# Data Privacy Laws in Asia—Context and History

(Chapter 1 of *Asian Data Privacy Laws – Trade and Human Rights Perspectives*, Oxford University Press, 2014)

Graham Greenleaf, Professor of Law & Information Systems, UNSW Australia

*Abstract:* The first chapter of *Asian Data Privacy Laws* opens with illustrations from across Asia of where laws protecting data privacy have made a difference to individual lives. The main focus of the book is those specialised laws which systematically regulate the use of information about people, covering either or both of a country's public sector or most of its private sector. Fourteen of twenty six jurisdictions in Asia now have such laws, from over 100 countries globally with such laws. 'Asia,' for the purposes of this book, comprises the three sub-regions of South Asia, South-East Asia and North-East Asia. Other laws regulating data privacy are also considered, including constitutional, criminal and civil law protections. All twenty six Asian jurisdictions are covered in this book.

When considering data privacy protection in Asia, it is necessary to remember 'we're not in Brussels anymore.' Whereas European data protection law is based on a few key legal instruments, and there are European institutions that give them life, in Asia there are no equivalent binding treaties, or equivalent pan-Asian (or even sub-regional) institutions. A study of data privacy protection in Asia must be a 'bottom up' study, whereas the European approach can properly be 'top down'. It is not only national laws that must be given priority in a study of privacy in Asian countries, but also the situation regarding democracy and the rule of law in each country, which can overwhelm other considerations. In contrast, when considering data privacy laws in Europe (either within the EU countries or the broader Council of Europe countries) it is reasonable to assume both the existence of national democratic institutions and the rule of law.

Comparative studies of national data privacy laws and their administration, or of the underlying principles of such laws and what constitutes effective administration of such laws, are still relatively uncommon, except for the region of the EU. However, a survey of existing comparative works on a global canvas provides a number of hypotheses about data privacy protections which a book such as this may help to test.

The book is structured into three Parts: Part I—Asia and international data privacy standards (chapters 1–3); Part II—National data privacy laws in Asia (chapters 4–16); and Part III—Regional comparisons, standards, and future developments (chapters 17–20).

This introductory chapter concludes with brief discussions of the relationships between fundamental rights and 'Asian values'; of the implications of democracy for data privacy in a half-democratic Asia; and of conflicting interests in surveillance (public and private sector) and in 'free flow' of personal data.

Also included with Chapter 1 are the Foreword by Allan Chiang, Privacy Commissioner for Personal Data, Hong Kong, the author's Preface and Acknowledgements, and the Table of Contents.

Details of availability of the book are at <http://ukcatalogue.oup.com/product/9780199679669.do> and at <http://www2.austlii.edu.au/~graham/publications/2014/Greenleaf_flyer-5.pdf>.

# Asian Data Privacy Laws

*Trade and Human Rights Perspectives*

GRAHAM GREENLEAF

OXFORD
UNIVERSITY PRESS

OXFORD
UNIVERSITY PRESS

Great Clarendon Street, Oxford, OX2 6DP,
United Kingdom

Oxford University Press is a department of the University of Oxford.
It furthers the University's objective of excellence in research, scholarship,
and education by publishing worldwide. Oxford is a registered trade mark of
Oxford University Press in the UK and in certain other countries



First Edition published in 2014

Impression: 1



Published in the United States of America by Oxford University Press
198 Madison Avenue, New York, NY 10016, United States of America

British Library Cataloguing in Publication Data
Data available

Library of Congress Control Number: 2014940428

ISBN 978–0–19–967966–9

Printed and bound by
CPI Group (UK) Ltd, Croydon, CR0 4YY

# *Foreword*

Hong Kong's Personal Data (Privacy) Ordinance came into force 17 years ago in December 1996. At that time, Hong Kong was the first jurisdiction in Asia to have a dedicated piece of legislation on personal data privacy. As at August 2014, eleven other jurisdictions in the region have similar legislation. Globally, at least 104 jurisdictions have enacted data protection laws.

This trend reflects the growing recognition by governments of privacy as a fundamental human right. It also underpins the challenges generated by the pervasive use of new information and communications technologies in today's digital society, which has enabled the collection and use of vast amounts of personal data with phenomenal ease and efficiency. No doubt, technological innovations and applications such as the internet, social media, mobile applications and cloud computing have created great economic and societal values, and enhance the productivity and competitiveness of enterprises in ways beyond our imagination. At the same time, they also pose immense risks to privacy and raise serious concerns about the protection of personal data.

Against this privacy landscape, it is incumbent upon governments to put in place a regulatory framework that balances between the privacy rights of their citizens against other rights and public and social interests. In the process of introducing legislative intervention and administrative measures, they strive to foster mutual trust between businesses and consumers, promote continued use and development of information and communications technology, and facilitate cross-border data flows in an increasingly global digital economy.

Substantial developments since 1996 have taken place regarding the promotion and enforcement of privacy rights in one form or another among the many jurisdictions in Asia. Reports of these developments are found in the publications of the relevant regulatory bodies, privacy law journals, overviews by law firms, local and international media. However, an omnibus text providing a comprehensive review of the present state of play in privacy regulation in Asia has never been published.

*Asian Data Privacy Laws* is the first ground-breaking work to examine data privacy laws and data protection authorities across Asia. There is no person more suitable than Professor Greenleaf, an eminent and erudite scholar, to undertake this work. He has done an outstanding job in illustrating the increasing worldwide significance of data privacy and providing a thorough comparative assessment of the twelve data privacy laws in Asia, and broad sectoral laws in two other countries, and their enforcement against international standards.

Asia is well known for its diversity in culture, ethnicity, languages, political and legal systems. To write a book on any subject covering the whole region is inherently an uphill task. This is even more difficult for privacy and data protection as it is a specialised subject which is constantly evolving and requires a thorough understanding of the intricacies of the interplay among human rights ideologies, societal values, government policies as well as business interests.

I applaud Professor Greenleaf for pioneering this work, based on the wealth of background materials and insightful analysis that he has mastered over a prolonged period of persistent research. This comprehensive and authoritative book, written with verve and vigour, should prove to be a rich source of knowledge of privacy laws and practices in Asia for regulators, lawyers, privacy professionals, and academics within and outside the region.

Allan Chiang
Privacy Commissioner for Personal Data, Hong Kong

# *Preface*

*This book is dedicated to the Hon. Michael Kirby AC, CMG, former Justice of the High Court of Australia, in honour of his lifelong work to protect human rights and particularly the right of privacy. Aspects of his career most relevant to this book include his work as Chair of the OECD Expert Groups that drafted the OECD Privacy Guidelines, and the OECD Security Guidelines, Chair of the Australian Law Reform Commission during its report on privacy, recipient of the Australian Privacy Medal, Commissioner of WHO's inaugural Global Commission on AIDS, co-recipient of the Gruber Justice Prize, inaugural UN Special Rapporteur on Cambodia, and Chair of the UN's commission of enquiry into human rights in North Korea.*

Although data privacy, or 'data protection' as it is called elsewhere, has over two decades of history in Asia, it is only in the last few years that there have been significant developments in more than a handful of jurisdictions. This book covers 26 jurisdictions, from Japan to Afghanistan, and more than half of them now have significant—though often incomplete—data privacy legislation, most of it very recent, much of it untested by courts, and as yet insufficiently enforced by regulators. This book is intended to provide an early benchmarking in Asia's development of data privacy protections. That requires consideration of constitutional and treaty protections, and those found in the general civil and criminal law, not only specialized data privacy legislation, particularly for countries that do not yet have such legislation. Each country's law reveals something surprising and worth stating about privacy.

The aim of this book is to be an explanation, comparison, and critique of the data privacy laws developing in Asia. The efforts of many people across Asia to enact and then to enforce effective privacy laws are gradually succeeding, and there are many reasons for optimism. Strong criticism of some aspects of these laws is consistent with respect for the achievements to date. It is also consistent with the conviction that stronger and more effective protection of privacy through law is essential for the future of human rights and humanity, and for a sustainable market economy.

I have been involved in privacy administration, research, and advocacy almost continuously since the mid-1970s, although not full-time. I have kept an eye on privacy developments in Asia since the mid-1990s, and have had the opportunity to live in three countries in Asia, and to work in many others, since 1999. This book had its origins in 2007 when I was asked to give a seminar in London on data privacy developments in the Asia-Pacific. I discovered that a lot more was starting to happen than I had previously realized. Since then I have written regularly on Asian developments for *Privacy Laws & Business International Report*.

This book is written in the belief that privacy, in its many forms, is worth protection as an important part of our human rights, and that while law is not sufficient to protect privacy, it is indispensable for its protection. It is therefore necessary to keep advocating for better privacy laws, despite often slow and discouraging progress, and to recognize and document progress when and where it occurs.

The state of legal and other developments covered in this book is as at 31 December 2013. Where important developments after that date are known, they are mentioned briefly. Information based on web addresses (URLs) stated are last accessed and valid as at 31 December 2013 or later dates.

