DATA PROTECTION LAW IN SINGAPORE
Privacy and Sovereignty in an Interconnected World

The adoption of the Personal Data Protection Act transformed the legal regime for data protection in Singapore. This book explains the history and evolution of data protection in Singapore, highlights issues that are being worked out in practice and derives lessons that Singapore can learn from other jurisdictions — and that other jurisdictions can learn from Singapore. Bringing together leading scholars and practitioners in the field, the book will be of interest to the academic, legal and business communities. Key questions include how to reconcile notions of privacy in an information age, and how national laws can regulate an increasingly interconnected world.

The second edition includes new chapters examining how the legislation has kept pace with technological change and how individual rights have been balanced against business interests in the course of enforcing the law. It also has specialist chapters on image rights and data protection, as well as new chapters on accountability and cross-border transfers and enforcement.

CONTRIBUTORS
David N Alfred
Jansen Ae
Simon Chesterman
Warren B Chik
Law Ceb
Graham Georgett
Hannah Yee Fen Lim
Abu Bakar Munir
David Ngoy
Brian Tan
Tan Cheng Han SC
David Tan
Steve Tan
Yeong Zee Kin

DATA PROTECTION LAW IN SINGAPORE
Privacy and Sovereignty in an Interconnected World

Second Edition

Edited by
Simon Chesterman

ACADEMY PUBLISHING
DATA PROTECTION LAW
IN SINGAPORE

Privacy and Sovereignty in an
Interconnected World

SECOND EDITION

Edited by

Simon Chesterman
Dean and Professor
National University of Singapore
Faculty of Law

2018
Foreword

Data, including personal data, is an increasingly important resource in the digital age. The discerning and intelligent application of personal data will allow us to unlock the benefits of our Smart Nation initiatives and enhance the lives of Singaporeans. For businesses, the ability to harness personal data will be a significant competitive advantage in the digital economy. As the impetus to collect, apply and share personal data grows, our policies must strike a careful balance between enabling the use of data for innovative business purposes and addressing legitimate societal concerns over privacy and safeguards.

It is against this backdrop that Academy Publishing, Professor Simon Chesterman and other distinguished scholars and practitioners in the field of data protection have come together to produce the second edition of this seminal text on data protection law in Singapore. The Personal Data Protection Act (“PDPA”) came into force four years ago. This book comes at a time when we are embarking on a review of the PDPA to keep abreast of technological advancements and global developments. Our data protection regime must evolve in tandem with emerging issues such as artificial intelligence, the Internet of Things and multilateral frameworks for cross-border data flows.

This second edition offers diverse perspectives on new topics such as the relationship between data protection law and privacy rights in Singapore, the significance of accountability to data protection, and cross-border data transfers and enforcement efforts. It will help readers gain a deeper and more nuanced understanding of Singapore’s data protection regime by elucidating the multifaceted issues that underpin our regulatory model. I congratulate the authors and publishers on
their timely contribution to the national and global discourse on this important subject.

S Iswaran
Minister for Communications and Information

6 June 2018
CHAPTER 1

Introduction

By Simon CHESTERMAN

1.1
It is a truth barely worth repeating that the digital revolution has transformed the global economy. The world’s biggest taxi service today (Uber) owns no vehicles, while the largest hotelier (Airbnb) owns no property; the most comprehensive retailer (Alibaba) holds no inventory, while the most valuable media company (Facebook) creates virtually no content. The vital commodity in this new digital economy is data, especially personal data. That economic reality is clear, yet most of the world’s politics and laws remain fixed in 20th-century ideas of countries exercising jurisdiction over their fenced-off portions of the planet, while individual consumers enter into contracts with organisations that wish to collect, use and disclose their data.

1.2
Four years ago, the first edition of this book highlighted how such tensions were putting strain on traditional conceptions of privacy and the manner in which governments have tried to respond.

1.3
Challenges to privacy arise because keeping information about oneself from the public gaze is becoming more difficult and less desirable. It is more difficult because governments and corporations have access to more personal data about more people than at any point in human history. This goes well beyond the surveillance powers of the State and includes the various “smart” devices that we routinely carry on our person, siphoning up details of our communications and our movements. As more of our daily interactions with the world take place online, it is far easier to store and analyse that data, developing profiles
1.4 The challenges to sovereignty lie in the fact that the traditional response to such developments would be through legislation. Such laws are generally jurisdiction-specific, their power and legitimacy tied to a territorially bounded state. In the case of global data flows, however, users in one country may store their data in a second country, accessing it using software run by a company in a third country and so on. This leads to predictable co-ordination problems, but also market pressure. Establishing domestic standards for data protection that are too high may lead to multinational companies avoiding that jurisdiction; if standards are too low then users may not be confident sharing their data. International regulation is possible, similar to the co-ordination of postal and telephone services, but key Internet functions continue to be performed by a non-profit organisation incorporated in California and there is understandable wariness about transferring control of the Internet to a body like the United Nations. For the time being, then, meaningful regulation with coercive powers therefore depends on states – but those regulations must be drafted with an eye on global as well as local concerns.

