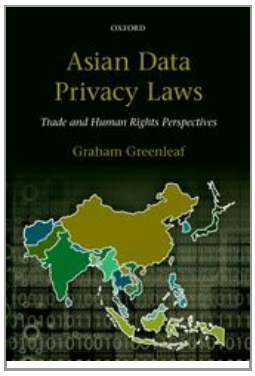
OXFORD

Asian Data Privacy Laws

Trade and Human Rights Perspectives

Graham Greenleaf



Asian Data Privacy Laws: Trade & Human Rights Perspectives

Graham Greenleaf

Print publication date: 2014
Print ISBN-13: 9780199679669
Published to Oxford Scholarship Online: December 2014
DOI: 10.1093/acprof:oso/9780199679669.001.0001

Title Pages

Asian Data Privacy Laws Asian Data Privacy Laws

OXFORD
UNIVERSITY PRESS

(p.iv) 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

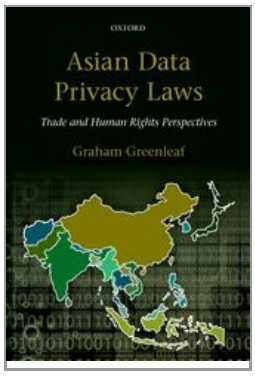
Library of Congress Control Number: 2014940428

ISBN 978–0–19–967966–9

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

Contents

Go to page:



Asian Data Privacy Laws: Trade & Human Rights Perspectives

Graham Greenleaf

Print publication date: 2014
Print ISBN-13: 9780199679669
Published to Oxford Scholarship Online: December 2014
DOI: 10.1093/acprof:oso/9780199679669.001.0001

(p.v) 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.

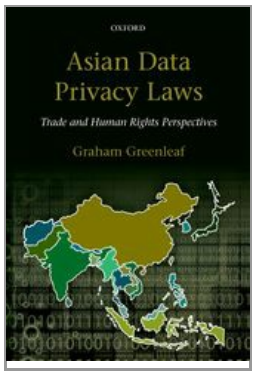
Asian Data Privacy Laws is the first ground-breaking work to examine data privacy laws and data protection authorities across Asia. There is no person more suitable than Professor Greenleaf, an eminent and erudite scholar, to undertake this work. He has done an outstanding job in illustrating the increasing 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



Asian Data Privacy Laws: Trade & Human Rights Perspectives
Graham Greenleaf

Print publication date: 2014
Print ISBN-13: 9780199679669
Published to Oxford Scholarship Online: December 2014
DOI: 10.1093/acprof:oso/9780199679669.001.0001

(p.vi) (p.vii) 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.

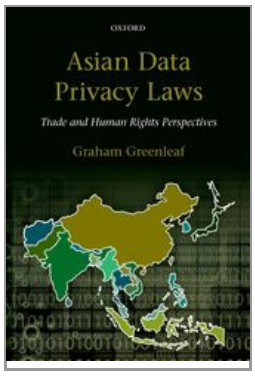
I have been involved in privacy administration, research, and advocacy almost continuously since the mid-1970s, although not full-time. I have kept an eye on privacy developments in Asia since the mid-1990s, and have had the opportunity to live in three countries in Asia, and to work in many others, 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



Asian Data Privacy Laws: Trade & Human Rights Perspectives
Graham Greenleaf

Print publication date: 2014
Print ISBN-13: 9780199679669
Published to Oxford Scholarship Online: December 2014
DOI: 10.1093/acprof:oso/9780199679669.001.0001

(p.viii) (p.ix) 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.

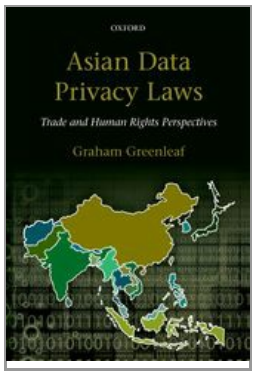
Valuable comments on various of the chapters in Parts I and III were made by Bob Gellman, Blair Stewart, Professor Charles Raab, Dr Roger Clarke; Professor Colin Bennett, Professor Dan Svantesson, Nigel Waters, and Chris Connolly. The publications of each of them, and those of Professor Jim Rule and 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 **(p.x)** & 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.

University Press Scholarship Online
Oxford Scholarship Online



Asian Data Privacy Laws: Trade & Human Rights Perspectives
Graham Greenleaf

Print publication date: 2014
Print ISBN-13: 9780199679669
Published to Oxford Scholarship Online: December 2014
DOI: 10.1093/acprof:oso/9780199679669.001.0001

(p.xv) Table of Cases

International

Europe

- Modinos v Cyprus (1993) 16 EHRR 485 42
- Társaság a Szabadságjogokért v Hungary (App No 37374/05), judgment of 14 April 2009 428

United Nations

- Toonen v Australia [1994] UNHRC 15; CCPR/C/50/D/488/1992 42

National

China

- Cao v Wang (2013), Shanghai Jing'an District People's Court 203
- China v Wang Zhengrong Shaoyang, Beita District People's Court, 26 October 2009 199

Hong Kong

India

Indonesia

Japan

Macau Special Administrative Region (SAR) of the People's Republic of China

Malaysia

Nepal

Pakistan

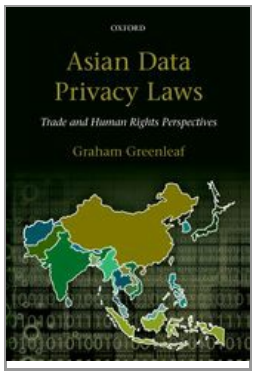
Singapore

South Korea

Taiwan

United Kingdom

University Press Scholarship Online
Oxford Scholarship Online



Asian Data Privacy Laws: Trade & Human Rights Perspectives
Graham Greenleaf

Print publication date: 2014
Print ISBN-13: 9780199679669
Published to Oxford Scholarship Online: December 2014
DOI: 10.1093/acprof:oso/9780199679669.001.0001

(p.xix) Table of Legislation

National Legislation

Afghanistan

- Constitution of Afghanistan 2004 466, 467, 472
  - Chap III 466
  - Art 58 467
- Draft Access to Information Law 467

Australia

- Privacy Act 1988 179, 241
  - s 98 111

Bangladesh

- Constitution 448

Hong Kong

Japan

Malaysia

- s 43 325
- s 43(5) 333
- s 44 333
- s 45 324
- s 45(1) 323
- s 45(2)(e) 323
- s 45(2)(f) 323
- s 46 324
- s 47 330
- s 48 331
- s 49 331
- s 53 330
- s 54 331
- s 57 331
- **(p.xxvii)** s 59 331
- s 60 331
- s 85 331
- s 87 331
- s 88 331
- s 93 331, 332
- s 94 331
- s 99 331
- ss 101–103 333
- s 108(1) 332
- s 108(3)(b) 332
- s 108(8) 332
- s 129 329, 330
- s 129(3)(f) 329
- s 130 326
- s 134 333
- s 135 333
- s 139 331
- s 144 324
- s 146 334

- Personal Data Protection Regulations 2013 318, 325, 326
  - s 3 325
  - s 3(1) 333
  - s 4 326
  - s 5 326
  - s 6 327, 333
  - s 7 327, 333
  - s 8 328, 333
  - ss 9–11 328
  - s 12 333

Nepal

Philippines

Singapore

- s 28 310
- s 29 310, 311, 312
- s 29 310
- s 31 311
- s 32 313
- s 32(1) 313
- s 32(2) 313
- s 32(3) 313
- s 33 311
- s 33(4) 311, 312
- s 34 311
- s 34(6) 312
- s 35 312
- s 35(2) 312
- s 35(4) 312
- s 49 309
- s 50 309
- s 50(3) 310
- s 50(3)(b) 310
- s 51 311
- s 52(1) 313
- s 52(3) 314
- s 52(4) 314
- s 52(5) 314
- s 53 313
- s 53(2) 314
- s 59 312
- s 62 296
- **(p.xxx)** Sch 1, para 3 309
- Sch 1, para 4 309
- Schs 2–4 298–9
- Sch 2, para 1(c) 294
- Sch 2, para 1(g) 297
- Sch 2, para 2 297
- Sch 3, para 1(c) 294
- Sch 4, para 1(d) 294
- Sch 5 300
- Sch 6 300
- Sch 7, para 1 311
- Sch 7, para 3(2) 311
- Sch 7, para 4 312
- Sch 7, para 4(8) 312
- Sch 9 309