Periodic updates to developments in Asian data privacy laws after 1 January 2014 will be available from my SSRN pages at <http://ssrn.com/author=57970>.

*Graham Greenleaf*

# *Acknowledgements*

I have had the extreme good fortune to work with expert and generous co-authors in many Asian countries, without whom this book would be most unlikely to have been written—not least because I speak none of the languages of Asia other than English. My colleagues' linguistic expertise has also been invaluable to me when English-language sources were not available. This book owes the greatest debt to them, and although our jointly authored work is cited throughout the book, they have also each provided indispensable comments on each chapter concerning the jurisdiction in relation to which they have expertise, and their friendship and encouragement has supported its completion. Robin McLeish of the Hong Kong bar, and former deputy Privacy Commissioner, has for over a decade jointly authored articles and book chapters with me. Professor Whon-il Park and I have jointly authored articles for almost as long, and he has translated South Korean regulations and legislation not otherwise available, written privacy law commentaries on his KoreanLII website, and guided me during visits to Korea. Hui-Ling Chen, partner of Winkler Partners, Taiwan, has co-authored articles with me, written others I have relied on, and translated regulations when they were not available. Dr George Yijun Tian has translated a number of Chinese regulations and co-authored articles with me about them. Professor Fumio Shimpo has co-authored with me a number of articles on enforcement of Japan's laws, and patiently answered many questions. Professor Sinta Dewi Rosadi was joint author with me on an article on Indonesia, and a colleague for many years. I would also like to acknowledge other special assistance from Dr Rebecca Yoke Chan Ong, who shared her own unpublished research with me, and valuable dialogues over some years with Hong Kong's Privacy Commissioner for Personal Data, Allan Chiang, who also kindly agreed to write the foreword. Ken Chongwei Yang of Macau's Office of Personal Data Protection was similarly generous with assistance. My single largest thanks is to Jill Matthews, whose encouragement and knowledge of privacy issues has helped shape the book from its beginnings, and who read and expertly edited every chapter and prepared the index.

Valuable comments on various of the chapters in Parts I and III were made by Bob Gellman, Blair Stewart, Professor Charles Raab, Dr Roger Clarke; Professor Colin Bennett, Professor Dan Svantesson, Nigel Waters, and Chris Connolly. The publications of each of them, and those of Professor Jim Rule and Professor Lee Bygrave, have been particularly helpful. The chapters in Part II concerning individual Asian jurisdictions, or articles preceding them, have benefited from valuable comments by Robin McLeish, Professor Michael Tilbury, Commissioner Allan Chiang, and Deputy Commissioner Lavinia Chang (Office of the Privacy Commissioner for Personal Data), Assistant Professor Doreen Weisenhaus, Julianne Doe (Brandt Chan & Partners), and Professor Rick Glochefski (*Hong Kong*); Professor Whon-il Park, Professor Kyung-Sin Park, Professor Youngjoon Kwon, Kwang Bae Park (Lee & Ko, Seoul), Professor Nohyoung Park and Professor Haksoo Ko (*South Korea*); Hui-Ling Chen, Michael Fahey, Paul Cox, and Shan Lee (Winkler Partners), and Justice Dennis TC Tang (*Taiwan*); Scott Livingston (Covington and Burling, Beijing), Assistant Professor Dr Rebecca Yoke Chan Ong, Professor Albert Hung-yee Chen, Dr George Yijun Tian (*China*); Professor Fumio Shimpo, Professor Andrew Adams, and Professor Kiyoshi Murata (*Japan*); Ken Chongwei Yang, and his colleagues at the Office of Personal Data Protection (*Macau*); Chris Connolly (*ASEAN*); Professor Simon Chesterman (*Singapore*); Professor Abu Bakar Munir (*Malaysia*); Assistant Professor Dr Pirongrong Ramasoota, and Dhiraphol Suwanprateep and Nont Horayangura, Baker

& McKenzie, Bangkok (*Thailand*); My Doan and Christian Schaefer, Hogan Lovells International LLP, Ho Chi Minh City, and Dr Patrick Sharbaugh (*Vietnam*); Professor Sinta Dewi Rosadi and Professor Veronica Taylor (*Indonesia*); Cécile De Terwangne and Claire Gayrel (CRIDS, Belgium), Elonnai Hickock, Sunil Abraham, Prashant Iyengar, and Professor Ursula Rao (*India*); Rajan Sharma and Shalik Ram Sharma (*Nepal*); Ahmed Swapan Mahmud and Farjana Akter (VOICE) (*Bangladesh*); and David Banisar (Article 19) (*South Asia*). Despite the valuable input I have received from many people, responsibility for all content lies solely with me.

As well as these many individuals, I wish to thank the institutions that have assisted the completion of this book: Privacy Laws & Business, particularly publisher Stewart Dresner and editor Laura Linkomes, for their continuing support; UNSW Australia Faculty of Law, which has supported all aspects of my research over 30 years; the Australian Research Council for funding the 'Interpreting Privacy Principles' project; the European Commission for consultancy projects concerning Japan, India, and Hong Kong; Kyung Hee University, Seoul for various research fellowships from 2009–12 in Korea; the Japan Society for the Promotion of Science (JSPS) and the Centre for Business Information Ethics, Graduate School of Business Administration, Meiji University, Tokyo for a fellowship in Japan in 2012; the University of Edinburgh AHRC SCRIPT Centre for research fellowships in 2007 and 2011; the University of Hong Kong Faculty of Law for appointment as a Distinguished Visiting Professor in 2001–02 which allowed me to teach Hong Kong privacy law; the Bureau of Convention 108 of the Council of Europe, for their open approach; the Australian Privacy Foundation and its International Committee for taking a global view of privacy, particularly Roger Clarke and Nigel Waters (and for the continuing inspiration of their privacy advocacy); the members of the Asian Privacy Scholars Network; Privacy International, for its series of 'Privacy in Developing Countries' reports; Mirela Roznovschi and GlobaLex for its research guides; and AustLII's Dr Philip Chung, Professor Andrew Mowbray, and Kent Soestano, for collaboration on the International Privacy Law Library. The late Jon Bing, who from the 1970s made major contributions to data protection, access to legal information, and copyright, was a continuing source of inspiration.

Ruth Anderson, Gemma Parsons, and Matthew Humphrys at OUP have been very supportive of a project that was larger than we all expected, and expert in their guidance to its completion.

# *Contents*

# PART I

# ASIA AND INTERNATIONAL DATA PRIVACY STANDARDS

# 1

# Data Privacy Laws in Asia—Context and History



## 1. Privacy protection matters in Asia

It is often said that privacy is impossible to protect, either against governments or corporations. States develop comprehensive information systems concerning their citizens. Local businesses want to 'know their customers', and international businesses that run global social networks, search engines and the like, gather unprecedented amounts of personal information on their users.

What then is the relevance of a book about data privacy laws in Asian countries? If the data privacy laws in those countries and elsewhere, are futile gestures, destined to sit unaccessed in legal databases and unused, then this will be a book not worth reading (nor writing). Fortunately, this is not the case, and across Asia there are instances where the enforcement of data privacy laws has delivered remedies to individual people, and acts as a restraining influence on both businesses (local and global) and government agencies, from misusing personal information. Here are a few examples:

- The Octopus stored-value transport card, once the most respected brand name in Hong Kong, was found to have sold details of its cardholders to banks and insurance companies. Public and legislative pressure caused the resignation of Octopus' chief executive and chairman, disgorgement of its profits, and massive reputational damage.

The Privacy Commissioner's investigations, though hampered by inadequate powers, led to new laws with stronger powers and very high penalties for unauthorized use of marketing information.

- Among many cases in which South Korea's Personal Information Dispute Mediation Committees have ordered that financial compensation be paid, two involved plastic surgery clinics posting movies on their websites of plastic surgery operations without their patients' consent. Each patient was awarded compensation of US$4–5,000 for mental suffering.
- In China, Dun & Bradstreet's subsidiary Shanghai Roadway D&B Marketing Services Co. Ltd. was prosecuted under the criminal law provision protecting privacy, for illegally buying personal information on consumers. It was fined US$160,640 and four former executives were sentenced to up to two years each in prison. Dun & Bradstreet subsequently sold the company.
- Macau's data protection authority caused the suspension of use of mobile traffic surveillance cameras by the Traffic Services Bureau and the Public Security Police because their use might involve the collection and processing of sensitive data outside the sphere of public roads, and therefore lacked legitimacy.
- Indonesia's Constitutional Court held that interception by government agencies of personal communications, authorized only by ministry regulations, is a violation of the constitutional right to privacy. The Constitution required an Act by the legislature setting out exactly when interception is legal. Similar constitutional challenges have succeeded in Japan, India, Hong Kong, and Taiwan.
- The Hong Kong Privacy Commissioner, upheld on appeal, found that 'paparazzi'-style photo-journalism using systematic surveillance and telescopic lens photography to take clandestine photographs of TV personalities within their private residences is unfair collection of personal information which breaches the Hong Kong law, and is not justified by public interest considerations in the absence of any illegal conduct being involved.
- The Delhi High Court held that legislation more than a century old which criminalized homosexual sexual acts was unconstitutional because it breached the implied right of privacy in India's Constitution, and that there was no exception justifying this. The Supreme Court overturned this, but the government is now considering legislation.
- Taiwan's Financial Supervisory Commission fined two banks US$130,000 each for poor security which allowed hackers to discover bank customers' personal information. It also fined two insurance brokers US$20,000 each, because they illegally released personal information about policy holders to a life insurance company to help it market policies.
- Nepal's Supreme Court upheld its Information Commission's ruling that every student has the right to see his or her exam answer sheet. In some South Asian countries such 'right to information' laws are the first step toward giving back control of personal information to the individuals it most concerns.
- Constitutional courts across Asia have frequently found legislation unconstitutional because of constitutional privacy rights including: 'real name' requirements for Internet use in South Korea; an ID card based on an administrative order in the Philippines; and compulsory fingerprinting for the purpose of an ID card in Taiwan. The language of 'informational self-determination' is familiar to Asian constitutional courts.

