Book Review

Review of Arne Hintz, Lina Dencik, and Karin Wahl-Jorgensen. 2019. *Digital Citizenship in a Datafied Society*. Cambridge: Polity Press.

194pp. Paperback. \$27.95. ISBN 9781509527158.

Thomas N. Cooke

Queen's University, Canada
tommy.cooke@queensu.ca

In our research community, the citizen's digital agency is met with healthy skepticism. At the nexus of surveillance capitalism (Zuboff 2019), surveillance culture (Lyon 2017), and surveillance realism (Dencik and Cable 2017)—an intersecting place propagated by an increasingly closed Internet coding infrastructure (Lessig 2006)—resistance seems futile. So much so, that the notion of even masking one's location and identity is perhaps more performative than pragmatic (Monahan 2015). In a world of rhizomes in which governments piggyback corporations to monitor populations, what exactly does agency look like, and is it possible to reason this way inside the conventional intellectual confines of digital citizenship scholarship?

The day I began this review is the day Mozilla announced Track THIS! It is one of a dozen initiatives undertaken by the company to position users to have more control over the who, what, and how of their data. This latest initiative combines education about which companies are mining data from cookies inside their devices, along with a strategy for stopping it. As social scientists, we have suspected cookie technologies to be highly problematic for user privacy (Shah and Kesan 2009; McStay 2012; Lyon 2015; Cooke 2016) – suspicious for a long time, indeed (Bennett 2001; Haggerty and Gazso 2002; Elmer 2003). And we have remained healthily skeptical about the extents of resisting them. But here is Track THIS!, a technology that opens one hundred browsing tabs at once. In doing so, it gives cookies poor ingredients: noisy metadata. It makes the user appear to be someone they are not. Is the premise of resistance technology naïve, or is it meaningful in the context of agency? Do these questions even matter if the privacy ship set sail long ago?

Hintz, Dencik, and Wahl-Jorgensen's book is a powerful contribution to digital citizenship studies precisely because it commits the conventional digital citizenship reader to entangle with these questions. Somewhere between a shroud of hope and some healthy skepticism is where we might find the authors' answer to these questions: if agency online is possible, in a realm where the odds are literally coded against them, a horizon for resistance exists—where concept transfers into practice, even if it is only meaningful because it is more admirable than it is effective. A strength of the book is the representation of what lays beyond the horizon: a constellation of surveillance cultures, policies, and practices that have tended to escape the purview of digital citizenship literature for a long time. The book is a guide to all meaningful technical, ideological, and practical developments in and around surveillance since the late 1990s. The book's small but important shortcoming is reflected not merely by an oversight of its own but perhaps within the surveillance studies and critical data studies communities within which the authors'

Cooke, Thomas N. 2019. Review of Arne Hintz, Lina Dencik, and Karin Wahl-Jorgensen's *Digital Citizenship in a Datafied Society*. *Surveillance & Society* 17(3/4): 588-591.

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

© The author(s), 2019 | Licensed to the Surveillance Studies Network under a [Creative Commons Attribution Non-Commercial No Derivatives license](#).

critique emerges: resistance techniques and technologies, like Track THIS!, as well as the unique notions of agency and resistance they exhibit, are empirically (and thereby theoretically and philosophically) under-represented. Nevertheless, the book is successful in its endeavour to sober celebratory attitudes about digital democracy by bringing the magnitude of global surveillance into the forefront.

Deploying the notion of datafication as a catch-all to embody the critiques, concerns, and reservations critical data studies and surveillance studies hold for agency online, the authors emphasize the inequalities, differences, and divisions that the processes of data create for users. The book is the culmination of a comprehensive, two-year empirical study funded via the UK ESRC project, “Digital Citizenship and Surveillance Society”—the largest scholarly undertaking of its kind of digital citizenship in a datafied society. The book’s seven chapters progress through three stages, with two chapters focusing on concepts and theoretical framework, problem-analysis, and with second-last chapter offering an agency-assessment prior to a conclusion that prompts us as analysts to keep in mind that “it is only by identifying [the] broader conditions in which citizenship is played out that we can understand its meaning and nature” (154). The book’s introduction establishes what the orientation of surveillance studies and critical data studies offers towards the study of datafication and digital citizenship and establishes the post-Snowden era as the predominant sociopolitical context within which the book’s analyses and discussions are situated.