- Personal Data Protection Commission, Advisory Guidelines on Key Concepts

Sweden

Taiwan

Thailand

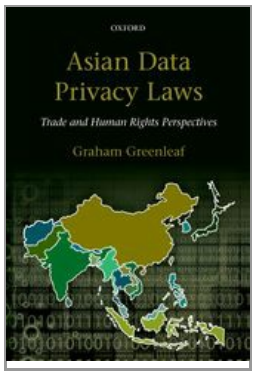
Timor Leste (East Timor)

European Legislation

Directives

Regulations

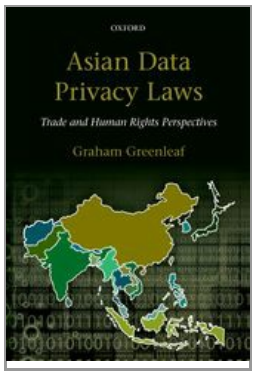
(p.xxxv) International Instruments



Asian Data Privacy Laws: Trade & Human Rights Perspectives
Graham Greenleaf

Print publication date: 2014
Print ISBN-13: 9780199679669
Published to Oxford Scholarship Online: December 2014
DOI: 10.1093/acprof:oso/9780199679669.001.0001

(p.xxxvii) List of Figures and Tables



Asian Data Privacy Laws: Trade & Human Rights Perspectives
Graham Greenleaf

Print publication date: 2014
Print ISBN-13: 9780199679669
Published to Oxford Scholarship Online: December 2014
DOI: 10.1093/acprof:oso/9780199679669.001.0001

(p.xxxviii) (p.xxxix) List of Abbreviations

- AA
  Accountability Agent
- AAB
  Administrative Appeals Board
- ADR
  alternative dispute resolution
- AEC
  ASEAN Economic Community
- AES Watch
  Automated Election System Watch
- AFAPDP
  Association of Francophone Data Protection Authorities
- AICHR
  ASEAN Intergovernmental Commission on Human Rights
- ALRC
  Australian Law Reform Commission
- AO

Adjudicating Officer

- APEC
  Asia-Pacific Economic Cooperation
- APF-NHRI
  Asia-Pacific Forum of National Human Rights Institutions
- APIPO
  Authorized personal information protection organization
- APPA
  Asia-Pacific Privacy Authorities
- ASEAN
  Association of Southeast Asian Nations
- BCR
  binding corporate rule
- BORO
  Bill of Rights Ordinance
- BPO
  Business processing outsourcing, or Business process outsourcing
- CAT
  Cyber Appellate Tribunal
- CBPR
  Cross-border Privacy Rules
- CBPRs
  Cross-border Privacy Rules system
- CCP
  Cambodian People's Party
- CCRI
  Citizens' Campaign for Right to Information
- CDRC
  Consumer Disputes Redressal Commission
- CIC
  Central Information Commission (India)
- CIC
  Classification of Information Committee (Nepal)
- CICRA
  Credit Information Companies (Regulation) Act 2005
- CNIC
  Computerized National Identity Card
- CoE
  Council of Europe
- COMELEC
  Commission on Elections
- CPBR
  Consumer Privacy Bill of Rights
- CPEA
  Cross-border Privacy Enforcement Arrangement

- CPPDPA
  Computer Processed Personal Data Protection Act 1995–2012
- CRA
  Credit reporting agencies
- CRAA
  Credit Reporting Agencies Act 2010
- CSTC
  China Software Evaluation and Test Center
- DBN
  Data breach notification
- DICT
  Department of Information and Communications Technology
- DMZ
  Demilitarized Zone
- DOJ
  Department of Justice
- DP Act
  Data Protection Act
- DP Mark
  Data Privacy Protection Mark
- DPA
  Data Protection Authority
- DPD
  Dewan Perwakilan Daerah (Regional Representatives Council)
- DPP
  Data protection principles
- DPP
  Democratic Progressive Party
- DPR
  Dewan Perwakilan Rakyat (House of Representatives)
- DPRK
  Democratic People's Republic of Korea
- DSCI
  Data Security Council of India
- DURS
  Data user returns scheme
- EC
  Election Commission
- ECHR
  European Convention on Human Rights
- ECJ
  European Court of Justice (also CJEU)
- **(p.xl)** ECOWAS
  Economic Community of West African States
- ECSG

Electronic Commerce Steering Group
- ECtHR
  European Court of Human Rights
- EFF
  Electronic Frontier Foundation
- ELSAM
  Institute for Policy Research and Advocacy
- ERP
  Electronic Road Pricing
- ESO
  Electronic system operator
- EU
  European Union
- FMS
  Federated Malay States
- FOI
  Freedom of information
- FRA
  Agency for Fundamental Rights, or Fundamental Rights Agency
- FSA
  Financial Services Agency
- FSC
  Financial Supervisory Commission
- GAO
  Government Accountability Office
- GATS
  General Agreement on Trade in Services
- GPCL
  General Principles of Civil Law
- GPEN
  Global Privacy Enforcement Network
- HKLII
  Hong Kong Legal Information Institute
- HKLRC
  Hong Kong Law Reform Commission
- HRC
  Human Rights Committee
- IC
  Information Commission
- IC
  Integrated circuit
- ICCP
  Information, Computer and Communications Policy
- ICCPR
  International Covenant on Civil and Political Rights

- ICDPPC
  International Conference of Data Protection and Privacy Commissioners
- ICESCR
  International Covenant on Economic, Social and Cultural Rights
- ICN Act
  Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.
- ICSP
  Information and communications service providers
- ICT Act
  Information and Communications Technology Act 2006
- ICT
  Information and communications technology
- ICTA
  Information and Communication Technology Agency
- IDT
  Information Disclosure Tribunal
- IISP
  Internet Information Service Provider
- IPCC
  Independent Police Complaints Commission
- IRR
  Implementing rules and regulations
- ISA
  Internal Security Act
- ISP
  Internet Service Provider
- IT Act
  Information Technology Act 2000
- IT Law
  2006 Law on Information Technology
- ITAA
  Information Technology (Amendment) Act 2008
- JCIC
  Joint Credit Information Center
- JIPDEC
  Japan Information Processing Development Cooperation
- JOP
  Joint Oversight Panel
- KCC
  Korea Communications Commission
- KCIA
  Korean Central Intelligence Agency
- KISA
  Korea Internet & Security Agency

- Komnas HAM
  Komisi National Hak Asasi Manusia (National Commission on Human Rights)
- KWP
  Korean Workers' Party
- LDP
  Liberal Democratic Party
- LTTE
  Liberation Tigers of Tamil Elam
- METI
  Ministry of Economy, Trade and Industry
- MIB
  Melayu Islam Beraja
- MIC
  Ministry of Internal Affairs and Communications
- MICT
  Ministry of Information and Communications Technology
- MIIT
  Ministry of Industry and Information Technology
- **(p.xli)** MKSS
  Mazdoor Kisan Shakti Sanghatan
- MoIC
  Ministry of Information and Communication
- MoIT
  Ministry of Industry and Trade
- MOJ
  Ministry of Justice
- MOSPA
  Ministry of Security and Public Administration
- MSAR
  Macau SAR
- NADRA
  National Database & Registration Authority
- NCACJ
  National Consumer Affairs Centre of Japan
- NCDRC
  National Consumer Disputes Redressal Commission
- NEIS
  National Education Information System
- NGO
  non-governmental organization
- NHRC
  National Human Rights Commission
- NIA
  National Information Society Agency
- NIC

National Information Commission
- NICT
  National Information Technology Committee
- NIN
  National Identification Number
- NLD
  National League for Democracy
- NPC
  National People's Congress (China)
- NPC
  National Privacy Commission (Philippines)
- NPR
  National Population Register
- NRIC
  National Registration Identity Card
- NTU
  National Teachers' Union
- OECD
  Organisation for Economic Co-operation and Development
- OIB
  Official Information Board
- OIC
  Official Information Commission
- OPDP
  Office for Personal Data Protection
- PAP
  People's Action Party
- PCPD
  Privacy Commissioner for Personal Data
- PDPA
  Personal Data Protection Act
- PDPC
  Personal Data Protection Commission
- PDPO
  Personal Data (Privacy) Ordinance
- PDR
  People's Democratic Republic
- PE
  privacy enforcement
- PEA
  Privacy Enforcement Authorities
- PET
  Privacy-enhancing technologies
- PI
  Privacy International