- The world's most powerful information business has been unable to make privacy laws irrelevant. Macau's data protection authority fined Google for breach of its law, because when the Street View mapping service collected images in Macau's narrow crisscrossing streets and alleys, it was collecting sensitive data that could reveal people's private lives. The first decision of South Korea's data protection authority found Google's unilateral change to its terms of service (TOS) breached South Korean law in three ways and required changes. In Japan, a court ordered Google to stop suggesting search terms which associated a person with a crime, and pay compensation of US$3,000, on privacy protection and defamation grounds.

These cases and others are discussed in this book. As Rule puts it 'privacy codes matter—often quite sweepingly'. 'The control available to individuals over their own information, stands to be vastly strengthened or undermined by crucial legislation or court decisions.'[1] This book is written in that spirit. It aims to shine a light on the variety and vitality of Asia's data privacy developments.

## 2. Data privacy laws and other protections of privacy

What are 'data privacy laws'? How common are they around the world? How do they differ from other methods by which privacy is protected?

### 2.1. Privacy and data privacy/data protection

'Privacy' is a disputed concept, both in law and philosophy.[2] Philosophical arguments about how 'privacy' should best be conceptualized and defined, and the resulting arguments about the extent to which aspects of such a concept of privacy should be protected by law, can take many directions. However, such arguments are by and large outside the scope of this book, because the concept of 'data protection' (or 'data privacy', which is the term used in this book) is now relatively well defined as a set of 'data protection principles', which include an internationally accepted set of minimum principles plus additional principles which are evolving continually through national laws and international agreements. 'Privacy' also encompasses aspects of physical privacy which are not part of data privacy. In addition, 'data privacy' laws only apply to data processing that occurs outside the sphere of family and personal affairs, whereas 'privacy protection' is not so restricted. Whether the concept of 'data protection' is a subset of a broader concept of 'privacy', or whether the two concepts are overlapping, need not be resolved for the purposes of this book.

### 2.2. What are 'data privacy laws'?

Data privacy laws systematically regulate the use of information about people. They are also known as 'data protection' or 'fair information practices' laws. We call this information 'personal data' or 'personal information', and the individuals affected are sometimes called 'data subjects'. Data privacy laws essentially comprise a set of enforceable data privacy principles based on the 'life cycle' of personal data (collection, accuracy, security, use,

[1] James Rule, 'Conclusion' in James Rule and Graham Greenleaf (Eds.), *Global Data Privacy Protection: The First Generation* (Edward Elgar, 2008), p. 269.

[2] For a discussion of these issues, see Simon Chesterman, 'After Privacy: The Rise of Facebook, the Fall of WikiLeaks, and Singapore's Personal Data Protection Act 2012' (2012) *Singapore Journal of Legal Studies*, pp. 391–415.

disclosure, access, deletion, etc.) coupled with an enforcement structure backed by legal measures requiring compliance. Enforcement usually involves a data privacy authority, often called a 'Data Protection Authority' (DPA) or 'Privacy Commissioner', but often involves other enforcement authorities as well.

A useful legal analogy to data privacy is copyright. Both are bundles of rights which defy summation in a single phrase, but require precise enumeration of each right that makes up the 'bundle' that we call 'copyright' or 'data privacy' in shorthand. We think we know intuitively what 'copyright' means, but technically it is a bundle of specific rights ('adaptation' 'reproduction', etc.), which benefit authors (or other copyright owners), and differ between types of works. 'Data privacy' does not have a simple definition either, and is similarly a bundle of specific rights ('access', 'limited collection', 'security' etc.), benefiting data subjects in this case, and which can differ between types of personal information (e.g. credit information, or 'sensitive data'). In both cases, enforcement differs between countries, and takes many forms.

Since Sweden's Data Act of 1973 became the first national legislation to include most elements of what we now consider to be a data privacy law, legislation to protect privacy in relation to personal information has evolved in a largely consistent fashion in over 100 countries across the world, with some major exceptions remaining. International agreements concerning data privacy have contributed a great deal to the development of consistency of national data privacy laws. From the start of the 1980s the non-binding Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines[3] and the first binding international agreement, the Council of Europe Data Protection Convention,[4] both embodied substantially similar privacy principles expressed in somewhat different language. These and other international standards are discussed in Chapters 2 and 3.

For the purposes of this book, a country is considered to have a 'data privacy law' only if it has a national law which provides, in relation to most aspects of the operation of the private sector, or its national public sector, or both, a set of basic data privacy principles, to a standard at least including most of the OECD Guidelines or Council of Europe Convention, plus some methods of statutorily mandated enforcement (i.e. not only self-regulation). This is discussed further in Chapter 3. The focus of this book is on these more comprehensive laws, and some relatively general e-commerce and consumer transaction laws, not on narrower sectoral laws protecting only one type of information (e.g. credit information, medical data, or criminal histories), nor the scattered protective provisions found in many other laws. These laws will be mentioned briefly where important.

## 2.3. The global context—expansion of data privacy laws

There are now 101 countries with data privacy laws, and little sign that the rate of increase in the number of new laws is slowing down.[5] The rate of expansion has averaged 2.5 new laws per year for 40 years since the first Act in 1973, but it has been growth at an

[3] Organisation for Economic Cooperation and Development (OECD), *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* adopted by OECD Council on 23 September 1980 (OECD Doc. C (80)58/FINAL).

[4] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (European Treaty Series No. 108; adopted 28 January 1981) ('CoE Convention 108').

[5] Graham Greenleaf, 'Scheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories' (2014) 23(1) *Journal of Law & Information Science*; including 'Global Tables of Data Privacy Laws and Bills (3rd Edn., June 2013)' <http://www.jlisjournal.org/abstracts/greenleaf.23.1.html>; also at <http://ssrn.com/abstract=2280877>.

accelerating rate, not just linear growth.[6] So far, this decade has been the most intensive period of expansion in the 40-year history, with an average of over five new laws per year for 2010–2014. If such expansion continues, 50 new laws will bring the total to 140 or more by 2020 and as many as 80 new laws this decade. There are currently 48 data privacy laws outside Europe, 48 per cent of the total.[7] There is little room for expansion within Europe,[8] so the majority of the world's data privacy laws will soon be found outside Europe, probably by 2015. Data privacy laws are therefore becoming ubiquitous among the world's countries.

As well as providing some global context for a discussion of Asian developments, these geopolitical facts have considerable implications, which will be discussed throughout this book. First, restrictions on international data exports will no longer be primarily a question of 'to which countries are European Union member states allowed to export personal data' (important though that will continue to be), because the majority of countries with data export restrictions will be from outside Europe. Second, the major influence on the data privacy laws outside Europe, including in Asia, will be shown to be 'European standards'.[9] Third, although the influence of US companies and its government will remain extremely important, the USA is in an increasingly isolated position in not having a national data privacy law covering its private sector, and this puts it in an increasingly defensive position when attempting to influence global data privacy standards. The theme of external influences on Asian developments is of continuing importance, and is best understood in this changing geopolitical context.

## 2.4. Other laws regulating data privacy—constitutions and general laws

Other forms of legal protection give intermittent protection to data privacy, with much variation between countries. These include privacy torts, breach of confidence (both general principles and statutory rules), constitutional rights, surveillance limitation laws, and consumer protection laws. However, they do not provide the thorough and evolving protection provided by sets of data privacy principles. Nevertheless, they are covered in this book to the extent necessary to explain their importance in each case for privacy protection, and to provide the legal context for data privacy laws.

Similarly, international human rights agreements sometimes create rights, or require creation of rights at national level, which may protect privacy. Some general privacy rights have been employed by many courts in the protection of privacy and less frequently to specifically protect data privacy. The best examples are Article 17 of the International Covenant on Civil and Political Rights,[10] directly relevant to Asia, and (outside Asia) Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms 1950 (usually referred to as the European Convention on Human Rights

[6] The number of new data privacy laws globally, by decade, is: 9 (1970s), +12 (1980s), +20 (1990s), +39 (2000s), and +21 (the first four years of the 2010s), giving a total of 101.