1.5 The ubiquity of data-collecting devices – on our person as much as on the streets and in the skies – has more recently given rise to a third set of challenges, which question the notion of data protection “law” as such.

1.6 The foundation of most data protection law around the world is consent. In theory, when personal data is collected, used and disclosed, that is in accordance with the agreement of the identifiable individual concerned, often through a contractual arrangement with an organisation. In practice, of course, users confronted with multi-page end-user licence agreements simply click “I accept” and get on with whatever they wanted to do in the first place. The British retailer GameStation provided a memorable example of this one April Fool’s Day, when more than 7,000 people clicked “I accept” to terms and conditions that included the surrender of their immortal souls to the
company. (The company later rescinded all claims, temporal and spiritual.)

1.7 Today, the sheer volume of data being collected renders such notions of consent questionable. Must one really “agree” with one’s phone, the lamp posts, Wi-Fi routers, bus route optimisers, autonomous vehicles, and so on that they can collect and use basic personal data? Even if one does, the proliferation of such “agreements” can lead to consent fatigue, making it hard for individuals to distinguish harmless services from those that are more pernicious.

1.8 This book once again examines the way in which Singapore has responded to these questions, in particular through the adoption of the Personal Data Protection Act 20121 (“PDPA”), the work of the Personal Data Protection Commission (“PDPC”) and the response of the private sector and the public at large in the years since the legislation came into force.

1.9 Singapore’s experience is of interest for at least three reasons. First, Singapore has long positioned itself as a hub for e-commerce and yet until 2012 had no data protection law. The PDPA was drafted in a sophisticated country with a highly connected population, drawing upon the experience of many other countries and extensive consultation with users and industry. The PDPA should be model legislation that is effective today, but also adaptable to changes in technology and user behaviour. It should be “future-proof”. As we will see, much still had to be worked out in practice and the ground has been laid for significant amendments in the near future.

1.10 A second reason to examine Singapore’s experience is that the goals of legislation were quite different from other jurisdictions. Whereas the European Union (“EU”) long approached data protection through the lens of human rights in general and the right to privacy in particular, Singapore’s legislation explicitly sought to balance the legitimate needs of business and the rights of individuals. In his second reading speech, Minister Yaacob Ibrahim emphasised that the purpose of the legislation was to:2

---

1 Act 26 of 2012.
2 Singapore Parliament Reports (Hansard) (15 October 2012) “Personal Data Protection Bill” vol 89 (Assoc Prof Dr Yaacob Ibrahim, Minister for (cont’d on the next page)
... strengthen Singapore’s overall competitiveness, and enhance our status as a trusted hub and choice location for global data management and processing services.

The emphasis on the economic impact of the legislation is clear – indeed, the word “privacy” does not appear even once in the Act. Yet it is also striking that, in the years since, many other jurisdictions have also backed away from the language of privacy – most prominently the EU itself: the new General Data Protection Regulation\(^3\) ("GDPR") that came into force in May 2018 similarly eschews the language of “privacy” in its human rights sense.\(^4\)

1.11
That is linked to a third point of interest, which is Singapore’s unique political environment and the nature of the relationship between the Government and the governed. Public agencies are excluded entirely from the PDPA’s coverage, with provision for the Minister to extend that exclusion to any statutory body by notification in the Gazette. When questioned on this in Parliament when the PDPA was enacted, the Minister stressed that the public sector has its own data protection rules, which he said are “guided broadly by the same principles”\(^5\) as the PDPA. As those rules are not public, however, this statement is difficult to evaluate. Since the first edition, there have been some steps towards greater accountability for government collection, use and disclosure of

---

3 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

4 Unlike the EU, Singapore does not recognise a right to privacy. Indeed, former Prime Minister Lee Kuan Yew’s dismissal of the idea is often invoked in such discussions:

I am often accused of interfering in the private lives of citizens ... Had I not done that, we wouldn’t be here today. And I say without the slightest remorse: that we wouldn’t be here, we would not have made economic progress, if we had not intervened on very personal matters – who your neighbour is, how you live, the noise you make, how you spit, or what language you use.