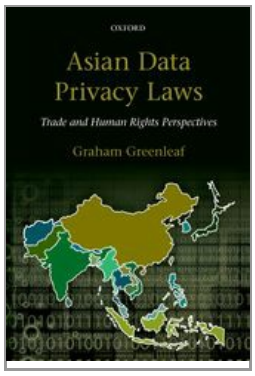
- PIA
  Privacy impact assessments
- PIDMC
  Personal Information Dispute Mediation Committee
- PIPA
  Personal Information Protection Act
- PIPC
  Personal Information Protection Commission
- PIPL
  Personal Information Protection Level Certification Management System
- PKI
  Communist Party of Indonesia
- PMIO
  Privacy Mark Issuing Organisations
- PPC
  Pakistan Penal Code
- PPIA
  Act on the Protection of Personal Information 2003
- PPIHAO
  Protection of Personal Information Held by Administrative Organs
- PPIHAOA
  Act on the Protection of Personal Information Held by Administrative Organs
- PPIHIAAA
  Protection of Personal Information Held by Incorporated Administrative Agencies
- PPS
  Privacy policy statement
- PRC
  People’s Republic of China
- PTA
  Pakistan Telecommunication Authority
- RBI
  Reserve Bank of India
- ROC
  Republic of China
- RPD
  Registration of Persons Department
- **(p.xlii)** RR
  Resident registration
- RTI
  Right to information
- SAARC
  South Asian Association for Regional Cooperation
- SAFTA
  South Asian Free Trade Area

- SAIC
  State Administration of Industry and Commerce
- SAR
  Special Administrative Region
- SBY
  Susilo Bambang Yudoyono
- SCC
  standard contractual clause
- SNS
  Social network service
- SOC
  State of Cambodia
- SPC
  Supreme People's Court
- SPIPC
  Specific Personal Information Protection Commission
- TBO
  Telecommunications business operators
- TDF
  Transborder data flows
- TLL
  Tort Liability Law
- TOS
  Terms of service
- TPIPAS
  Taiwan Personal Information Protection and Administration System
- UDHR
  Universal Declaration of Human Rights
- USDP
  Union Solidarity and Development Party
- UID
  Unique Identification Number
- UIDAI
  Unique Identification Authority of India
- UMID
  Unified Multi-Purpose ID
- UMNO
  United Malays National Organisation
- UN
  United Nations
- UNCTAD
  United Nations Conference on Trade and Development
- UNHCHR
  UN High Commissioner for Human Rights
- UNHRC

UN Human Rights Committee

- UNTAC
  United Nations Transitional Authority in Cambodia
- UNTAET
  United Nations Transitional Administration in East Timor
- WIPO
  World Intellectual Property Organization
- WPISP
  Working Party on Information Security and Privacy
- WTO
  World Trade Organization
- YHHK
  Yahoo! Hong Kong

University Press Scholarship Online
Oxford Scholarship Online



Asian Data Privacy Laws: Trade & Human Rights Perspectives

Graham Greenleaf

Print publication date: 2014
Print ISBN-13: 9780199679669
Published to Oxford Scholarship Online: December 2014
DOI: 10.1093/acprof:oso/9780199679669.001.0001

Data Privacy Laws in Asia—Context and History

Graham Greenleaf

DOI:10.1093/acprof:oso/9780199679669.003.0001

[–] Abstract and Keywords

This chapter situates the development of data privacy laws in Asia in the global history of this form of regulation. It explains what ‘data privacy laws’ are, their global expansion since the 1970s to over 100 countries, and how they differ from other forms of protection of privacy. It explains the focus on ‘Asia’, seen as the three sub-regions of Northeast Asia, Southeast Asia (ASEAN), and South Asia (SAARC). It outlines the 25-year history of data privacy laws in Asia, and asks whether they are ‘legal transplants’. The ‘bottom up’ approach that must be taken in Asia is compared with the ‘top down’ approach which is appropriate in the European Union, and the resulting structure of the book and each chapter is explained. The chapter concludes by discussing the values and interests involved in data protection in Asia, particularly given that Asia is only ‘half-democratic’.

Keywords: data protection, privacy, Asia, democracy, human rights, trade

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. **(p.4)** 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.

(p.5) • 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, **(p.6)** 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 **(p.7)** 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 **(p.8)** (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. **(p.9)**

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 **(p.10)** 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 **(p.11)** 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 **(p.12)** 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 **(p.13)** 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.

(p.14) 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 **(p.15)** 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 **(p.16)** 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.

(p.17) 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 **(p.18)** 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.

(p.19) 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:

> **(p.20)** • *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.

(p.21) 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, **(p.22)** 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.

Notes:

([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.

([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>.

([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).

([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/>.

([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.

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

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

([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.*).

([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.

([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.

([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*.

([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.

([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.

([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).

([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.

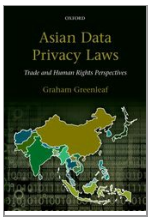
([61]) In Asia since World War II, the movement has been largely in the direction of democracy, from authoritarian regimes to semi-democratic regimes (perhaps Myanmar), and often all the way to democratic regimes (South Korea, Taiwan, the Philippines, Indonesia, Timor Leste). There has been movement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

([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).

University Press Scholarship Online
Oxford Scholarship Online



Asian Data Privacy Laws: Trade & Human Rights Perspectives
Graham Greenleaf

Print publication date: 2014
Print ISBN-13: 9780199679669
Published to Oxford Scholarship Online: December 2014
DOI: 10.1093/acprof:oso/9780199679669.001.0001

International Structures Affecting Data Privacy in Asia

Graham Greenleaf

DOI:10.1093/acprof:oso/9780199679669.003.0002

[–] Abstract and Keywords

This chapter considers all of the international standards, instruments, and institutions affecting data privacy in Asia. There are no Asia-wide instruments or institutions comparable to those central to privacy protection in the European Union. At the sub-regional level there is only one ASEAN (South-East Asia) declaration. The Organisation for Economic Co-operation and Development (OECD)'s privacy Guidelines of 1981 have been influential at the national level in Asia, as has the EU's data protection Directive of 1995, and the Asia-Pacific Economic Cooperation (APEC)'s Privacy Framework of 2004. The protection of privacy in general human rights treaties in Asia mainly stems from the International Covenant on Civil and Political Rights 1966 (ICCPR). The chapter also considers the effect of trade agreements such as the General Agreement on Trade in Services (GATS), and the International Organization for Standardization (ISO), and other technical standards. Finally, it considers the role played by global and regional associations of privacy-related authorities, and interest groups.

Keywords: data protection, privacy, Asia, OECD, European Union, ICCPR, human rights, GATS, ISO

1. Purpose of this chapter

There are no pan-Asian instruments or institutions which determine the structure of data privacy laws in individual Asian jurisdictions in ways

comparable to what occurs in Europe (as discussed in Chapter 1). Nor are there any relevant global instruments and institutions which can play a similar role. There is no global organization 'governing' data privacy equivalent to, say, ICANN in the field of domain names and numbers, nor as yet any global treaties equivalent to the Berne Convention in relation to copyright.

This chapter therefore aims to explain a wide range of international instruments and institutions, both global and sub-regional, which influence the content of data privacy laws in individual Asian jurisdictions. They are considered in this order: sub-regional **(p.24)** intergovernment institutions; international data privacy instruments relevant to Asia; international human rights instruments relevant to Asia; other international instruments (trade agreements, technical standards, etc.); and privacy-related authorities and interest groups. This chapter focuses on current influences, leaving new international developments, and their potential future impact for consideration to Chapter 19.

2. Sub-regional intergovernmental institutions and privacy engagements

As explained in Chapter 1, the 'Asia' of this study involves three sub-regions comprising 26 jurisdictions: Southeast Asia (the 10 members plus one candidate member of ASEAN); South Asia (the eight members of SAARC); and Northeast Asia (seven jurisdictions with no equivalent sub-regional institution to ASEAN or SAARC).

2.1. ASEAN and the Southeast Asian sub-region

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). Timor Leste applied in 2011 to be the eleventh member. Papua New Guinea has had observer status since 1976, but has not applied for membership. ASEAN was established in 1967 by five countries (Indonesia, Malaysia, the Philippines, Singapore, and Thailand), originally with an anticommunist orientation during the wars in Vietnam, Laos, and Cambodia. ASEAN's significance has been described as 'transformed from a periodic meeting of ministers to become the most important regional organisation in Asia's history'.[1] Its 10 member countries have a combined population of approximately 600 million (nearly 9 per cent of the world population), and a GDP of around US$2 trillion, which if it was a single entity would make it the world's eighth largest economy.[2] The ASEAN region is one of the largest and most integrated regions outside Europe.