Chapter Two exposes how the concept of citizenship is received and intellectualized in the academy and in the public sphere. These orientations are problematized by revisiting some of the key movements and case studies they take up, by uncomfortably situating them within the context of the power-effects that inescapably bind, complicate, and undermine them. Digital agency oft heralded through the emergence of online protests, from the Arab Spring to the hacktivist and resistance efforts embodied by the undertakings of Anonymous Group and WikiLeaks, not to mention the advocacy efforts charged by the Electronic Frontier Foundation and the American Civil Liberties Union, are counterbalanced in particular by the authors’ exploration of the architectural and sociopolitical constraints imposed by big data, surveillance capitalism, machine learning algorithms, technological determinism (dataism), along with some brief but astute consideration of the ontological and empirical perils caused by the exceedingly difficult existence (let alone study) of surveillance metadata.

Chapters Three and Four deal with the regulation and mediation of digital citizenship, respectively. The scope and means of data policy *prior* to the Snowden Revelations irrefutably establishes the double-binding nature of data policy *after* the Snowden Revelations. While the explosion of revised and extended government data policies established a key policy window for inviting critical and self-reflexive questioning about the surveillance practices, new problems flew in through that window along the way. What stands out are the pitfalls associated with the legislating of the user consent model of data protection—a move that was particularly problematic upon the galvanization of the public technoscientific imaginary. Policy changes in the post-Snowden Era also gave rise to a plethora of oversight committees and entirely new bodies of regulation, such as the GDPR. While such efforts are indeed heralded by conventional intellectual attitudes, they are quickly (re)grounded in the realities of extended state surveillance capacities. Their argument is deftly exemplified through the authors’ analysis UK IPAct. Despite being designed to regulate data collection, the act did the opposite. As state powers were identified as problematic, a new discursive foundation unfolded to, rather conversely, reify why such powers are necessary in the realm of digital anarchy. The IPAct did not enhance rights and liberties. It restricted them by clarifying precisely why and how the GCHQ must be aggressive in the name of national security. In a similar vein of exposing caveats of seemingly progressive institutional reform, the authors similar discuss how the media have played a role in normalizing, and not challenging, global surveillance. This is best exemplified by the sensationalist tendency to disproportionately empower the voices of technology journalists, such as Geoff White, who downplayed the significance of metadata in relation to user privacy and thereby ignored the explosion of concerns coming from journalists such as Glenn Greenwald at the same time.

Chapter Five questions how citizens come to negotiate digital environments. How does an individual who is implicated in a discrete and globally reaching data infrastructure discover and determine the parameters required for tangible, legible, and visible action? The potentiality for agency, and any such determination for agency, is situated within the tension-space between the Snowden Leaks themselves and surveillance culture. If action depends upon understanding, and understanding is premised upon visibility and legibility, then the Snowden Leaks are only as instructive as they are delimiting: “numerous surveys and opinion polls have highlighted general confusion and uncertainty about how data is generated and collected in digital environments. While many people... are generally aware of data collection and use... the level of understanding of how this works and what it means in practice is much lower” (106).

Chapter Six is the most thought-provoking section of the book. It deals with capacities for challenging datafication, and thereby big data-oriented surveillance, as an expression of digital citizenship. Recalling Monahan’s (2015) famous declaration from above, the lines between tractable and symbolic resistance blur together when considering the enormity of mass surveillance; wearing a mask in front of a facial-recognition algorithm, and protesting on forums online, gesture resistance but perhaps do not halt, impede, or redirect it, *per se*. The authors are a bit more hopeful than Monahan. Publishing a few years later levies the advantage of time to empirically engage novel and emergent digital resistance repertoires. From RiseUp.net and The Onion Router to Signal—not to mention the data ethics and privacy shortcomings even the most progressive Open Data campaigns unfolding alongside Smart City projects worldwide—inclusion of such developments balances the ontological playing field. These technologies have made important, lasting impressions upon how certain appendages of mass surveillance can be avoided, negotiated, and even deflected. However, a shortcoming of the book resides in its rather limited empirical inclusion of agency-enabling concepts, movements, and technologies on the fringe of even the most resistance-oriented surveillance studies and critical data studies empirical horizons.

The belief that the horizon of potentiality for meaningful and tractable agency online is limited, temporary, and overwhelmingly outpowered, is as much a problem with datafication as it a problem with our intellectual and empirical orientations; to challenge power is not to reveal an alternative truth (e.g., surveillance can be destroyed), but to detach power from truth in a way that creates a stumbling point for resistance and a starting point for an opposing strategy (Foucault 1998). There is an entire realm of resistance technologies that have escaped the purview of the book, and our research communities in general, that can alter how we think about agency online. I have argued elsewhere that we can (re)invigorate our representations and understandings of meaningful and tractable resistance to surveillance by attending to noisemaking technologies (Cooke 2018)—those that cease, redirect and confuse surveillance by feeding it meaningless, inaccurate, and intentionally disruptive data.

