Book Review

Review of Sarat, Austin (ed). 2015. *A World Without Privacy: What Law Can and Should Do?* New York: Cambridge University Press.

287pp. Hardback. US\$102.00. ISBN 978-1-107-08121-5.

Michael Carter

Queen's University, Department of Geography and Planning, Canada.
michael.carter@queensu.ca

In 2013, Edward Snowden sparked a global privacy panic by releasing evidence of indiscriminate mass surveillance conducted by several intelligence agencies, most notably members of the network known as the Five Eyes. The surveillance involved mass state access to personal data stored by privately owned information intermediaries that acquired it in the course of providing services such as search engines, email, blogging platforms, social network sites and video calling. The rapid adoption of these services reflects a broad cultural shift towards digitally mediated social life. Appreciating the inherent benefits and risks of this shift requires an analysis of power relations. Legal and surveillance scholarship are both especially useful for this task, particularly when it comes to the topic of privacy. *A World Without Privacy* offers readers a range of rich and insightful perspectives on the benefits and risks associated with the ever-deeper integration of information communication technologies with daily social life.

The origins of American privacy law can be traced back more than a hundred years to the pioneering work of Samuel Warren and Louis Brandeis. Warren and Brandeis developed the 'right to privacy' in response to a privacy panic ignited by the emergence of portable cameras and free press. In the introductory chapter, Austin Sarat claims contemporary privacy law remains moored to this traditional framing of privacy as protection against the intrusion of a protected sphere. Sarat sees little opportunity for this framing to offer protection to the increasing number of individuals routinely "exposing their private lives to millions" (pg. 16). A culture of self-publication, new forms of surveillance, and the war on terror have created a climate in which he believes the "threats to privacy are ubiquitous" (pg. 5). In this climate, Sarat questions the capacity of the privacy establishment to protect individual privacy. This capacity is debated in the chapters that follow.

Many individuals believe that privacy is dead. In his chapter, Neil Richards disagrees. He believes "privacy is one of the most important issues facing modern information societies" (pg. 81). He argues that framing privacy as the amount of information known about individuals has led to the belief that privacy is dead. He points to the dramatic expansion of the privacy establishment as proof that privacy has "...never been more alive" (pg. 43). Highlighting research conducted by danah boyd and Alice Marwick, which shows the great lengths youth go to protect their personal data, Richards debunks the myth that "(young) people don't care about privacy" (pg. 34). Richards easily discards a third myth, that privacy is for people with dark secrets, by suggesting few individuals "would be comfortable with having images of their activities in the bedroom or bathroom made public" (pg. 61). Finally, Richards claims privacy is in fact

Carter, Michael. 2017. Review of Sarat's *A World Without Privacy: What Law Can and Should Do?* *Surveillance & Society* 15(1): 176-178.

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

© The author(s), 2017 | Licensed to the Surveillance Studies Network under a [Creative Commons Attribution Non-Commercial No Derivatives license](#).

good for business, pointing to the currency of trust as competitive advantage. He points to earlier professions including doctors, lawyers and accountants as relevant examples. For Richards, it seems, the future of privacy is bright.

The benefits of privacy are often interpreted in a limited way by focusing attention on protection from being seen or heard. Rebecca Tushnet skilfully demonstrates how pseudonymity creates opportunities for women to speak while “remaining unseen” (pg. 88) by protecting them from harassment and cultural norms that amplify male voices while silencing those of females. According to Tushnet, large corporations, including Google, “have little sympathy for pseudonymic participation” (pg. 101). From their positions of power, teams comprised of “mainly men” (pg. 108) do not see the need for pseudonymity and choose instead to implement real name policies to discourage people from being offensive to other users. As she develops her argument, it becomes clear (though not stated explicitly) that pseudonymity has “beneficial and protective uses” (pg. 108) for all individuals. Tushnet argues a sustainable personality decoupled from legal identity affords individuals the time and space to experiment with different aspects of self. A professional, regardless of their gender, race or religious beliefs can benefit from the safety afforded by separating personality from legal identity.