The ASEAN Charter (2007)[3] is a constitutional document governing relations among the ASEAN members and establishing ASEAN itself as an international legal entity, and is part of a transformation of ASEAN from a body based on consultation and consensus toward 'a community governed by law'.[4] It establishes a regional Secretariat and national Secretariats, and adoption of principles including consensual decision-making, peaceful settlement of disputes,[5] the rule of law, and others that must be given a liberal interpretation (primarily 'adherence to…the principles of democracy'). ASEAN membership is limited to countries in Southeast Asia, requires adherence to the ASEAN Charter, compliance with the free trade agreement within ASEAN, and capacity to provide an embassy in each member state and attend all necessary meetings.

(p.25) ASEAN Intergovernmental Commission on Human Rights

ASEAN has always been trade-oriented and 'reluctant to take part in the field of human rights cooperation'[6] with a professed reluctance to interfere in the internal affairs of member countries. Its interest in human rights has been slowly growing, commencing with a declaration of ASEAN Foreign Ministers in 1993 concerning non-toleration of interferences with basic human rights, and that a regional human rights organization should be considered. This was reiterated in 2007 by the Eminent Persons Group set up to advise on the ASEAN Charter.[7] The Charter includes as an objective 'to promote and protect human rights and fundamental freedoms' but qualified 'with due regard to the rights and responsibilities of the Member States of ASEAN', and that, in conformity with this, ASEAN would 'establish a human rights body'.[8]

The 'human rights body' was established in the form of the ASEAN Intergovernmental Commission on Human Rights (AICHR)[9] in 2009. According to its Terms of Reference[10] it is a 'consultative body', 'an inter-governmental body', and 'an integral part of the ASEAN organizational structure'. It comprises one member from each ASEAN member state, 'accountable to the appointing government', and having (in default) a three-year term with one possible term of reappointment, but able to be replaced by the appointing government at any time and without need for any reason. Decision-making is to be based on 'consultation and consensus in accordance with Article 20 of the ASEAN Charter'. AICHR has many functions, some of which are positive in relation to human rights, although this apparent generosity may be because these functions are not backed up with any powers. These include the development of an ASEAN Human Rights Declaration (discussed below), encouraging ASEAN member states to consider acceding to and ratifying international human rights instruments, and performing any tasks assigned to them by the ASEAN Foreign Ministers Meeting.[11] AICHR is therefore not independent of governments, and would not constitute a human rights body according to the Paris Principles.[12] It does not have any stated functions in relation to human rights protections within member states of ASEAN. It does not have any capacity to receive and investigate complaints.

Although Baik considers it is 'still too early to judge the usefulness of the AICHR',[13] others have been more critical. An Asian regional civil society organization, the Asian Forum for Human Rights and Development ('Forum-Asia') has published annual reports on AICHR's performance. In its report on AICHR in 2011–12, the best it could say was that AICHR had taken 'limited steps in the direction of transparency and consultation with civil society', mainly in respect of the ASEAN Human Rights Declaration.[14] It considers, correctly, that the current approach gives each country veto power.

(p.26) ASEAN Human Rights Declaration (2012)

In 2012 the ASEAN heads of state adopted the ASEAN Human Rights Declaration,[15] article 21 of which states: 'Every person has the right to be free from arbitrary interference with his or her privacy, family, home or correspondence including personal data, or to attacks upon that person's honour and reputation. Every person has the right to the protection of the law against such interference or attacks.' Although based on the terminology of the Universal Declaration of Human Rights, the specific references to 'personal data' and the right to legal protection increase the internal incentives to all ASEAN members to enact data privacy laws.

However, the Declaration has come under savage criticism and outright rejection[16] from a coalition of 55 global and regional human rights organizations.[17] The United Nations (UN) High Commissioner for Human Rights considered that the Declaration 'retains language that is not consistent with international standards'.[18] These criticisms do not relate directly to article 21. However, it is clear that both the AICHR and the Declaration have not yet established credibility. It is difficult to agree with Baik's conclusion that '[w]ith the AICHR, ASEAN is already functioning as an important foundation for human rights cooperation'.[19] At best, it is possible to conclude that ASEAN has very recently recognized that it needs to address human rights by adoption of both principles and instruments, but that the value of its initial steps have not yet been demonstrated.

ASEAN data privacy commitments

In 2012–13 ASEAN became one of the most active regions of the world for data privacy developments, with data privacy laws in three countries (the Philippines, Malaysia, and Singapore), and more limited laws in three others (Vietnam, Indonesia, and Thailand). To what extent this has been influenced by ASEAN developments is unclear. However, ASEAN countries a decade ago made a commitment to 'adopt electronic commerce regulatory and legislative frameworks', including to 'take measures to promote personal data protection and consumer privacy'.[20] A 2010 study of e-commerce development across all ASEAN countries resulted in two recommendations (out of eight) relevant to, but not directly about, privacy protection.[21] ASEAN member countries have made a **(p.27)** commitment to develop 'best practices / guidelines' on data protection by 2015, as part of their commitment to establish an integrated ASEAN Economic Community (AEC) by 2015. Although this falls short of a commitment to legislate on data protection, it is possible that the ASEAN commitments are one of the influences on the recent developments in ASEAN. As Connolly notes, ASEAN 'does have a history of the successful harmonisation of laws—something that is absent in APEC'.[22]

ASEAN trade agreements and privacy

The ASEAN Framework Agreement on Services (1995) provides in effect[23] that the exemption for laws protecting data privacy in article XIV(c)(2) of the GATS (see section 5.1 of this chapter), applies under the ASEAN Framework, in default of specific provisions. There is, therefore, no impediment to data export restrictions resulting from ASEAN agreements.

2.2. SAARC and the South Asian sub-region

The South Asian Association for Regional Cooperation (SAARC) comprises eight member states (Afghanistan, Bangladesh, Bhutan, India, the Maldives, Nepal, Pakistan, and Sri Lanka).[24] These countries (minus Afghanistan) formed the Charter of the SAARC in 1985. It has an annual summit, and a council of ministers meets twice-yearly.[25] The emphasis of SAARC is clearly on economic matters, such as the SAARC Agreement on South Asian Free Trade Area (SAFTA)[26] in force since 2006 but of little relevance to data privacy as it deals primarily with trade in goods.

SAARC trade agreements and privacy

The only reference to privacy protection in the SAARC agreements and conventions is in the SAARC Agreement on Trade in Services,[27] made in 2010. That agreement allows for exceptions to be made in the domestic laws of SAARC countries for measures for the protection of data privacy which might otherwise be contrary to its free trade requirements. Clause 23 is in all relevant respects the same as article XIV(c)(2) of the GATS (see section 5.1 of this chapter), except that it only applies as between the SAARC countries. While this is essentially a negative measure, it is an important one, allowing SAARC member states to impose restrictions on data exports, and on outsourced data processing to other SAARC member states, in order to protect data privacy.

(p.28) SAARC and human rights

There are as yet no positive commitments to the protection of human rights generally, or privacy specifically, in the SAARC agreements, beyond some very general recitals.[28] Nevertheless, Baik sees some evidence in recent SAARC summits of interest in some human rights issues, particularly those concerning women and children, and that it is 'making more effort to include human rights in its regional discussions and cooperation'.[29] It seems more realistic to say that, after nearly 30 years of existence, SAARC still has only shown minimal interest in these issues. Regional agreements are therefore unlikely to be a factor in influencing data privacy laws in SAARC countries in the short term. However, in the long run the further development of SAARC as a regional body, and other developments may put data protection on the regional agenda.

2.3. The Northeast Asian sub-region and its institutional weakness

Northeast Asia comprises China (People's Republic of China or PRC), Hong Kong, Japan, Macau, North Korea, South Korea, and Taiwan (Republic of China). There is no regional agreement in Northeast Asia equivalent to SAARC or ASEAN involving all or most of these seven jurisdictions.[30] 'Northeast Asian states have been largely divided and separated from each other due to historical and political animosity that exists between them.'[31] However, they have important shared cultural characteristics including Confucian and Buddhist influences, and historical influences such as the? Chinese language and script. All except Hong Kong have modern legal histories in which the civil law played a major role, but these influences have taken different forms, particularly since the mid-twentieth century. There has been much discussion of the formation of an 'East Asian Community', usually proposed to include ASEAN members as well as the jurisdictions of Northeast Asia, but these have not yet amounted to any concrete steps.[32] There are many other competing models for regional and broader cooperation which include a number of Northeast Asian states, but none are emerging clearly.[33] Similarly, no proposals for a sub-regional human rights agreement or body have commanded significant attention. There is therefore as yet no sub-regional agreement from which data privacy standards are likely to emerge.