[7] The geographical distribution of the current 101 laws by region is: EU (28); Other European (27); Asia (12); Latin America (9); Africa (11); North Africa/Middle East (6); Caribbean (4); North America (2); Australasia (2); Central Asia (2); Pacific Islands (0).

[8] There are 25 separate European jurisdictions which are not EU member states but do have data privacy laws, giving 53 European data privacy laws. Turkey and Belarus are the only remaining European states without data privacy laws.

[9] Graham Greenleaf, 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108' (2012) 2(2) *International Data Privacy Law*, pp. 68–92 <http://papers.ssrn.com/abstract_id=1960299>. This is discussed in detail in Chapter 19.

[10] UN International Covenant on Civil and Political Rights 1966 (ICCPR).

(ECHR)). These treaty protections do provide a basis in human rights law for data protection, but they have not yet been interpreted to encompass all the aspects of data privacy provided in specific data privacy instruments,[11] and their enforceability in Asia is far more limited than in Europe. The relevance of these rights to Asian countries is discussed in Chapter 2.

## 2.5. Regulation of data privacy other than by law

Laws are not the only means of regulating behaviour. In the area of information law, non-legal constraints are often given a tripartite classification:[12] markets, morality, and infrastructure (or 'code' in the terminology popularized by Lessig[13]), and (correspondingly) data privacy is affected by changes in business practices (competition), social attitudes (morality), and technology (infrastructure). There is little convincing evidence over the last 40 years that any non-legal constraints (without legislative backing) can prove effective in protecting data privacy against business and government self-interest in expanded surveillance. This negative conclusion applies to the effect of competition between firms based on 'good privacy practices', voluntary self-regulation (through codes of conduct, standard-setting, privacy seals, or spontaneous adoption by companies of privacy-enhancing technologies (PETs) or privacy-by-design), or the adoption by consumers of technical self-help methods (security measures, PETs, and counter-surveillance technologies). Bennett and Raab[14] survey most of these approaches and find little significant evidence of their success unless they are integrated into a data privacy regime. In that case they become 'co-regulation' supported by legal requirements, not 'self-regulation', and may be more effective, though studies are still lacking. A report focusing on the USA found that 'the majority of the industry self-regulatory programs that were initiated failed in one or more substantive ways, and, many disappeared entirely'.[15] In this book the adoption and effectiveness in countries across Asia of these means of non-legal regulation is discussed, where it is known, in the chapters on each country. However the emphasis remains on data privacy laws as the most likely effective means of protection. The lack of international standards for such non-legal measures is also discussed in Chapter 2.

Relevant here is the difference between enforcement of laws and compliance with them. The extent of compliance with data privacy laws is generally largely unknown, requiring studies of the sociology of businesses and government agencies that have rarely yet been done. Such compliance may occur for many reasons, and the extent of compliance with similar laws may vary between countries, but we usually have little evidence beyond the anecdotal. Enforcement of laws is often (but not always) more visible, and its effectiveness and extent can to some extent be measured and compared between countries.

[11] Lee Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer, 2002), p. 247; Lee Bygrave, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties' (1998) 6(3) *Int J of Law and Information Technology*, pp. 247–84.

[12] Additional regulating factors may need to be added to this theoretical structure, such as self-help and surveillance, but their relationship to the previous three factors is outside the scope of this book.

[13] Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books, 1999). For a summary of this approach, see Graham Greenleaf, 'An Endnote on Regulating Cyberspace: Architecture vs Law?' (1988) 21(2) *University of New South Wales LJ*, p. 593 <http://ssrn.com/abstract=2188160>.

[14] Colin Bennett and Charles Raab, *The Governance of Privacy* (2nd Edn., MIT Press, 2006), chs. 6 and 7.

[15] Robert Gellman and Pam Dixon, *Many Failures: A Brief History of Privacy Self-Regulation* (World Privacy Forum, 14 October 2011) <http://www.worldprivacyforum.org/2011/10/report-many-failures-a-brief-history-of-privacy-self-regulation/>.

## 3. The history and scope of Asian data privacy laws

What justifies a focus on 'Asia', and what does 'Asia' mean in this context? From that starting point, a brief sketch of the development of data privacy laws across Asia is provided.

### 3.1. 'Asia' as the focus

'Asia' is always a contentious term, partly because the origin of the word itself, indicating a relative position to the east of somewhere else, rather than a specific place.[16] The uses of 'Asia' are therefore legion, and often inconsistent. There is no correct usage, only uses that are explained and justified. For the purposes of this study, 'Asia' refers to the countries extending from Japan in the east to Afghanistan in the west, and from China in the north to Timor Leste in the south. It encompasses 26 jurisdictions, including the two separate legal jurisdictions within the People's Republic of China (i.e. the Hong Kong and Macau Special Administrative Regions (SARs)).

These 26 jurisdictions fall into three sub-regions that have distinctive political characteristics, and are the principal reason for confining the meaning of 'Asia' in this study to them. In geographical terms, these sub-regions are best referred to as Northeast, Southeast and South, because for two of them those terms have now become part of their self-description (as ASEAN and SAARC). In Northeast Asia six of the seven jurisdictions (the exception being North Korea) have significant data privacy laws. Part of the argument of this book is that sub-regional initiatives to protect human rights (including data privacy), and to promote trade, can be significant drivers in the development of data privacy laws, so it is reasonable to focus on three highly interconnected sub-regions. For convenience, the three regions are collectively described as 'Asia' in this book, but that is no more than a matter of convenience. Furthermore, this view of 'Asia' encompasses the two rising economic superpowers, China and India, the sub-regions within which they are the most significant geographical and economic countries, and the region between them (which is of considerable economic importance in itself).[17]

In South Asia the South Asian Association for Regional Cooperation (SAARC) comprises eight member states (Afghanistan, Bangladesh, Bhutan, India, the Maldives, Nepal, Pakistan, and Sri Lanka). SAARC has a moderately strong intergovernmental organization. Because Afghanistan is part of SAARC, it is covered briefly in this study, but other countries in 'West Asia' (e.g. Iran) and 'Central Asia' (mainly ex-USSR nations and Mongolia) are excluded.

The Association of Southeast Asian Nations (ASEAN) comprises 10 members (Brunei Darussalam, Cambodia, Indonesia, Lao People's Democratic Republic (PDR), Malaysia, Myanmar, the Philippines, Singapore, Thailand, and Vietnam). The modern self-identification of all these countries is now very clearly with ASEAN, although this was not always so, and so 'Southeast' is the most appropriate geographical term.[18] ASEAN has the strongest intergovernmental organization of the three sub-regions. Timor Leste has a well-advanced

[16] Tae-Ung Baik, *Emerging Regional Human Rights Systems in Asia* (CUP, 2012), pp. 13–17.

[17] Myint-U Thant, *Where China Meets India: Burma and the New Crossroads of Asia* (Farrar, Straus, and Giroux, New York, 2011).

[18] Some of these countries were sometimes described as 'Indo-China' to indicate the cultural and other influences of both India and China because of their geographical situation. During the British colonial period, Myanmar (Burma) would have been more closely identified with South Asia, and at some points in its history Vietnam would have been more closely identified with the Confucian-oriented Northeast Asia.

candidature to be the eleventh ASEAN member, and is therefore included in this book. New Guinea is not an ASEAN member (nor is its candidature well advanced), and it and the countries of the Pacific Islands are excluded from this study.

There is no regional intergovernmental organization which covers the seven jurisdictions of Northeast Asia considered here (China, Hong Kong SAR, Japan, Macau SAR, North Korea, South Korea, and Taiwan), but they have important shared cultural characteristics including Confucian and Buddhist influences, are politically closely engaged, and all except Hong Kong have modern legal histories in which the civil law plays a major role.

These 26 Asian jurisdictions are extremely diverse: politically (including in terms of democratic development), ethnically, linguistically, culturally (including religions), and in terms of historical development and colonial experience. Their diversities are far greater than those of the countries of Europe. Approximately half of these jurisdictions have a legal system derived from the common law, and half from the civil law tradition. Despite this diversity and the complexities it creates for any region-wide analysis of a particular type of law, such an analysis of the development of data privacy laws is worth undertaking. These laws, as will be seen, have a 'family resemblance' (not only in Asia but globally) from one jurisdiction to another, which makes comparative analysis possible and valuable.

An alternative focus for a study of data privacy laws could have been the countries that make up APEC ('Asia-Pacific Economic Cooperation'), a grouping of 21 'member economies' including nine from east Asia (but not India or other South Asian countries) and 12 from the Americas (north and south), Australasia, the Pacific (Papua New Guinea) and Russia. However, as this book will show, APEC's influence on data privacy developments in Asia is not very strong, probably no stronger than that of ASEAN, and of less influence than the European Union. This book covers APEC developments, developments in APEC countries in Asia, and all the non-APEC Asian countries, including the countries of South Asia.

