DAVID **TAN**
Associate Professor
Faculty of Law, National University of Singapore

Data Protection Law in Singapore: Privacy and Sovereignty in an Interconnected World BY SIMON **CHESTERMAN**, ed. [Singapore: Academy Publishing, 2014. xi + 313 pp. Paperback: S$64.20]

Privacy has been said to be a concept in an utter mess. In his influential treatise, *The Rights of Publicity and Privacy* (2nd ed., 2005), J. Thomas McCarthy laments: "It is apparent that the word 'privacy' has proven to be a powerful rhetorical battle cry in a plethora of unrelated contexts… Like the emotive word 'freedom', 'privacy' means so many different things to so many different people that it has lost any precise

legal connotation that it might once have had" (at para. 5.59). *Data Protection Law in Singapore*, edited by Professor Simon Chesterman, is a timely and much-welcomed collection of essays that not only address myriad perspectives on the issue of data protection, but also provide tantalising views on the challenges to privacy and sovereignty brought about by the digital revolution. Singapore enacted the *Personal Data Protection Act 2012* (Act 26 of 2012) [*PDPA*] on 15 October 2012 and it came into effect on 2 January 2013, with businesses given 18 months to comply before the *PDPA* became enforceable on July 2014. The book's examination of the way in which Singapore has responded to the problems brought about by data collection, aggregation, use and dissemination in the 21st century through the enactment of the *PDPA* will no doubt be of great interest to practitioners, policy makers and legal scholars.

The book is divided into 8 chapters. In Chapter 1, Simon Chesterman echoes the frustration of many scholars when he writes: "Many privacy laws are… confusing and confused" (at p. 2). He sets out how the conception of privacy in the United States (based on the protection of a liberty interest as a freedom from external interference) is different from the European understanding that is premised on human dignity, and then proceeds to elucidate how the legal regimes in these jurisdictions have developed over the years based on these disparate normative frameworks. Chesterman points out that a number of Asian jurisdictions have passed laws to protect privacy in terms of "functional restrictions", that is, "an activity is identified—the collection, use or dissemination of information characterised as private—and a legal regime is developed in the hope of restricting that activity to legitimate purposes" (at p. 11). Chesterman is correct to note that data protection is not synonymous with privacy, and that for Singapore, unlike in the United States or Europe, "the driving force behind reforms… was the economic imperative of globalization and the need to adopt standards that will afford trust in national institutions and seamless integration into global networks" (at p. 14). This pragmatic approach to data protection will inevitably clash with the notion of personal privacy. An individual may prefer to be "let alone"—the idea first mooted by Samuel Warren and Louis Brandeis in 1890 that has since become the foundation for a number of modern privacy torts recognised in the United States. It seems that some concession has been given to this interest with the inclusion of the Do Not Call ("DNC") Registry within the *PDPA*. Given Chesterman's comment that this is a "slightly odd fit" (at p. 39), it is a pity that this point is not explored in greater detail beyond two short paragraphs in the introductory chapter. Finally, Chesterman cites influential American privacy scholar Daniel Solove in his observation that "[r]ather than seeking an overarching theory of privacy, a better approach may be to consider whether it is possible to reconceptualise privacy from the bottom up, focusing on 'the concrete, the factual, and the experienced situations' of privacy" (at p. 12). This is a sensible way ahead for Singapore, but it is unclear if he agrees with Solove's taxonomy to identify and understand the different kinds of socially recognised privacy violations in contemporary society based on four basic groups of harmful activities: (1) information collection; (2) information processing; (3) information dissemination; and (4) invasion.

Chapter 2 by Tan Cheng Han S.C. examines the relationship between the online and offline (or "real") worlds, and highlights how new communication technologies can greatly facilitate the maintenance of familial and social bonds, but at the same

time, this democratisation of news can present significant challenges to governance and public policymaking. He observes that personal information that is posted on social networking sites, such as contact information, gender, preferences and partners, can be mined, used and abused by others. In particular, Tan notes that while the enactment of the *PDPA* is a step in the right direction to manage the flow of information online, "more needs to be done to educate individuals as to the effects that online behaviour can have offline" (at p. 47). Indeed, combating cyber-harassment, defamation and the invasion of privacy should not be confined to legislative enforcement, and Tan's comments underscore the importance of educating the public, especially the young, on the etiquette of online behaviour. The broad coverage of the new *Protection from Harassment Act 2014*, with its extraterritorial application, is likely to address some of Tan's concerns about the making of any threatening, abusive or insulting online communication that is likely to cause harassment, alarm or distress to an individual.

Chapters 3, 4 and 5 authored by Bryan Tan, Daniel Seng and Hannah Lim Yee Fen respectively, provide practical observations and approaches that help one navigate through the provisions of the *PDPA*. Chapter 3, titled "A Practitioner's Perspective", explores how the *PDPA* potentially impacts organisational behaviour and discusses a number of "hot-button" issues that could be focused on in the near term by legal practitioners advising organisations seeking to achieve compliance with the *PDPA*. Tan warns that there is no one-size-fits-all solution to comply with s. 24 of the *PDPA* (which requires an organisation to "protect personal data in its possession or under its control by making reasonable security arrangements to prevent the unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks") and postulates a useful list of administrative, physical and technical measures that organisations can consider. The complementary Chapter 5 highlights nine key principles outlined in the *PDPA* and applies them to employment settings, namely the pre-employment, employment and post-employment phases. These two chapters perhaps inadvertently expose some of the onerous obligations placed on organisations and employers, despite the intended adoption of a light touch approach in the design of Singapore's nascent data protection regime.