Mozilla’s Track THIS! is not an isolated example. ProtectMyPrivacy, designed by Carnegie Mellon’s Human-Computer Interaction Institute, is a smartphone-based metadata detection and interception tool that not only educates Android and iPhone users about what kinds of data are being transferred between an operating system and an app. It also crowdsources responses from tens of thousands of users worldwide who find themselves in similar situations, just prior to prompting them as to whether or not they are interested in “fudging” the data by injecting noise into it. This development is led by academics, and practiced by researchers, common users, and hacktivists alike. It is one of a growing range of resistance repertoire that works by hacking into corporate technologies like iPhones and Androids: iCleaner, Locus, PrivaCy, LocationFaker, not to mention the data mining discovery tool PiOS that educates the user about which apps and processes are the most adversarial to their privacy. The Decentralized and Distributed Systems (DEDIS) research group at EPFL is currently undertaking numerous projects similarly working within the concept and practice of noisemaking, developing tools that (finally) encrypt metadata (PURBs), that sample randomness in public servers and presents it to third-parties (RandHound), as well as the late Dissent project—previously undertaken at Yale University and UT Austin—that pioneered a radically new method for anonymizing user identity by flooding Internet pathways with noisy data designed to mislead surveillance.

These examples represent not only an emergent way of doing resistance, but also a way of thinking about resistance through noise—or what Nissenbaum and Brunton (2016) implied in “obfuscation.” Their work is as much a conceptual engagement as it is a pragmatic engagement with an entirely different space for action and expression. This space is not individualized; it depends upon community to be successful. The more it is practice, the more likely we are as analysts to precondition the empirical foundation required for quantitatively and qualitatively evaluating challenges to surveillance. This is not a critique of Hintz, Dencik, and Wahl-Jorgensen. Their contribution is an important challenge to conventional thought that compels reflexive and critical inquiry into the paradoxes of expression and change online. Future contributions that similarly intersect surveillance studies and critical data studies will continue to challenge extant thought by expanding the empirical repertoire not only to account for the perils instantiated by the institutional domination of the Internet, but by also being mindful not to reify it at the cost of excluding elusive yet emergent resistance efforts.

References

- Bennett, Colin J. 2001. Cookies, web bugs, web cams and cue cats: Patterns of surveillance on the world wide web. *Ethics and Information Technology* 3(3): 195-208.
- Cooke, Thomas N. 2016. Cookies. In *Making Things International 2: Catalysts and Reactions*, edited by Mark B. Salter, 228-240. Minneapolis: University of Minnesota Press.
- Cooke, Thomas N. 2018. Noise, Data, Silence, Privacy. In *Political Silence: Meanings, Functions, and Ambiguity*, edited by Sophia Dingli and Thomas N. Cooke, 20-40. Milton Park, UK: Routledge Press.
- Dencik Lina and Oliver Leistert, eds. 2015. *Critical Perspectives on Social Media and Protest: Between Control and Emancipation*. Lanham, MD: Rowman & Littlefield.
- Greg Elmer. 2003. *Profiling Machines: Mapping the Personal Information Economy*. Cambridge: The MIT Press.
- Haggerty, Kevin D. and Amber Gazso. 2005. Seeing beyond the Ruins: Surveillance as a Response to Terrorist Threat. *The Canadian Journal of Sociology* 30(2): 169-187.
- Lessig, Lawrence. 2006. *CODE 2.0*. New York: Basic Books.
- Lyon, David. 2017. Surveillance culture, ethics and digital citizenship. *International Journal of Communication* 11: 1-13.
- McStay, Andrew. 2012. I consent: An analysis of the Cookie Directive and its implications for UK behavioral advertising. *New Media & Society* 15(4): 596-611.
- Monahan, Torin. 2015. The Right to Hide? Anti-Surveillance Camouflage and the Aestheticization of Resistance. *Communication and Critical/Cultural Studies* 12(2): 159-178.
- Shah, Rivaj C. and Jay P. Kesan. 2009. Recipes for cookies: how institutions shape communications technologies. *New Media & Society* 11(3): 315-336.
- Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.