All of the Northeast Asian jurisdictions except North Korea have enacted significant data privacy laws. South Korea, Japan, Taiwan, Hong Kong, and Macau have comprehensive laws. China has a number of significant laws but no overall private sector law. The broader grouping in which most of the East Asian economies are members is APEC but, as discussed in part 3.3 following, and in Chapter 3, APEC's Privacy Framework and CBPR scheme have as yet had little impact on these jurisdictions. Nevertheless, APEC's data privacy subgroup and the Asia-Pacific Privacy Authorities (APPA) are the fora most likely to involve data privacy discussions with multiple participants from this sub-region. **(p.29)**

3. International data privacy instruments relevant to Asia

There is no Asian or sub-regional agreement dealing specifically with data privacy. The agreement which has the greatest number of members among Asian countries is the APEC Privacy Framework, of which 13 of the 21 members are Asian economies. However, of greater influence in the development of Asian data privacy laws have been the OECD privacy Guidelines and the European Union (EU) Data Protection Directive. The nature and structure of these and other international data privacy instruments relevant to Asia are discussed in this section. The discussion of their content continues in the next chapter, dealing with standards for comparing data privacy laws.

3.1. The OECD Guidelines (1980)

The Organisation for Economic Co-operation and Development (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[34] (the 'OECD Guidelines') were one of the first formulations of a comprehensive set of information privacy principles, and continue to be influential, particularly outside Europe. The OECD is an intergovernmental organization with 34 member countries[35] and plans for enlargement.[36] All OECD members other than Turkey and the USA (in relation to the private sector), now have data privacy laws implementing the Guidelines. The OECD Guidelines were revised in 2013 (see further Chapter 19), but it is the 1980 version of the Guidelines that has been influential to date and which is discussed here. Japan and South Korea are the only Asian countries that are members of the OECD (though China, India, and Indonesia have been offered 'enhanced engagement'), so the influence of the Guidelines in Asia is not primarily in terms of the number of countries that formally adhere to them. It is rather their influence as a standard that non-member countries aspire to; the fact that all of the OECD principles are included in the EU's Data Protection Directive; and their substantial influence on the APEC Privacy Framework.

Form and content of the OECD's 1980 Guidelines

The Guidelines are in the form of a Recommendation by the Council of the OECD, adopted in 1980. Unlike Decisions, Recommendations of the Council are not legally binding on member states. The Guidelines are proposed as minimum standards for the protection of privacy and individual liberties. They attempt to balance two 'essential basic values': the protection of privacy and individual liberties and the advancement of free flows of personal data.[37] They apply to both the public and private sectors. They have **(p.30)** been criticized as an inadequate standard,[38] including by the chair of the committee that drafted them.[39]

The core of the Guidelines are the eight 'basic principles of national application' in Part Two (principles 7–14). These are principles concerning collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. The Guidelines contain four 'basic principles of international application' concerning the free flow of personal data, and legitimate restrictions on such data exports (principles 15–18). The main thrust of these four principles is that member countries should avoid restrictions on the free flow of personal data among themselves, coupled with the recognition that restrictions on data exports can be legitimate, as set out in three exceptions in Guideline 17, the first of which is where the other member country 'does not yet substantially observe these Guidelines'. The implementation requirements of the OECD Guidelines are minimal. Principle 19 states the methods of implementation required for compliance with the Guidelines, but they only amount to encouragement to member states to adopt whatever mix of legislation and self-regulation they consider appropriate, provided that they deliver 'reasonable means for individuals to exercise their rights', 'adequate sanctions and remedies' and 'no unfair discrimination against data subjects'. All of these principles 7–19 are discussed in Chapter 3.

The 2013 revised OECD Guidelines

In 2013 the revision of the OECD Guidelines was completed. The Principles of National Application remain unchanged, but many other aspects of the Guidelines are changed very substantially. Although only Japan and South Korea are OECD members, the revised Guidelines are also aimed at non-members. It remains to be seen what effect they will have in Asia. Discussion of the 2013 Guidelines is therefore deferred until Chapter 19.

3.2. The EU Data Protection Directive (1995)—standards and 'adequacy'

The European Union, which had tended to leave human rights issues to the Council of Europe, became involved in data privacy in the early 1990s, and by 1995 adopted the general data protection Directive 95/46/EC (the 'EU Directive').[40] Many accounts of the Directive are available, ranging from the comprehensive[41] to a succinct account which describes its text as 'nebulous, dense and somewhat ambivalent'.[42] The Directive gave EU member states until October 1998 to bring their legislation and other measures into compliance with it. The content of the Directive's principles go considerably beyond **(p.31)** those required by the OECD Guidelines.[43] In its enforcement mechanisms it requires an independent data protection authority (DPA), and access to the courts, both additions to the OECD requirements. The principles and enforcement are discussed in Chapter 3.

The adequacy mechanism

Article 29 of the EU Directive creates a 'Working Party on the Protection of Individuals with regard to the Processing of Personal Data' (the 'Article 29 Working Party') comprised primarily of the representatives of each EU member state's DPA. It has various responsibilities under the Directive and, as the collective voice of the EU's DPAs, its many opinions[44] carry very significant international weight on all issues that it examines. It also plays a role in the EU Directive's most original and controversial feature, 'adequacy assessments'.

The EU Directive was the first[45] international instrument to control exports of personal data to countries not bound by the same data privacy rules (in this case, non-EU/EEA countries). Article 25 permits such exports from EU member states 'only if…the third country in question ensures an adequate level of protection'. 'Adequate' does not mean 'equivalent', but what it does mean remains somewhat elusive,[46] and has its most authoritative explication in two Opinions by the Article 29 Working Party (discussed further in Chapter 3).[47] The normal procedure is that the EU Commission obtains an 'expert report' from a consultant on the protection provided by the country in question, discusses it with representatives of that country, and if it considers that a positive decision on adequacy is possible, forwards the matter to the Article 29 Working Party for its Opinion (which is made public). After that the matter is considered by the Article 31 Committee of state parties and the European parliament.[48]

As yet, the EU has only made positive 'adequacy' assessments in relation to 11 jurisdictions as a whole, a minority of which are of economic or political significance.[49] An unknown number (but not a very large one) have received negative assessments, but the list of countries has not been formally disclosed. No Asian country has as yet received a positive adequacy assessment from the EU and, even among APEC members, only Canada and New Zealand have received positive assessments. India is known to have been assessed at least twice (in 2010 and 2013), but no recommendation of adequacy has gone forward from the EU Commission to the Article 29 Working Party. Australia is also known to have **(p.32)** been assessed twice, with the same result. The tardiness with which the EU has applied the adequacy principles—after nearly 20 years their application is only known definitively in regard to a handful of countries—has not improved their reputation.

Where no positive adequacy finding exists, transfers may still be made if they come within the exceptions set out in Article 26 of the Directive,[50] or where standard contract clauses or binding corporate rules are applicable (discussed below).

Significance of the Directive to Asia

The significance of the EU Directive to Asian countries is therefore: (i) it embodies the 'European standards' for data privacy which have been and continue to be very influential in the development of national data privacy laws in Asia and elsewhere outside Europe, because of the aspiration of countries to adopt what is perceived as international 'best practice'; (ii) some Asian countries want to obtain an 'adequacy assessment' for trade reasons; and (iii) it is developing a 'third generation' of data privacy principles in the course of moving from a Directive to a Regulation. The first of these matters is discussed further in Chapter 3, and the third in Chapter 19.

Use of standard contractual clauses and binding corporate rules in EU-originated outsourcing to Asia

From the perspective of companies based in the EU that are outsourcing personal data processing to Asian countries, the controller-to-processor contract model clauses ('standard contractual clauses' or SCCs) developed by the European Commission under article 26(4) of the EU Directive are of particular relevance.[51] The 2010 version of the SCCs[52] contain provisions which aim to benefit data subjects. These include that the clauses should be governed by the law of the member state in which the data exporter is established.[53] Assuming that the laws of all EU member states recognize the rights of third party beneficiaries to contracts, this means that in all controller-to-processor contracts between European and Indian companies utilizing the clauses, data subjects can enforce relevant contract terms in the courts of the European country.

