that challenge state interpretations. I wondered if use of freedom of information and access to information requests could be considered ethical cuts into the state; however, Birchall did not mention these mechanisms. As Birchall puts it, “creative interruptions of shareveillance can make ethical cuts and, in the process, show up the incisions that have constructed the neoliberal securitized settlement of which shareveillant subjectivity is a part” (46). Birchall suggests “guerrilla archiving” (63) may assist against the anticipated ‘post-truth’ closing off and erasing of some (notably scientific) data. And “tactical opacity” (64) may be required to resist new forms of data collection being established. Tactical opacity is about rendering ineligible or illegible the categories and classifications of shareveillance practice. This is not a call to simply reject all data or accept open data as a trade-off for covert state information collection. Instead, Birchall argues we must work with opacity and cut into these data flows however we can: “these experiments and imaginative cuts become ethical, political acts” (58).

In an Afterword entitled “Trumping Shareveillance,” Birchall comments on the ideas of openness and enclosure in relation to the contemporary American state. This work was published before the Facebook and Cambridge Analytica scandal, which only further substantiates Birchall’s main claims in *Shareveillance*.

Shareveillance is an impressively rich conceptual work that provides many terms and questions for thinking about and investigating the social and digital world we have created. There are excursions on Deleuze and Derrida as well that I have not mentioned here. I certainly would have liked to have seen more reflection on the relationship between creative interruptions of shareveillance on the one hand and social movements and collective action on the other, but no book can do it all. *Shareveillance* is an interrogation of the ethics of information sharing, which should be taken seriously by all scholars of surveillance, security intelligence, Web 2.0, and digital culture.