5 Singapore Parliament Reports (Hansard) (15 October 2012) “Personal Data Protection Bill” vol 89 (Assoc Prof Dr Yaacob Ibrahim, Minister for Information, Communications and the Arts) (closing speech after the second reading of the Personal Data Protection Bill 2012, included as Appendix C in this book).
information through the Public Sector (Governance) Act\(^6\) passed in January 2018, which imposes fines and jail terms for public sector officers who share data without authorisation.\(^7\) This is particularly important with initiatives like Smart Nation and a proposed national digital identity scheme gathering ever more data about the population.

1.12 Moves to ensure high levels of security in the public sector – including the extraordinary step of isolating hundreds of thousands of government computers from the Internet – show that issues of cybersecurity are taken seriously. Even as the private sector is being encouraged to hold itself more accountable to regulators and consumers, it is timely to see greater transparency about the Government’s own accountability structures in the handling of personal data.

1.13 The second edition of the book includes five new chapters and an entirely new structure, dividing the volume into three parts.

1.14 Part I examines the changing context within which data protection debates are played out.

1.15 In the next chapter, I discuss the ways in which information is now produced, stored and shared, and the implications for privacy and data protection. Legal protections of privacy have always been reactive, but the coherence of any legal regime has also been undermined by the lack of a strong theory of what privacy actually means. There is more promise in the narrower field of data protection. Singapore offers an interesting study of this shift. In particular, the passage of the PDPA suggests the possibilities and limitations of an approach to data protection that eschews both the EU’s privacy-rights-based understanding and the \textit{ad hoc} sectoral patches that have characterised US legislation on the subject.

1.16 Chapter 3 by Tan Cheng Han SC looks at the changing relationship between the online and the offline (or “real”) world. Early analysis of

\(^6\) Act 5 of 2018.
\(^7\) Public Sector (Governance) Act 2018 (Act 5 of 2018) s 7. This is not limited to personal data but does include reidentification of anonymised data: s 8.
Data Protection Law in Singapore

the impact of the Internet assumed that these two worlds could be kept distinct. That view is no longer tenable. As the boundary between them blurs, there is enormous promise in greater connectivity that facilitates social interaction, commerce and a more informed relationship between Government and governed. Yet there are also risks to privacy and exploitation of personal data. Legislation such as the PDPA is therefore necessary but not sufficient in protecting individuals and managing the flow of information. Understanding that landscape and educating users as to its promise – and its pitfalls – will be essential.

1.17
In chapter 4, Lanx Goh and Jansen Aw offer a detailed study of the relationship between data protection laws and privacy. Across various common law countries, privacy has come to be recognised as a standalone right – though its content remains ill-defined and its contours unclear. This trend has not yet reached Singapore. Data protection law, it is argued, offers more certainty – but it is routinely conflated with a right to privacy. Taking recent case law of Singapore’s PDPC as a departure point, Goh and Aw contrast the protections under the PDPA and other provisions such as the common law rights under breach of confidence and legislative provisions that might be loosely termed “privacy rights”.

1.18
The other rapidly evolving context for data protection law is the technology with which it must keep up. Steve Tan surveys this fast-moving landscape in chapter 5, focusing on two changes in particular. The first is the proliferation and interlinkage of networked devices known as the Internet of Things. As “smart” devices communicate with each other, vastly more data will be collected and used, often linked to identifiable individuals. This gives rise to the second change, which is the ability to analyse that data to tailor goods and services to the needs of consumers, or to track what they do and predict what they will do next. Both raise significant data protection issues that challenge the existing legal framework.

1.19
Part II of the volume turns to various practical matters that arise in implementing data protection law in specific contexts.

1.20
Bryan Tan offers the perspective of a practitioner in chapter 6. Many organisations’ business models now depend on the collection, use and disclosure of personal data. Compliance with the PDPA was never intended to be unduly onerous, but it has required many organisations
to develop new processes and practices. The chapter focuses in particular on the need to address questions of how data is retained and transferred, as well as limitations on its use for analytical, recruitment, and marketing purposes.

1.21 Chapter 7 turns to a key problem in data protection, which is its application to data intermediaries. Daniel Seng highlights the difficulty of distinguishing data intermediaries from data organisations under the PDPA. The significance of the distinction is more than semantic, as intermediaries have less onerous obligations. Yet the way in which information is now collected, used and disclosed makes drawing the line between the two classes of entities extremely difficult. It may also be undesirable, as the less onerous obligations may leave users with no remedy in the event of a data breach by the “intermediary” that is not attributable to the “organisation”.