Lisa Austin offers a sophisticated analysis of legal theory in her chapter. Austin’s “power-over” (pg. 162) focuses on the rule-of-law underpinnings of trespass, which serve as a constraint on the arbitrary use of power to cross the boundaries of private property. In her “power-to” analysis, Austin notes “trespass is not an injury based tort” (pg. 175), rather its function is to facilitate legal powers related to exclusive use of private property. By emphasizing power relations, Austin shifts attention away from protecting isolated spheres of privacy and towards securing the conditions of social interaction in contemporary surveillance society.

Austin uses examples from Canada to demonstrate structural defects in consent based privacy models. First, she notes fair information practices frame the flow of personal data as a closed circuit while in reality information intermediaries traffic user data across political and institutional borders with different privacy contexts. Second, Austin problematizes the implementation of consent based privacy regimes arguing they “undermine privacy and facilitate surveillance” (pg. 134). She notes that when competing interests between users and corporations emerge, the Office of the Privacy Commissioner of Canada has ruled in favour of the latter. Austin problematizes Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA), which facilitates warrantless access through a clause that allows voluntary disclosure of user data. Considering the failure of consent based models, Austin calls for greater oversight of informational practices on both sides of the corporate-state nexus. To achieve this, she suggests applying the principle of procedural fairness in administrative law to the development of rights of participation and rules about transparency.

Discussions of privacy are often dominated by “legal centrism” (pg. 196), according to Kevin Haggerty. He argues privacy law, with its focus on “immediate, identifiable and concrete harms” (pg. 199) is inadequate for the task of curtailing surveillance particularly with the emergence of informational capitalism. In his chapter, Haggerty notes the dissolution of Alberta’s Personal Information Protection Act (PIPA) in its entirety due to the constraints it placed on private firms collecting personal data from users, as one example. He distinguishes his perspective of “the reality of privacy” (pg. 193) from legal interpretations that conceptualize it mainly through the lens of actionable violations. In his view, expanding surveillance mechanisms are often articulated within the rule of law despite the skill and passion of privacy advocates. Haggerty notes court based privacy in the United States and the privacy institutions of Canada produce similar shortcomings: courts and commissions frequently side with the political and economic objectives of large organizations. He points to expanded CCTV networks, ineffectual ‘do not call’ registries (pg. 212), and the formation of ‘fusion centres’ (pg. 213) as examples. Haggerty surmises readers will point to a lack of agency in his work and states that while he firmly

believes in the potential for agency his primary concern is with a societal naïveté about the potential for totalitarian regimes to appropriate contemporary surveillance systems.

Despite finding little common ground with the contributors, Ronald Krotoszynski believes there is hope for legal systems to strengthen privacy. While he appreciates Tushnet's presentation of protected speech as empowering for marginalized groups, Krotoszynski suggests the potential for "corrosive and distortionary" (pg. 265) speech is substantial. He suggests Austin's rule-of-law approach could in fact facilitate efforts by government to collect personal information. Krotoszynski recognizes Haggerty correctly problematizes the idea of government as privacy advocate while challenging his claims that privacy is doomed by declining expectations of privacy held by citizens and the emergence of informational capitalism. He points to a ruling by the Supreme Court of Canada as evidence that citizen privacy remains shielded by constitutional rights. Krotoszynski offers a fifth myth, adding to Richards' four, that local cultural norms have such a strong influence on privacy that a global discussion is fruitless. Krotoszynski clearly favours comparative analysis involving (mainly) European privacy legislation to inform more privacy legislation on a range of issues including free speech, free press and revenge porn. From his perspective, the state has seniority in the corporate state nexus and is well positioned to keep Big Brother Incorporated in line.

The authors make it clear that any legal framework seeking to protect the privacy of citizens must treat privacy as a complex, nuanced concept. A curious omission from *A World Without Privacy* is any engagement with (or even mention of) the topic of encryption despite regular reference to the efforts of Edward Snowden. It is a topic that certainly sits at the centre of tensions produced by unequal relations of power between citizens and the corporate state nexus. The timing of *A World Without Privacy* offers some explanation for the silence given the encryption debate ignited as this text was being published. What is interesting to note then is how quickly the privacy landscape continues to evolve, when a topic that is such an obvious omission to readers today was not even a footnote just months ago.

References

Warren, Samuel D. and Louis D. Brandeis. 1890. Right to Privacy. *Harvard Law Review* 4(5):193–220.