## 3.2. A brief history of data privacy laws

The OECD's Privacy Guidelines (1980)[19] were an early influence on the development of data privacy laws in Asia. Japan has had an Act on the Protection of Personal Information Held by Administrative Organs governing public sector data since 1988, but it was strengthened to cover paper-based files and provide penalties for disclosures in 2003. South Korea first introduced a data protection law covering its public sector with the Public Agency Data Protection Act of 1995. Both Japan and South Korea, as OECD member countries, in covering only their public sectors, took a similar approach to some other OECD members outside Europe, namely Australia (1988), Canada (1982), and (prior to the OECD Guidelines) the USA (1974). Thailand's Official Information Act 1997 provided very incomplete data protection in relation to government agencies, and it has not yet been extended to the private sector.

In 1995 the colonial government of Hong Kong enacted the Personal Data (Privacy) Ordinance, which covered both the public and private sectors, and was therefore Asia's first comprehensive data privacy law. Taiwan's Computer Processed Personal Data Protection Act was enacted in 1995, dealing generally with the public sector but only eight specified private sector areas. South Korea's Act on Promotion of Information and Communications

[19] Organisation for Economic Cooperation and Development (OECD), *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*.

Network Utilization and Information Protection of 2001 (often called the 'Data Protection Act') did not cover the whole private sector but applied most generally to entities that process personal data for profit through telecommunication networks and computers. In 2003 Japan extended its laws to cover the private sector with its Act on the Protection of Personal Information. The Macao Special Administrative Region (SAR) Personal Data Protection Act (2006) was the first data protection law in Asia modelled directly on a European Union (EU) law (that of Portugal), and is potentially one of the strongest. Vietnam enacted a consumer law covering most aspects of private sector privacy protection in 2010, following e-commerce laws in 2005 and 2006, further strengthened by a 2013 regulation. In 2007 Nepal included almost all elements of a data privacy law for the public sector in its Right to Information Act. India purported to enact a data privacy law in 2011, for the private sector only, by delegated legislation under its IT law, with uncertain meaning, enforcement, or validity. In China, the most significant Asian country not to have a general data privacy law, the National People's Congress Standing Committee and one ministry have, since 2011, enacted five generally consistent laws and regulations covering Internet services and consumer transactions. They are of major significance in themselves because of the size of China's economy, whether or not a general data privacy law emerges from them.

In 2009 Malaysia became the first ASEAN country to legislate in relation to the private sector, but this legislation was only brought into force in 2013. In 2012 the Philippines enacted the Data Privacy Act, but it is not currently in effect because the data protection authority has not yet been appointed. Singapore enacted its Personal Data Protection Act in 2012, and by January 2013 it was in force, with a data protection authority appointed. Indonesia enacted a government Regulation in 2012 to bring the data privacy part of the Law on Electronic Information and Transactions of 2008 into effect. This ASEAN activity in 2012–13 also involved the first regional declaration in Asia concerning data privacy, the ASEAN Human Rights Declaration,[20] with a specific reference to personal data included in its clause concerning protection of privacy.

Further progress in 2012–13 made this the most intense period of development of data privacy laws in Asia: existing data privacy laws have been strengthened a great deal. There have been comprehensive amendments (effectively new laws) in South Korea (on paper, the strongest law in Asia) and in Taiwan (extending the law to all sectors, and strengthening it), plus major amendments in Hong Kong (generally strengthening enforcement, and with major new rules and penalties concerning sale of personal data), and new e-commerce regulations in Vietnam and Indonesia. Asia has therefore now commenced on a 'second generation' of stronger data privacy laws. Further new laws are also likely. At the time of writing in 2013, a comprehensive private sector Bill is before Thailand's Parliament. Japan has created the nucleus of a data protection authority, and proposed the first major revisions to its law, and a full DPA, by 2015. Government preparation of Bills has been reported in relation to Brunei and Laos, and various official and semi-official Bills for comprehensive laws have been drawn up in India but do not yet have government endorsement.

From this brief survey we can conclude that, as at the end of 2013, data privacy laws are found in 12 jurisdictions in Asia, from all three sub-regions, covering most of the private sector in nine jurisdictions (South Korea, Hong Kong SAR, Macau SAR, Taiwan, Singapore, the Philippines, Malaysia, Japan, and India), and the public sector only in two

[20] *ASEAN Human Rights Declaration*, 18 December 2012, <http://www.asean.org/news/asean-statement-communiques/item/asean-human-rights-declaration>.

jurisdictions (Thailand and Nepal). Three more (China, Vietnam, and Indonesia) have broad sectoral laws, dealing with the Internet, e-commerce, and consumer transactions. Fourteen of the 26 jurisdictions covered in this book therefore already have significant laws, and proposed Bills have been drafted which when enacted will extend this. Each of the remaining 12 countries have some other forms of privacy protection (at least on paper), and some may well enact data privacy laws, so the political and legal context in each is discussed briefly. The number of new data privacy laws in Asia is expanding, and the strength of existing laws increasing, factors shared with other regions of the world. Data privacy laws are therefore now a common factor in the Asian legal landscape, although not universal nor (as we will see) anything close to uniform.

### 3.3. 'Legal transplants'

'Legal transplants', or the importing of legal rules from one country to another, can range from the adoption of large parts of a whole legal system (such as Japan's adoption of German commercial law in the late nineteenth century), to the incorporation of a single legal rule into an otherwise existing body of law (from Japan again, the adoption from US corporate law in 1950 of a single rule concerning a director's duty of loyalty).[21] They are controversial at many levels: 'Commentators are split between those who proclaim the feasibility of transplantation as a device of legal change, and those who claim that they are impossible.'[22] Furthermore, there is disagreement on both the conditions for successful transplants, or even how success should be measured. Perhaps, as Kanda and Milhaupt suggest, success simply means 'use of the rule in the same way as it is used in the home country, subject to adaptations to local conditions', whereas failure is marked by the rule being ignored in the host country, or resulting in unintended consequences.[23]

Are data privacy laws legal transplants? Data privacy laws originated as a 'Western' notion, in that their earliest legislative instantiations were in North America (1970 and 1974[24]), and in seven western European countries in the 1970s.[25] Furthermore, the principal players who negotiated their transformation into an international standard, the OECD Guidelines, in 1978–80 were from Europe, North America, and Australasia. In that sense, data privacy laws are not indigenous to any Asian country. The collection of legal rules that characterize a data privacy law was not to be found anywhere in Asia prior to 1988, and any of the laws enacted up to the early 1990s would be unlikely to have been enacted if it were not for the existence of the OECD Privacy Guidelines. Since the mid-1990s, the EU Data Protection Directive[26] (the 'EU Directive') has been at least as strong an influence as the OECD Guidelines.

This study will not bear directly on the fundamental disputes about legal transplants within the field of comparative law, but it should provide an interesting case study of the history of a legal transplant, taking place across Asia. Assuming data privacy laws are legal transplants, this study will aim to reveal whether any of these laws are merely window

[21] Hideki Kanda and Curtis Milhaupt, 'Reexamining Legal Transplants: The Director's Fiduciary Duty in Japanese Corporate Law' in Daniel Foote (Ed.), *Law in Japan: A Turning Point* (University of Washington Press, 2007), p. 437.

[22] Kanda and Milhaupt, 'Reexamining Legal Transplants' in Foote (Ed.), *Law in Japan*, p. 439.

[23] Kanda and Milhaupt, 'Reexamining Legal Transplants' in Foote (Ed.), *Law in Japan*, pp. 437–40.

[24] US Fair Credit Reporting Act of 1970 and US Privacy Act of 1974 (Federal agencies).

[25] Graham Greenleaf, 'Scheherezade and the 101 Data Privacy Laws'.

[26] *European Communities (EU) Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, adopted 24 October 1995* (O.J., L 281, 23 November 1995, p. 31 *et seq.*).

dressing (i.e. ignored), or whether they are misused, producing consequences contrary to those in their place of origin. We also need to ask: if data privacy laws are legal transplants, where are they transplants from, other than diffusely from 'the West'? Are they from the common law or civil law traditions of the West, or from some hybrid source? Is a law a transplant if its main drivers are international agreements (consider the Berne and World Intellectual Property Organization (WIPO) conventions on copyright), even if only of the 'soft' variety, such as the influences of the OECD Guidelines or the EU Directive?

## 4. Structure and purposes of this study

This section considers where this study fits in with previous scholarship on data privacy and concludes with an outline of the structure of the book.

### 4.1. We're not in Brussels anymore . . .

Kuner's *European Data Protection Law*[27] centres its analysis around the unifying Europe-wide (or in most cases, EU-wide) features of European data privacy law, and regards national laws as the 'important details contained in the law of the EU Member States'. But Asia is not Europe, so this must be a very different book. As Kuner says in the first chapter, 'European data protection law is based on a few key instruments' and there are European institutions that give them life. However, in Asia there are no binding treaties equivalent to Council of Europe Data Protection Convention 108, or Article 8 of the ECHR or other mandatory instruments like the EU's 'constitutional' data protection,[28] or the EU Directive. There are no international courts which can make binding decisions on issues relating to data protection, unlike the European Court of Justice (ECJ or CJEU) on questions such as whether EU member states have properly implemented the Directive (for example, the cases on independence of data protection authorities), or the European Court of Human Rights (ECtHR) on the interpretation of Article 8 of the ECHR. There is no equivalent to the European Commission or the Article 29 Working Party, organizations that give substance to the EU Directive. There is none of this at all.