The SCCs go on to provide that the data subject (i) can enforce against the data exporter, as a third party beneficiary, numerous of the clauses and sub-clauses; (ii) can enforce other clauses against the data importer, but only where the data exporter has 'factually disappeared'; and (iii) can enforce certain clauses against the subcontractor, but only where both data exporter and data importer have 'factually disappeared'; and have no objection to data subjects being represented by an association or other body.[54] The provisions in the data privacy laws of some Asian countries that allow data exports on the basis of contractual guarantees do not require the types of protections that the SCCs require.

(p.33) The result seems to be that, if the SCC are utilized, and the law of the controller-to-processor contract is the law of the European country, then data subjects will be able to legally enforce rights expressed to be in their favour in either the courts of the European country concerned, or in the court of an Asian country enforcing the law of the European country as a matter of private international law. But if the law of the contract is a country with the strict doctrine of privity of contract (such as India), it is unlikely that data subjects can enforce rights expressed to be in their favour. It is beyond the scope of this chapter to review the efficacy of the EU's SCCs and whether the rights expressed to be in favour of data subjects are broad enough, or to consider the analogous questions raised by intracompany binding corporate rules (BCRs).[55]

3.3. APEC's Privacy Framework (2004)

In November 2004 Ministers of APEC (the Asia-Pacific Economic Cooperation) economies, meeting in Santiago, Chile, adopted the APEC Privacy Framework, which had been developed during 2003–04 by APEC's Electronic Commerce Steering Group (ECSG) data privacy subgroup. The fact that 21 APEC economies[56] made a commitment to adopt common information privacy standards is significant. This was the first international commitment to detailed data privacy standards made by any of the Asian APEC members, other than Japan and South Korea which are already OECD members. The APEC economies are located on four continents, account for more than a third of the world's population, half its GDP, and almost half of world trade. It is still possible that APEC may expand beyond 21 members but, unlike the EU, its membership currently seems frozen. Numerous countries have been trying to join for some time, without success.[57]

APEC as an organization and the status of APEC 'agreements'

APEC is unusual in being an organization of states which does not have a constitution or a treaty to establish it (unlike ASEAN), operates by consensus, and undertakes commitments on a voluntary basis. It claims to be 'the only inter governmental grouping in the world operating on the basis of non-binding commitments'.[58] APEC 'agreements' such as the Privacy Framework do not have any legal status, and are best seen as agreed aspirations, supported by consensus-based commitments to cooperate. Nevertheless, their practical effect is often very significant. This structure limits to some extent what can be expected from the APEC Privacy Framework.

(p.34) The APEC Framework—limitations of its principles

The APEC Privacy Framework[59] of 2004 (although not finalized until 2005)[60] includes a set of nine 'APEC Privacy Principles'[61] and a Commentary, analysed in a history of the Framework to 2010.[62] The main differences between the principles in the APEC Privacy Framework and earlier international standards are found in a number of definitions and in three additional principles, next discussed. Apart from these differences, the APEC Privacy Framework of 2004 is largely the same as the Principles of National Application in the 1980 OECD Guidelines, except for very minor variations.[63] However, it does not contain any of the additional and stronger principles contained in the EU Data Protection Directive of 1995,[64] not even a requirement for deletion of personal data when its uses are completed. Even in 2004 the existing data privacy laws in APEC member economies[65] included many principles which went beyond those in the APEC Framework.[66] In summary, the principles in APEC's Privacy Framework are at best an approximation of what were regarded as acceptable information privacy principles in 1980 when the OECD Guidelines were adopted, though in some respects they are weaker. Its principles are not as strong as those of the European Privacy Directive, or (as will be seen in Part II), of most existing data protection laws in the Asia-Pacific.

'*Preventing Harm*' *(APEC principle I)* is based on the argument that privacy remedies should concentrate on preventing harm ('should be designed to prevent the misuse of such information' and should be 'proportionate to the likelihood and severity of the harm threatened'). This might appear unexceptional in sentiment but it conceals many dangers. It is anomalous to elevate it to a privacy principle because it neither creates rights in individuals nor imposes obligations on information controllers. To treat it on a par with other principles makes it easier to (i) allow any collection and use of personal data unless it is shown in individual cases to result in harm; (ii) justify exempting whole sectors as not sufficiently dangerous (e.g. 'small business' in the laws of Australia or Japan); (iii) justify providing piecemeal remedies only in 'dangerous' sectors (as in the USA); or (iv) restricting **(p.35)** 'harm' to pecuniary losses, excluding distress, humiliation etc.[67] This 'principle' would make better sense in Part IV on implementation, as a means of rationing remedies, or lowering compliance burdens. As a separate principle, a 'harm-based' approach is the antithesis of the EU Directive and not consistent with the OECD Guidelines.

'*Choice*' *(APEC principle V)* requires that, where appropriate, individuals should be offered prominent, effective, and affordable mechanisms to exercise choice in relation to collection, use, and disclosure of their personal information. Since consent is already an exception to the collection and use and disclosure principles (III and IV), this only adds an emphasis on the mechanisms of choice, and is redundant. Elevation of choice to a separate principle also carries with it some risk of mis-application in national laws to allow contracting out of other principles. It is hard to see the value of this principle.

'*Accountability*' *(and data export limitations) (APEC principle IX*), has two elements. In what can be called 'domestic accountability' it is uncontentious and similar to the OECD Guidelines, in requiring that 'a data controller should be accountable for complying with measures that give effect to the Principles', with no requirement that further obligations be imposed on processors. Where information is transferred to a third party, this requires either (a) the consent of the data subject or (b) that the discloser 'exercise due diligence and take reasonable steps to ensure that the recipient…will protect the information consistently with these Principles'. Once the transferor has 'exercis[ed] due diligence and taken reasonable steps' (which are not further defined), the transferor has no further liability to the data subject, no matter what breaches of the principles occur in the hands of the recipient. However, in what can be called 'export accountability', principle IX explicitly applies when the recipient is overseas ('whether domestically or internationally'), even if that importer is the agent (processor) acting for the exporter. If the data is exported to a jurisdiction without applicable privacy laws, the data subject will have no remedy against the exporter, and none against the importer, unless there is some other enforceable mechanism for compliance. A contractual clause between exporter and importer requiring APEC compliance, will not provide such a remedy, even in theory, unless the importer is in a jurisdiction where consumers can enforce such clauses benefiting third parties (i.e. where doctrines of privity of contract do not prevent this). The accountability principle is APEC's only substitute for a data export limitation principle,[68] and means that such a 'due diligence' requirement in a national law, or any other enforcement process, is sufficient for compliance with the APEC Privacy Framework. This sub-principle was proposed by the USA, and initially resisted by other jurisdictions.[69]

The significance of this discussion is to underline that the principles in the APEC Privacy Framework are weaker and less privacy-protective than those found in any other international agreement. As discussed later in this section, this has not turned out to be very important in relation to the development of data privacy laws in Asian jurisdictions, as most of them have already incorporated stronger protections than the APEC Framework requires. However, the low standard represented by the APEC Privacy Framework is important and must be remembered in three contexts, discussed in Chapter 19: (i) it is the standard that companies are required to meet in order to comply with the APEC **(p.36)** Cross-border Privacy Rules (CBPR); (ii) it is the standard that would be relevant in any 'interoperability' between the APEC region and other regions; (iii) principle IX ('export accountability') has been implemented in a number of Asian privacy laws.

The APEC Framework—no enforcement requirements

In relation to implementation, Part IV of the Framework exhorts APEC members to implement the Framework without requiring any particular means of doing so, or providing any means of assessing whether they have done so.[70] Legislation is not required. Any 'peer assessment' of APEC compliance was expressly rejected,[71] and even the provision of 'country reports' has failed.[72] APEC members have no legal obligations to implement the Framework, and no court or other body can question their failure to do so. In terms of its implementation requirements, the Framework is, therefore, considerably weaker than any other international privacy instrument.

Influence of the APEC Privacy Framework between 2004 and 2013

The APEC Privacy Framework involves voluntary participation in six-monthly meetings of APEC's data privacy subgroup. Since 2006 these meetings have been primarily concerned with development of the APEC CBPR, and have had little to do with encouraging development of data privacy laws in countries without such laws.