1.22 In chapter 8, Hannah Lim Yee Fen focuses on data protection in the employment setting. Contrasting the PDPA with the EU Data Protection Directive, she maps out how nine data protection principles will affect employer-employee relationships. Though there has been much concern expressed on the part of small and medium enterprises worried about compliance costs, the exceptions applicable to an employment setting – in particular, circumstances in which notification is not required, consent can be deemed and access to data can be denied – are broad. In general, she concludes that the “light touch” regime is largely favourable to employers.

1.23 David Tan offers an analysis of image rights and data protection in chapter 9. “Personality rights” are recognised in jurisdictions like the US, encompassing the right of famous persons to exercise commercial control of their identity. This has not extended to Singapore, but the possibility of private action for breaches of the PDPA might allow for some measure of compensation in the event that the personal data in such images is collected, used or disclosed inappropriately. In the alternative, the tort of passing off might provide for a remedy in some cases.

---

8 Directive 95/46/EC of the European Parliament and of the Council 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.
1.24 Warren B Chik discusses the part of the PDPA that frequently generated the most interest and which came into force first on 2 January 2014: the Do Not Call Registry. After setting out the challenges that the rise of electronic marketing have presented, chapter 10 recounts the experience of the US and other jurisdictions and how this helped shape Singapore’s approach. He also discusses emerging debates in related areas, in particular the move to provide for “do not track” software and discussion in the EU as to whether individuals should have a “right to be forgotten”, as well as how the DNC has been enforced in practice.

1.25 Part III examines some of the new frontiers of data protection, both metaphorical and literal.

1.26 There is a tendency in many jurisdictions, for example, to focus on compliance as the motivating factor in data protection law. Chapter 11, by Yeong Zee Kin, discusses the past, present, and future use of accountability as a data protection principle. Though the term is not used in Singapore’s laws at present, it is broadly consistent with the current approach and may offer a more robust framework for handling personal data protection that does not rely on outmoded conceptions of consent. This is important as Singapore moves to broaden the bases for collection, use and disclosure to include deemed consent by notification and a legitimate interest exception, for which consent is not a requirement.

1.27 Chapter 12, by David Alfred and Lanx Goh, considers cross-border issues in data protection. The shrinking and flattening of the world has led to two types of challenge for meaningful data protection. The first is how to ensure data receives appropriate protection even as it moves beyond the jurisdiction. The second is how to balance the need for international co-operation in enforcing data protection laws without unduly restricting the free flow of data more generally.

1.28 The final chapters situate Singapore’s legislation in its regional context. In chapter 13, Abu Bakar Munir provides an overview of Malaysia’s Personal Data Protection Act, which was enacted in 2010 and came into effect on 15 November 2013. Malaysia’s experience provides a useful counterpoint to Singapore’s. This includes some similarities, such as the exclusion of public bodies from the data
protection regime. It also includes significant differences, such as the creation of data user forums that can generate binding codes of practice and the process for managing transfer of data outside the jurisdiction.

1.29
The final chapter by Graham Greenleaf casts a more sceptical eye over the PDPA, comparing it with the legislation adopted in other Asian jurisdictions. The protections that it offers are more limited than in many of those jurisdictions – though half have no data protection legislation at all. Those protections that are included are subject to exceptions and potential exemptions that may limit the impact on data users, arguably due to the need for the regime to be “business-friendly”. That said, the enforcement mechanisms in Singapore’s PDPA are significantly stronger than its regional counterparts – in both the variety of penalties and their relative seriousness, including fines of up to $1m.

1.30
The medium- and long-term impact of the legislation is still to be determined. The commencement of another round of consultations with an eye to amendment reflect an acknowledgement that the PDPA remains a work in progress. Regulations and guidelines have helped to shape implementation, even as sanctions have been imposed on the more egregious violators of the law. The lasting effects will depend not only on the global environment and the various branches of government, but also on how consumers and industry react to the evolving regime. In a post-privacy world, in which sovereignty can only be expressed meaningfully by remaining interconnected with a globalised economy, the challenges to regulating data protection appropriately are complex and complicated. The starting point is understanding. In that project, it is hoped that this second edition offers some further illumination as to how Singapore can achieve its aim of being a trusted node in the new digital economy.

Excerpt from Simon Chesterman (ed),
Data Protection Law in Singapore
(2nd edn; Academy Publishing, 2018).
Click here for more information and to buy the book.