In Asia, as we will see in the next chapter, there is no 'Brussels', nor even a 'Strasbourg'—no Asian equivalents to the EU or the Council of Europe, their deliberative bodies or their courts. In Asia there are no binding international agreements on data privacy, with the exception of the few words in Article 17 of the International Covenant on Civil and Political Rights 1966 (ICCPR), equivalent to ECHR Article 8. Even so, very few Asian countries have adopted the Optional Protocol to allow it to be enforced through the UN human rights system, which in any event lacks any equivalent to the ECtHR. APEC is based on the fact that it is *not* a treaty, and APEC does not usually develop any legally enforceable or otherwise binding agreements. Whether APEC's Cross-border Privacy Rules (CBPR) will succeed in adding something binding remains to be seen. ASEAN has not developed binding commitments on privacy, only the non-binding ASEAN Declaration on Human Rights. SAARC has done nothing. In Northeast Asia there is no regional organization. There is no Asia-wide organization of states equivalent to the Council of Europe.

[27] Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (2nd Edn., Oxford, 2007).

[28] The Treaty of Lisbon 2009, including the European Union's Charter of Fundamental Rights: see Sybe de Vries, Ulf Bernitz, and Stephen Weatherill (Eds.), *The Protection of Fundamental Rights in the EU After Lisbon* (Hart, 2013), pp. 1–3.

From one end of Asia to the other, there is therefore nothing comparable to the European-wide or EU-wide data privacy structures which are at the core of data privacy protection in Europe. Consequently, an Asian analysis of data privacy must take the national laws, in all their very considerable diversity, as the starting point. In Asia, national laws are the foreground, with international considerations in the background (and even then, global not regional considerations have been more important). This must be a 'bottom up' study, whereas the European approach can properly be 'top down'.

### *Democracy and the rule of law in Asian countries*

It is not only national laws that must be given priority in a study of privacy in Asian countries, but also the situation regarding democracy and the rule of law in each country, which can overwhelm other considerations. In contrast, when considering data privacy laws in Europe (either within the EU countries or the broader Council of Europe countries) it is reasonable to assume both the existence of national democratic institutions and the rule of law. In almost all cases European countries are fully developed democracies with periodic changes of governing political parties through free and fair elections. Similarly, the rule of law in these countries is maintained by courts with at least moderate levels of integrity in enforcing laws, with only a few exceptions. Neither of these generalizations hold true across the whole of Asia. While some Asian countries have democratic institutions as strong as those typical of Europe, the 26 Asian jurisdictions covered in this study are at best 'half democratic', as a whole, summarized in section 5.2 of this chapter as 12 democracies, 9 semi-democracies, and 5 authoritarian states. Similarly, while some Asian jurisdictions have extremely high reputations for maintenance of the rule of law (and these are not necessarily the 12 democracies), in many Asian countries, perhaps most, the rule of law is still a work-in-progress at best. Unlike in Europe, these matters cannot be assumed.

## 4.2. Comparative studies of data privacy

Comparative studies of national data privacy laws and their administration, or of the underlying principles of such laws and what constitutes effective administration of such laws, are still relatively uncommon, except for the region of the EU. Few comparative works are on a global canvas. Rule et al., *The Politics of Privacy*[29] (1980) while primarily focusing on US developments, provided an analysis of the development of privacy principles, prior to the first international privacy instruments in 1980–81, which has continuing global relevance. Flaherty's classic study *Protecting Privacy in Surveillance Societies*[30] (1987) compares the early experiences of data protection authorities in five European and North American countries. Bennett's *Regulating Privacy*[31] (1992) compares the development of data privacy laws in Sweden, the USA, West Germany, and the UK. A decade later, Bygrave's *Data Protection Law*[32] (2002) undertakes a comparative analysis of how the key privacy principles have been implemented with reference to both European and non-European examples, but only briefly in a study focusing on other matters.[33] Bennett and

[29] James Rule et al., *The Politics of Privacy* (New American Library, 1980).
[30] David Flaherty, *Protecting Privacy in Surveillance Societies* (Chapel Hill, 1989).
[31] Colin Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press, 1992).
[32] Lee Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer, 2002).
[33] Lee Bygrave's 2014 book was not available at the time of writing.

Raab's *The Governance of Privacy*[34] (2006) is the standard work on 'privacy regimes' as a whole but, as is reasonable from two political scientists, it does not attempt any detailed legal explanations of privacy principles or enforcement, and has little to say on individual countries. There are recent comparative studies of some key aspects of data privacy regimes. Kuner's *Transborder Data Flows and Data Privacy Law* (2013)[35] compares cross-border data flow regulation in both international instruments and national laws. Svantesson's *Extraterritoriality in Data Privacy Law*[36] does a similar comparison for claims of extraterritorial effect. Both are considered in Chapter 17 and elsewhere.

The most extensive collections of country studies are the collectively authored global survey *Privacy & Human Rights 2006*,[37] which focused equally on data privacy laws and surveillance developments, and covered over 70 countries in its tenth (and, it seems, final) edition, including many countries in Asia.[38] *Global Data Privacy Protection: The First Generation*,[39] edited by Rule and Greenleaf, contains chapters on the histories of privacy protection in seven countries in Europe, North America, Asia, and Australasia, but does not include a detailed comparison of national laws. There are now many compilations of descriptions of the privacy laws of various countries by authors based in law firms, with varying coverage of Asian countries, but these (while sometimes useful) are usually limited to the basic facts about each country's key data privacy legislation. In relation to Asia, there is no comprehensive comparative study. Books on data privacy in specific Asian countries are noted and cited in the country chapters to which they are relevant.

## 4.3. Hypotheses about data privacy protections—global and regional

In the absence of comparative Asian studies of privacy it may be valuable to ask what hypotheses or conclusions have been put forward in European or global studies, and to what extent have these been supported or contradicted by the experience of Asian data privacy laws? From at least the 1970s onward, scholars (in particular, those mentioned in the previous section) have advanced important and interesting hypotheses, on issues such as: what ideologies or policy choices underlie the standards (privacy principles) embodied in data privacy laws; whether such laws, and the role of data protection authorities in particular, function to legitimate the expansion of data surveillance, or to critique and limit its expansion; whether a dedicated data protection authority is necessary (or optimal) for a data privacy law to be effective; to what extent is there convergence or divergence in the form and content of data privacy laws; what explains such convergence as exists; and whether there is a 'race to the top' or a 'race to the bottom' in the strength of data privacy laws, between jurisdictions competing for economic advantage (a theory of 'regulatory arbitrage' or 'relocation thesis'). The extent to which data privacy developments in Asia shed light on these hypotheses is discussed in the concluding chapter of this book, and in other chapters where this becomes relevant.

The big questions in the study of data privacy are rarely new questions. It can usually be argued that new technologies and practices—mobile computing, cloud computing, social

[34] Colin Bennett and Charles Raab, *The Governance of Privacy* (2nd Edn., MIT Press, 2006).
[35] Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press, 2013).
[36] Dan Svantesson, *Extraterritoriality in Data Privacy Law* (Ex Tuto, 2013).
[37] EPIC and PI, *Privacy & Human Rights 2006* (10th Edn., EPIC and Privacy International, 2006).
[38] People's Republic of China; Hong Kong; India; Japan; Malaysia; Mongolia; the Philippines; Singapore; South Korea; Sri Lanka; Taiwan, Thailand.
[39] Rule and Greenleaf (Eds.), *Global Data Privacy Protection: The First Generation*.

networks, and so on—may give them a new urgency, but they have been with us in some form for decades if not longer. However, there are some technical and social developments—'big data' and data analytics are often suggested—which may pose genuinely new issues not previously confronted. These current issues are not the focus or structure of this book, but will arise in the discussion of particular countries.

### 4.4. Structure of this book

The book is structured into three Parts: Part I—Asia and international data privacy standards (chapters 1–3); Part II—National data privacy laws in Asia (chapters 4–16); and Part III—Regional comparisons, standards, and future developments (chapters 17–20).

Part I sets out the aspects of international law, agreements and politics relevant to Asian privacy laws, and the standards by which privacy laws can be assessed.

Part II examines data privacy laws in each of the 26 countries in Asia (briefly for the 12 currently without general data privacy laws), generally in a standard order. This analysis includes what evidence is available of the effectiveness and transparency of the enforcement of the laws. On the assumption that many readers will not be familiar with the relevant historical background, legal systems, or surveillance context for all 26 countries examined, brief background information and non-specialist references are provided for each country.

The analysis of national data privacy laws in each country chapter in Part II is based on the following outline, though it is not followed strictly in each chapter:

(1) *Contexts of data privacy*: historical and political context; surveillance context; attitudes to privacy; legal system; international obligations concerning privacy; constitutional and general law protections; other legislation.