Twelve of the 21 APEC member 'economies' now have comprehensive data privacy laws. In addition, Malaysia and Singapore have private sector only laws. Vietnam, Indonesia, and China have substantial e-commerce and consumer transaction laws. Thailand and the USA have public sector only laws. Thailand has a Bill for a private sector law. Brunei, and Papua New Guinea have no privacy laws. The principles in most of these laws exceed the requirements of the APEC Framework, and so any influence of the Framework is not obvious.[73] Another approach is to ask whether the three distinctive 'APEC Principles'—'preventing harm' (principle I); 'choice' (principle V); and 'accountability' concerning data exports (principle IX)—have had any influence on the development of national privacy laws, in APEC economies or elsewhere. Their influence appears to be minimal. New Zealand had a provision (not a principle) which could be recognized as 'preventing harm' before the APEC Framework existed, and Canada had an 'accountability' principle relevant to data exports. The 'choice' principle is not explicitly included in any national data protection principles, and it is difficult to assess whether it is impliedly and diffusely implemented anywhere. Vietnam has none of the 'APEC trio', although otherwise it joins Japan as the least 'European' of Asian laws. The Mexican law, the 2012 Singaporean Act, the 2012 Philippines Act, and the Australian law as amended in 2012 do include versions of **(p.37)** the APEC 'accountability' principle in relation to data exports, so this is the one 'APEC principle' which seems to have had some influence.

APEC's CBPR scheme and the future

APEC has been developing since 2004 what is now called its Cross-Border Privacy Rules (CBPR) system, which received ministerial endorsement in 2011. In 2013 the USA became the first APEC country to become a full participant in the CBPR system, with an enforcement body (the Federal Trade Commission), an APEC-approved Accountability Agent (TRUSTe), and three US companies approved as CBPR-compliant (IBM USA). No Asian country is yet a full participant, though Japan applied to participate in 2013. Any influence of APEC CBPR in Asia (or elsewhere) is a matter for the future, and is therefore discussed in Chapter 19.

3.4. The CoE Data Protection Convention 108 (1981) and Protocol (2001)

The Council of Europe (CoE) Data Protection Convention 108 of 1981[74] ('CoE Convention 108') is the only genuine treaty which deals explicitly with data protection.[75] It is binding in international law on its parties, and enforceable within the severe limits that treaty enforcement through diplomatic means allows (see Chapter 19 for proposed changes). Citizens of European states can also indirectly enforce data protection standards similar to those in CoE Convention 108, via actions in the European Court of Human Rights, under the privacy protections in Article 8 of the European Convention on Human Rights (ECHR). It is global in its potential membership (see Chapter 19). The similarities of many aspects of the contemporaneously developed[76] OECD Guidelines and CoE Convention 108 'are due partly to the extensive co-operation that took place between the bodies charged with drafting the two codes'.[77] The Convention applies to both public sector and private sector organizations.

CoE Convention 108 includes a set of data privacy principles that, while stated briefly, contain versions of all of the elements we now recognize as 'minimum' data privacy principles. Articles 5–8 set out the data protection principles in what has been correctly described as 'broad brush fashion',[78] particularly in Article 5, which requires that:

> Personal data undergoing automatic processing shall be: 1. obtained and processed fairly and lawfully; 2. stored for specified and legitimate purposes and not used in a way incompatible with those purposes; 3. adequate, relevant and not excessive in relation to the purposes for which they are stored; 4. accurate and, where necessary, kept up to date; 5. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

(p.38) These articles also require 'appropriate' data security, and rights to ascertain the existence of personal files, to access them, and to correct them. Provisions concerning 'sensitive' data and deletion go beyond what the OECD Guidelines require.[79] However, CoE Convention 108 required few enforcement mechanisms. The 2001 Additional Protocol[80] to CoE Convention 108 (the 'Additional Protocol'), in force since 2004, added a commitment by its parties to data export restrictions, to an independent data protection authority, and to a right of appeal to the courts, bringing the standards of the Convention approximately up to the same level as the EU Directive. The Additional Protocol did not change the limitations on how CoE Convention 108 could be enforced against member states, its most significant weakness.

Forty-four of the 47 CoE member states have ratified the Convention, and have data privacy laws.[81] Turkey is the only ratifying member that has not enacted a data privacy law. Forty-three countries have signed the Additional Protocol, and 35 have ratified it[82] (including Uruguay's 2013 ratification).

Significance to Asia

The significance of CoE Convention 108 to Asia comes from the following factors: (i) the original (1981) version of the Convention, in tandem with the OECD Guidelines of the same year, created the 'minimum' set of privacy principles that have since been incorporated in all subsequent international privacy standards, and have been the broadest influence on national data privacy laws globally; (ii) the Convention plus 2001

Additional Protocol, in tandem with the 1995 EU Directive, created the 'European standards' that have been extremely influential on most national data privacy laws outside Europe adopting privacy principles with higher than 'minimum' standards; (iii) the CoE is now developing a third generation of privacy principles (as is the EU); and (iv) since 2008 the CoE Convention is being 'globalized', open to accession by non-European countries including those in Asia. The first two factors are discussed in Chapter 3, the last two factors in Chapter 19.

3.5. UN Guidelines for the Regulation of Computerized Data Files (1990)

The UN Guidelines for the Regulation of Computerized Data Files were adopted by the General Assembly on 14 December 1990,[83] following the adoption by the UN Human **(p.39)** Rights Committee in 1989 of its General Comment on Article 17 of the ICCPR (see section 4.1 of this chapter). The Guidelines arose from a French initiative. The Guidelines, although not mandatory, set out 'minimum guarantees that should be provided in national legislations', covering lawful and fair collection, processing and purposes, accuracy, purpose specification, access, non-discriminatory use, security, supervision and sanctions, transborder data flows (allowing limitations), and scope ('public and private computerized files', with the option of extension to manual files). Although the Guidelines do suggest means of implementation, they state that implementing procedures 'are left to the initiative of each State'. They have not had a significant impact since their adoption by the General Assembly, but it is possible that they may have some influence in future, particularly as privacy is back on the UN agenda (see Chapter 19), and in their application to 'Government International Organisations' (made applicable by Part B of the Guidelines). The possibility of a UN data privacy treaty in future is discussed in Chapter 19.

4. Privacy in human rights instruments relevant to Asia

The protection of privacy in general human rights treaties stems from the general requirement not to arbitrarily interfere with privacy included in the Universal Declaration of Human Rights 1948 (UDHR), Article 12,[84] which has no binding force. There is no Asia-wide human rights declaration, unlike in Europe, Africa, and the Americas,[85] but there is now a sub-regional ASEAN declaration, discussed in section 2.1 of this chapter.

4.1. International Covenant on Civil and Political Rights, Article 17

The International Covenant on Civil and Political Rights 1966 (ICCPR)[86] is the only human rights agreement affecting privacy protection relevant to Asia. Article 17 has similar wording to the UDHR, Article 12[87] and provides:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour or reputation.
> 2. Everyone has the right to protection of the law against such interference or attacks.

This section therefore considers the extent to which ICCPR, Article 17 acts as a privacy protection in relation to Asian countries.

(p.40) Enforcement of the ICCPR

There are in theory three methods of enforcement of the ICCPR, but in practice the third is not significant. The UN Human Rights Committee (UNHRC)[88] monitors implementation of the ICCPR by its state parties. It consists of 18 independent experts,[89] elected for terms of four years. First, individuals 'under the jurisdiction' of a state can complain to the UNHRC of breaches, if they have first exhausted all local remedies, but only if the state has adopted the First Optional Protocol to the ICCPR (as discussed in the following sections). Second, state parties must provide reports to the UN Human Rights Committee concerning implementation of the ICCPR rights. These may result in criticisms by the Committee of local laws which do not adequately implement Article 17.[90] Such reports are mentioned in the relevant country chapters in Part II. Third, one state party can in theory complain to the UN Human Rights Committee concerning violations by another state party under article 41 of the Covenant, but this is 'a dead letter which has never been invoked'.[91] In addition, there are various ways by which Article 17 can become part of the domestic law of countries that have ratified the ICCPR (discussed below in this section).

Applicability of the ICCPR and its Optional Protocol to Asian countries

Sixteen Asian countries have ratified the ICCPR,[92] and China signed the ICCPR in 1998 but has not ratified it. Six have not even signed it: Bhutan, Singapore, Malaysia, North Korea, Myanmar, and Brunei. Three other jurisdictions are not eligible to sign, as they are not UN members: Taiwan, Hong Kong, and Macau. However, the UK ratified in relation to Hong Kong while it was still a colony, and Hong Kong does provide periodic reports to the UNHRC. Seventeen Asian jurisdictions should therefore provide periodic reports to the UNHRC.