In Chapter 4, Daniel Seng presents a masterful analysis of the scope of data protection obligations of "data organisations" and "data intermediaries" under the *PDPA*. This is a must-read chapter. Seng contends that a "robust, purposive, activity-oriented characterisation exercise be undertaken so that data intermediaries may be properly classified as 'data organisations' under the *PDPA*—and be subject to the same data protection obligations" (at p. 107). He compares the *PDPA* regime to the EU's Data Protection Directive (EC, *Commission Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, [1995] O.J. L 281/31) and the Hong Kong *Personal Data (Privacy) Ordinance* (Cap. 486, E.R. 1 of 2013), and concludes that the absence of a clear definition of "organisations" in the *PDPA* is "patently unsatisfactory" (at p. 89). Seng proposes that a *pro tempore* definition of what constitutes a "data organisation" that is subject to the full obligations of the *PDPA* should be "a natural or legal person who *either alone or jointly with others* controls the collection, processing, use or disclosure of personal data" (at pp. 91, 92). Policymakers should certainly study his recommendation in greater detail.

Warren Chik in Chapter 6 expertly tackles the thorny issue of the DNC Registry which had received significant coverage in the Singapore media. He astutely discerns that "although the DNC provisions in Singapore are placed within the framework of a 'Personal Data Protection Act', in reality these provisions constitute something more like a 'Personal Privacy Law"' (at p. 145). Data protection regimes usually deal with personal data that can be pulled from individuals and seek to empower the individual by according to him or her greater control over how personal data is managed and stored. However, the DNC provisions appear to protect one's right to be let alone by preventing organisations that collect or have access to personal data from pushing unsolicited electronic marketing information to an individual, especially in an intrusive and aggressive manner. Chik does an admirable job of comparing the scheme under the *PDPA* to those in the United States, Canada, Australia and the United Kingdom. He highlights a number of areas in which Singapore's DNC regime may be improved—for example, expanding the regime to cover unsolicited messages sent using Voice over Internet Protocol technology, and specified messages addressed to Internet Protocol addresses and personal online accounts (at pp. 172, 173). Finally, Chik suggests that a Do Not Track ("DNT") regime, which consists of measures against both indirect marketing and geo-location tools, may be an appropriate evolution for Singapore's DNC regime in step with legal developments in the United States and Europe.

Chapter 7 by Abu Bakar Munir presents a descriptive view of Malaysia's Data Protection Law. While it is an informative essay, it sits awkwardly in the book with nary a comparison with analogous provisions of Singapore's *PDPA*. In contrast, in the final Chapter 8, titled "Comparison with Other Asian Jurisdictions", Graham Greenleaf pulls no punches in his incisive and candid critique of the *PDPA*. It is superbly researched and filled with penetrating insights. Greenleaf starts off by noting that the most informative comparisons for Singapore's *PDPA* are with South Korea, which may have the strongest data protection law in Asia, and Hong Kong, whose law is the longest-established comprehensive law and has seen a history of active enforcement (at p. 204). He also observes that Singapore has no constitutional protections of privacy, nor is it a party to any enforceable international conventions protecting privacy. He provocatively asserts that (at p. 220):

> The data protection principles in Singapore's PDPA can most positively be described as a minimal version of a "normal" data privacy law… It is also an extremely conservative implementation of data protection principles for the second decade of the 21st century, where the drafters seem to have learned little from European developments and almost nothing from their Asian neighbours.

In his analysis of the *PDPA's* regulation of international data flows, Greenleaf concludes that the Personal Data Protection Commission is proposing "to allow Singaporean organisations to otherwise wash their hands of any responsibility for exports of personal data from Singapore to anywhere in the world" and that this is "a bad result for Singapore's citizens and for any foreigners whose personal data end up in Singaporean hands" (at p. 227). On the issue of civil remedies, he looks to the Hong Kong regime, and observes that (at p. 237):

> Given the costs of initiating litigation in Singapore, and the risks of costs being awarded against the plaintiff, there is therefore no low-cost or low-risk means by

which Singaporean data subjects can seek modest amounts of compensation for data protection breaches.

Last but not least, Greenleaf concludes that even for such minimal principles, the *PDPA* is riddled with exceptions and the result is one of the weakest sets of principles in Asian data protection laws. There is much in this chapter for the Singapore government to consider and respond to, and for legal scholars to continue the debate of what an optimum regime might look like for Singapore.

Data Protection Law in Singapore contains many gems and it is a well-curated collection of essays that not only elucidate the operations of various provisions of the *PDPA*, but also challenge the narrow scope of this new data protection regime. It is a book that will appeal to anyone interested in privacy or data/information collection, management and use in the 21st century. Singapore is one of the last economically advanced countries in the world to enact a data protection law for its whole private sector. In his opening chapter, Chesterman suggests that the *PDPA* aspires to be "future-proof" (at p. 43). Perhaps the appropriate compass for the Singapore policymakers is to aim to be "future-ready" by embracing a legislative review process that not only keeps pace with the digital evolution, but more boldly anticipates and responds to the challenges ahead.

DAVID **TAN**
Associate Professor
Faculty of Law, National University of Singapore