(2) *Data privacy legislation*: key legislation; scope and exemptions; core concepts, and definitions.

(3) *Data privacy principles—obligations of data controllers*: general structure; purpose specification; collection; use and disclosure; data quality; data security (including data breach notification); 'openness'; data retention/deletion; other.

(4) *Principles—international data flows:* extraterritoriality; data exports; processor obligations (and privity); transfers in (outsourcing 'exemptions').

(5) *Principles—rights of data subjects*: notice; access; correction; erasure; blocking; other.

(6) *Principles—special concerns*: sensitive data; automated decisions; file interconnection ('data matching'); direct marketing; identity information; publicly accessible data ('public registers'); Internet.

(7) *Enforcement authorities:* Data Protection Authority (DPA) or ministry; structure and powers; independence.

(8) *Reactive enforcement*: types of investigations; DPA/ministry remedies (enforcement notices, administrative fines, publicity, etc.); rights of court action (compensation, other remedies); criminal offences; effectiveness; transparency.

(9) *Systemic enforcement*: codes; education; audits; registration; privacy impact assessments, etc.; effectiveness; transparency.

(10) *Self/co-regulation and Codes of Conduct*: self-regulation; seals and certifications, etc.; effectiveness.

(11) *Conclusions*: scope; relative strength and novel elements of standards; 'responsive regulation'; transparency; prospects.

Finally, Part III compares the data privacy laws across all the countries of Asia, measured against international standards as discussed in Chapter 3. It also draws conclusions about the overall trajectory of Asian privacy laws (particularly in light of impending international developments), and the extent to which their development sheds light on the questions raised by earlier studies.

## 5. Values and interests in Asian data privacy protection

This introduction concludes by considering some of the values and interests involved in data privacy protection, the parties holding those values and interests, and to what extent Asian countries may exhibit significant differences from Europe.

### 5.1. Human rights, fundamental rights, and 'Asian values'

Those studying the development of European data privacy law have not had to spend much time on equivalent arguments to the 'Asian values' debate, since data protection legislation has generally only been a feature of European countries subsequent to their democratic development, and the argument that privacy is inimical to 'European values' is not heard. Also, all countries that become members of the Council of Europe have to be parties to the ECHR, and therefore accept privacy as a value protected under Article 8.

It is clear at one level that privacy is a human right in Asia, as elsewhere. It is recognized as such in the Universal Declaration of Human Rights (UDHR), and the International Covenant on Civil and Political Rights (ICCPR). However, there is no Asian regional convention on human rights, although there is now an ASEAN Declaration. Privacy is recognized, either expressly or impliedly (as interpreted by court decisions) as a constitutional right (a fundamental right) in the constitutions of many Asian countries, but far from all of them (see Chapter 17). Where this occurs it is equivalent to privacy being recognized as a human right. As Davis notes,[40] the absence of a regional human rights agreement means that human rights developments in Asia have not been imported 'vertically' from a regional agreement according to regional transnational practice, but instead 'there has tended to be a process of horizontal or comparative importation of international human rights standards through domestic constitutional debates and interpretations'.

This is the point, says Davis, at which these debates have 'engaged concerns with Asian cultural values and economic development . . . the so-called "Asian values debate"'.[41] Although he focuses on constitutional issues, the same arguments could be raised concerning the introduction of data privacy legislation. He identifies three main streams of 'Asian values' claims and rejects each of them (concentrating on East Asia), with the aim of 'rebutting the claim that human rights and democracy are culturally unsuited to Asian soil'.[42] First, the claim that 'Asian values are illiberal and anti-democratic' is, in his view, rebutted by the fact that in recent decades formerly authoritarian countries have adopted liberal-democratic human rights regimes, in Japan, South Korea, Taiwan, the Philippines, and Indonesia. These include some of Asia's most economically successful countries. Second, claims that countries without various specific cultural prerequisites are not suitable for democracy or human rights, seem to be contradicted by the democratizations that have

[40] M.C. Davis, 'The Political Economy and Culture of Human Rights in East Asia' (2011) 1(1) *Jindal Journal of International Affairs*, pp. 48–72, at pp. 49–50.

[41] Davis, 'The Political Economy and Culture of Human Rights in East Asia', p. 50.

[42] Davis, 'The Political Economy and Culture of Human Rights in East Asia', p. 5.

occurred in countries that could not be said to have previously developed those features. Third, community-based arguments, whether of the romantic, 'civic virtue', or communitarian versions, are more difficult to rebut in their prioritization of the common good over liberal individual rights, but neither can they be asserted as fact.

Davis also identifies the 'East Asian authoritarian development model' argument as an 'Asian values' argument separate from the above cultural arguments, which he says has 'represented a powerful East Asian challenge to universal human rights'.[43] It is, as Davis explains, a rather shaky premise that the model of economic development success demonstrated by Japan, South Korea, Taiwan, Singapore, and (more recently) China and Vietnam, requires denial of international human rights standard. Japan was always a democracy and not a particularly authoritarian one, and since the early 1990s the adoption of democracy and human rights standards by Taiwan and South Korea has done no harm to their economic success. Whether China's continuing economic success depends on denial of human rights, or just the opposite, is a strongly contested issue.

Baik's study of the emergence of regional human rights mechanisms in Asia is also dismissive of the argument that 'human rights are incompatible with Asian society', pointing to humanist concepts as part of Asian cultures before the development of international law models, the adoption of the ICCPR, and the inclusion of human rights in constitutions and embrace of constitutionalism.[44] Privacy is a human right central to liberal ideology, and is therefore quite a good example against which to test 'Asian values' theories. The final chapter of this book will discuss whether the history of development of data privacy laws in Asia has been influenced by 'Asian values' arguments.

### *Attitudes to privacy in Asian countries*

Rejection of 'Asian values' arguments is not the same as arguing that privacy has the same meaning in all societies, and that local cultural values are irrelevant. There is a separate and sophisticated literature on the differences between the meanings of 'privacy', and the values underlying data privacy laws, in particular Asian countries compared with European and other western countries.[45] Ess suggests that it may be possible to generalize that 'China, Japan, Thailand—and other Asian countries and regions such as Hong Kong—defend privacy rights, at least initially, in terms of data privacy protection that is *instrumentally* necessary for the development of e-commerce'. He contrasts this with Western countries which, because there is a pluralistic continuum of privacy justifications, 'justify privacy as an *intrinsic* good, as well as one which is instrumentally needed for the sake of democratic polity'.[46] However, instrumental trade-related justifications have not been absent from the reasons for introducing data privacy laws in Western countries, and were central to the development of the OECD Guidelines (in the form of concerns over 'trans-border data flow' limitations), and the EU Data Protection Directive ('internal market' considerations). Local attitudes to and justifications for data privacy laws will be discussed in the chapters in Part II looking at particular countries where information is available, but this book is not a sociological study.

[43] Davis, 'The Political Economy and Culture of Human Rights in East Asia', p. 56.
[44] Baik, *Emerging Regional Human Rights Systems in Asia*, p. 296.
[45] See C. Ess, '"Lost in Translation"?: Intercultural Dialogues on Privacy and Information Ethics (Introduction to the special issue on Privacy and Data Privacy Protection in Asia)' (2005) 7 *Ethics and Information Technology*, pp. 1–6, and the articles on China, Japan, and Thailand in that issue.
[46] Ess, 'Lost in Translation?', p. 2. Emphasis in original.

### 5.2. Democracy's implications for data privacy in a half-democratic Asia

Democracy is one of the plurality of values that support data privacy laws. Bygrave summarizes that the safeguards protecting privacy 'help to prevent the accumulation of political, social and/or economic power within the hands of a small group of people . . . [and] . . . serve to secure the necessary conditions for active citizen participation in public life; in other words, they serve to secure democracy'.[47] As well as supporting negative liberties, privacy therefore supports positive liberties such as the freedom to participate in the political sphere, particularly by limiting the extent to which people are under surveillance by the state or others while they are so participating. Bygrave points out that privacy therefore underpins a Habermasian or Republican perspective on political theory.[48] This does of course assume that the scope of such laws includes the public sector, and while this is always so in Europe that is not the case in Asia (Singapore, Malaysia, and India have private-sector only laws). The 'watchdog' aspect of data privacy laws and institutions, particularly in relation to the state, are also a good fit for recent theories of 'monitory democracy'[49] with its emphasis on the development of a multitude of watchdogs monitoring the public sphere. Keane regards post-independence India as the exemplar of the development of monitory democracy, which he sees as the most significant advance in democratic practices since the development of representative democracy.[50] Although data privacy laws and institutions do not feature in his analysis, they fit it very well.

Globally, countries which have data privacy laws generally apply those laws to both their public and private sectors.[51] The significance of privacy laws to democracy is, of course, primarily found in the extent to which they act as a check on the state (i.e. the public sector) misusing personal information about its citizens, and in particular in it doing so in a way which interferes with democratic processes.

Those studying the development of European data privacy law do not have to put the relationship between democracy and privacy into the foreground of their thinking to any great extent,[52] because European states are almost all now democratic (with imperfections within the normal range).[53] The main tensions likely to arise are over whether the few European countries with very questionable democratic institutions can develop an effective system of data protection.[54] But in Asia the position is quite different, because only half of the 26 countries which this book examines are democratic. Adopting a modified version of the regime classification used by Case,[55] we can classify current Asian regimes into one of three categories, based on largely procedural notions of democracy:

[47] Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits*, p. 135.
[48] Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits*, p. 136.
[49] John Keane, *The Life and Death of Democracy* (Pocket Books, 2011).
[50] Keane, *The Life and Death of Democracy*, particularly Part III.
[51] Graham Greenleaf, 'Scheherezade and the 101 Data Privacy Laws'.
[52] This has not always been so: memories of misuse of personal information by fascist regimes were one of the drivers for data privacy law in western Europe; and the adoption of data privacy laws was part of the package of civil liberties reforms that characterized post-authoritarian eastern Europe.
[53] Countries that are demonstrably not democratic are refused admission to the Council of Europe, and they do not have data privacy laws (Belarus is the main remaining example), so the question does not arise.
[54] Russia is the most important example, but its law only came into force in 2011, so the answer is not yet known.
[55] William Case, *Politics in Southeast Asia: Democracy or Less* (Curzon, 2002).

- *Democratic regimes*[56]—India, Japan, South Korea, Taiwan, Indonesia, the Philippines, Timor Leste, Bangladesh, Sri Lanka, Nepal, Thailand (at present), and (despite a temporary regression) the Maldives.
- *Semi-democratic regimes*[57]—Singapore, Malaysia, Pakistan, Sri Lanka, Afghanistan, Bhutan, and (arguably) Cambodia; Hong Kong, and Macau.
- *Authoritarian regimes*[58] —Broader authoritarian category: People's Republic of China, Brunei, Vietnam, Lao PDR, and (for now) Myanmar. Hard authoritarian category: North Korea.

By this categorization, Asia currently includes 12 democracies, 9 semi-democratic regimes and 5 authoritarian regimes.[59] Given the population size and economic significance of many of the democratic countries, it seems a reasonable generalization to refer to the current state of Asia as 'half democratic', which is consistent with other assessments.[60] This makes Asia very different from Europe as a context for development of data privacy laws, as explained above. Of course, such categorizations are not permanent, and countries move between categories,[61] but while Asia may still only be semi-democratic (unlike Europe), since World War II the trend has been slowly moving towards democracy (like Europe). This categorization of Asian regimes by democracy also allows us to ask questions such as whether there are correlations between democratic regimes and the adoption of data privacy laws (or their effectiveness); and whether such laws can be effective in semi-democratic or authoritarian regimes in relation to either the public sector or private sector. These questions will be considered in the final chapters of this book.

[56] Case, *Politics in Southeast Asia*, p. 6. Democratic regimes, while usually falling short of an ideal notion of a democracy, are characterized by civil liberties including free speech, press, and assembly, so as to make citizen participation in politics meaningful, and regular multi-party elections that are substantially free and fair. I would add that these conditions must also have resulted in at least one change of government by election, including the coming to power of the current regime. If these conditions have not (yet) been fulfilled, a regime is at best a candidate to become a democratic regime, and is classified as still being 'semi-democratic'.

[57] Case, *Politics in Southeast Asia*, p. 6. Semi-democratic regimes are 'tinged with authoritarian residues' while having some elements of a democracy, and are characterized by regular multi-party elections, but with limited civil liberties beforehand, and opposition parties that are free to organize but are unfairly hindered in many ways from ever forming a government (methods include electoral mal-distribution, restrictions on assembly, and government hegemony over means of mass communication) while still being able to win some seats so as to hold the government 'mildly accountable'. Hong Kong and Macau SARs are not fully democratic regimes but their governments are more than 'mildly accountable' to their local populations (and there are constitutional goals of democracy), so they are also included here. Myanmar seems to be en route to this category.

[58] Case, *Politics in Southeast Asia*, pp. 8–9. Authoritarian regimes do not provide civil liberties sufficient for political involvement in free elections, nor do they have multi-party elections at the level of national government. This authoritarian category includes what Case classified as 'pseudo-democratic' regimes, where elections are held but they are a sham, and opposition parties have no autonomy. Case's 'hard authoritarianism' 'which offers no trace of civil liberties or elections' is now a category into which only North Korea would fit.

[59] But the boundaries are porous, circumstances change every month, and in another year the numbers will probably be different. The justifications for including each country in these categories can be found in the relevant country chapter.

[60] Categorizations of countries by such factors as 'democracy' are always contentious, but other categorizations also produce a similar 'half democratic' conclusion. The US-funded Freedom House categorization in 2011 resulted in a similar result for 23 states in Asia, although it did not consider Taiwan, Hong Kong, Macau, or Afghanistan. It found 5 free, 11 partly free, and 7 non-free states. The differences resulted from more pessimistic assessments of the Philippines, Timor Leste, Bangladesh, and Thailand than in the above categorization. Nevertheless, 'half free' (or 'half democratic') is still the overall result. See Baik, *Emerging Regional Human Rights Systems in Asia*, pp. 28–30.

[61] In Asia since World War II, the movement has been largely in the direction of democracy, from authoritarian regimes to semi-democratic regimes (perhaps Myanmar), and often all the way to democratic regimes (South Korea, Taiwan, the Philippines, Indonesia, Timor Leste). There has been movement in the other direction, often temporary (India during the Emergency, Bangladesh, Sri Lanka, Pakistan, and Thailand at various times).

### 5.3. Surveillance and other interests—'security', the state, and commerce

Surveillance is the other side of the coin from data privacy. Surveillance of individual behaviours has been an essential aspect of most institutions of the modern state at least since the French Revolution. Since the post-WWII rise of consumer credit facilities, surveillance has become an essential aspect of modern commerce, and more intensively since the post-1995 growth of consumer use of the Internet. Many of the mechanisms of personal surveillance were given early conceptual clarity by the unrelated but complementary studies of Rule's *Private Lives and Public Surveillance*[62] in 1973 and Foucault's *Discipline and Punish*[63] in 1975. Since the 1980s a whole discipline of 'surveillance studies' has grown up,[64] but what it has added to the insights of Rule and Foucault is beyond the scope of this book.

The relationship of data privacy laws to surveillance practices of both the state and commerce is both obvious and controversial. On the one hand, an ostensible purpose of data privacy laws is to ensure that forms of surveillance which are regarded as being in the public interest operate in a way which is fair to those who are under surveillance, and to make illegal other forms of surveillance which are not regarded as being in the public interest. On the other hand, critics of data privacy laws (and the data protection authorities that administer them) from Rule and Flaherty onwards, have claimed that the objective function of many laws and DPAs has been to legitimize data surveillance practices which otherwise had only very dubious public legitimacy (discussed in the final chapter). It follows that a comprehensive study of privacy protection in any particular country should examine the details of the surveillance practices of both the state and commerce in that country, and the extent to which the country's data privacy laws are capable of properly regulating those practices. Such a worthy aim is beyond the scope of this book, particularly given the number of countries involved. However, data privacy laws cannot be understood without at least a sketch of the surveillance context within which they operate, so this is provided in each country chapter.

### 5.4. 'Free flow' of personal data and conflicts with human rights

Attempts to find a balance between demands for 'free flow' of personal data in the interests of facilitating trade, and the desire of states and their citizens to have personal information protected to at least an agreed minimum standard no matter to where that data was transferred, have been at the heart of the development of data privacy laws and standards since the earliest years of their development. The terminology has changed from 'trans-border data flows' to 'data export limitations' to 'interoperability', but the significance of the international dimension has remained.

An additional complicating factor which has come more into focus in the past few years requires mention. Because of the Internet, an international imbalance has arisen between most countries in the world, whose citizens are subjects to (and the subjects of) the surveillance activities of companies overwhelmingly based in other countries, particularly,

[62] James Rule, *Private Lives and Public Surveillance* (Allen Lane, 1973).

[63] Michel Foucault, *Discipline and Punish: The Birth of the Prison* (Penguin 1977, transl. Sheridan, first published as *Surveiller et punir: Naissance de la prison*, Editions Gallimard, 1975).

[64] A major compendium is Kirsty Ball, Kevin Haggerty, and David Lyon (Eds.), *The Routledge Handbook of Surveillance Studies* (Routledge, London, 2012). See also David Lyon, *Surveillance Studies: An Overview* (Polity, 2007); for a collection of studies of national ID systems see Colin Bennett and David Lyon, *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective* (Routledge, 2008).

but not exclusively, in the USA. Data privacy laws have great difficulty in coping with this, as we will see. The same applies to the international operation of security agencies of some countries, once again particularly, but not exclusively, the USA. Fears of both private sector and state surveillance increase suspicions of international 'free flow of personal data' at the same time as it has become far more pervasive.

These international factors mean that that it is appropriate to address the international agreements and organizations affecting data privacy in Asia in the next chapter of this book.