Only five Asian countries have ratified the First Optional Protocol, allowing complaints ('communications') by their citizens to be made to the UNHRC: the Philippines (1989), Republic of Korea (1990), Nepal (1991), Sri Lanka (1997), and the Maldives (2006). Cambodia has signed (2004) but not ratified.[93] There are as many as 90 decisions of the UNHRC on communications against states that refer to privacy issues, but none of those decisions concern any of these six countries.[94] Therefore, in practice privacy issues under Article 17 are not yet enforced in Asia via this means.

(p.41) Despite the incomplete pattern of ratifications in Asia of both the ICCPR and the Optional Protocol, Baik argues that 'the slow but steady ratifications of human rights treaties by Asian states over time ensure us that that the normative development of human rights in Asia is ongoing, and the normative common ground is solidly expanding', and he provides tables to demonstrate this.[95]

Information privacy and UNHRC 'General Comments' on Article 17

The UNHRC also provides General Comments on the meaning of particular rights found in the ICCPR. It commented[96] in 1989 on the applicability of Article 17 to information privacy:

> The gathering and holding of personal information on computers, databanks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by states to ensure that information concerning a person's private life does not reach the hands of persons who are not authorised by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, each individual should have the right to ascertain in an intelligible form whether, and if so what, personal data are stored in automatic data files, and for what purposes. Every individual should be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.[97]

Bygrave argues that 'case law developed around Art 17 of the ICCPR provides the clearest indication that the right to privacy in international

law harbours core data protection principles'[98] and that the above General Comment 'clearly establishes that Art 17 necessitates protection of persons from interferences by private bodies' data processing practices'. The Committee is reading into Article 17 many of the elements of information privacy principles found elsewhere, and it could therefore be expected that it would favourably entertain complaints (communications) based on the lack of information privacy legislation, or its inadequacies, in relation to those Asian counties where it has jurisdiction.

Application of ICCPR, Article 17 in Asian domestic laws—direct and indirect effects

In those Asian states that have ratified the ICCPR and are considered to be monist states, Article 17 should be regarded as part of their domestic law: Cambodia, Japan, Nepal, the Philippines, South Korea, Sri Lanka, and Timor Leste.[99] However, in Japan, only self-executing treaties are part of domestic law.[100] The extent to which this will allow Article 17 **(p.42)** to be regarded as a basis for a civil action, or a defence, will depend on the law of each state, and is beyond the scope of this book.

A more indirect effect of ICCPR, Article 17 is that where local constitutional provisions are substantially the same as Article 17, they can also result in laws being held invalid, as has occurred in Hong Kong (see discussion in Chapter 4). The UNHRC decisions on Article 17 may be persuasive in such, as may be cases on the equivalent European provisions. While decisions of regional human rights bodies in Africa or the Americas might be of some persuasive value in courts in Asia, the decisions most likely to be persuasive are those of the European Court of Human Rights, and those of the highest courts in European countries such as the UK or Germany which various Asian countries are accustomed to take into account.

Relevance of European Convention on Human Rights, Article 8 to Asia

Article 8 of the European Convention on Human Rights (ECHR) is similar to ICCPR Article 17 in relation to its protection of privacy. Article 8 is significant for countries outside Europe because a considerable body of case law, primarily by the European Court of Human Rights (ECtHR), has built up around it, much more so than ICCPR Article 17.[101] Some similar issues have been decided by the ECtHR and the UNHRC.[102] Discussing the early case-law that developed around both ICCPR, Article 17 and ECHR, Article 8, Bygrave concluded that there was often imprecision in the decisions as to exactly which aspects of data processing practices were in breach, so the decisions were not as valuable as might be hoped. However, the main problem was that the predominance of decisions concerned surveillance by state agencies, and almost none involved private sector bodies. Nevertheless he saw as a positive sign that both bodies were sensitive to the need to adapt the respective provisions to accommodate new forms of data processing.[103]

5. Other international instruments relevant to data privacy

A number of other types of international instruments have some effect on the development of data privacy laws and practices in Asia, including international trade agreements, international technical standards, privacy seals or trustmarks, and standards proposed by data protection authorities collectively. As yet, none of these have had a major impact on data privacy developments, in Asia or elsewhere, but they are necessary for a full understanding of the international environment.

5.1. International trade agreements—WTO, GATS, and bilateral agreements

These agreements are not likely to be sources of privacy rights, but may act as limitations on the operation of privacy laws. The issue of privacy laws being used as trade barriers could potentially be raised at the World Trade Organization (WTO).

(p.43) Article XIV(c)(2) of the GATS (General Agreement on Trade in Services) provides that:

> Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures:…(c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to:…(ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts.

There has not been much discussion of the implications of this and other GATS provisions[104] for data privacy restrictions, but the New Zealand Law Commission[105] in 2008 found it 'difficult to predict' and merely agreed with Bennett and Raab that it is possible 'that at some point, and in some context, international data protection will be tested within the WTO'.[106] In a detailed discussion of GATS, they had noted Shaffer's conclusion[107] that it was unlikely that the EU's 'adequacy' requirements could be successfully challenged at the WTO.[108] Despite statements by US officials that the EU's requirements are contrary to WTO commitments, the US has never challenged them in that forum. As noted in section 2.2 of this chapter, the SAARC Agreement on Trade in Services (2010) has replicated the GATS provisions. ASEAN trade agreements do not prevent personal data export restrictions.

New bilateral or multilateral trade agreements must also be kept in mind. Countries negotiating such agreements, particularly but not exclusively the USA, are likely to attempt to include a requirement that the parties do not include any significant data export restrictions in their laws.

5.2. International technical standards—ISO and others

International standards organizations, particularly the International Organization for Standardization (ISO),[109] have been developing numerous standards relevant to data privacy and data security for over two decades.[110] These include data security standards,[111] and standards for biometrics, identity management,[112] and privacy impact **(p.44)** assessments.[113] Such technical standards may assist data controllers and processors to provide privacy protection in a more consistent manner, but this depends on the extent to which they implement high or low international privacy standards, and the extent to which they meet local legislative requirements.

The most important recent development has been the publication in 2011 of ISO 29100[114] as a standard for privacy principles. It includes 11 principles stated to be derived from existing principles developed by a number of states and international organizations, and applicable by all parties involved in the processing of personal information.[115] ISO standards are not available for free access, but there is a summary of the privacy principles in ISO 29100 by Wright and Raab.[116] The ISO 29100 principles include all of the OECD Guidelines principles of national application, and go further than the Guidelines in various respects such as requiring that only information which is necessary for the specified purpose of collection is collected, and that information is deleted after completion of the specified use. However, on the key question of limits on

international transfers of personal data, ISO 29100 is silent. It is also ambiguous on whether disclosures (but not uses) are limited to the purpose of collection plus statutory exceptions.

The International Conference of Data Protection and Privacy Commissioners (ICDPPC) has welcomed the development of privacy standards by the ISO, first in their 2004 'Wroclaw Resolution', and reiterated in their 2007 Conference resolution,[117] but this has not resulted in any substantive development. Bennett and Bayley questioned in 2007 whether 'a management standard for privacy protection is an idea whose time has passed', while considering that the 'vision' of standards systems supporting existing law was still as valid as ever. Although ISO 29100 is still too new for any assessment of its influence, it does seem that the idea of a privacy standard still has some life in it. The extent to which it may be utilized within Asian jurisdictions is unknown, as it is elsewhere, but there is considerable interest in such standards in Japan, though this does not seem replicated elsewhere in Asia.

5.3. Privacy seals and 'trustmark' schemes—no international standards

It is convenient to deal here with privacy seals and trustmarks, not because there is any international standard for them, but because they have a relationship with the international technical standards discussed above. However, the relationship is often rather like that **(p.45)** between a US$500 designer handbag and one that looks similar and is available for US$5 over the Internet. As defined by Rodrigues et al.:[118]

> A privacy seal is a certification mark or a guarantee issued by a certifying entity verifying an organization's adherence to certain specified privacy standards. A privacy seal is a visible, public indication of an organization's subscription to established, largely voluntary privacy standards that aim to promote consumer trust and confidence in e-commerce.

There are no international standards for privacy seals or trustmarks. There is a European-wide EuroPrise seal programme operated by the data protection authority in the German region of Schleswig-Holstein. The largest commercial provider internationally is TRUSTe, but this company is not yet significant in Asian jurisdictions. In Asia, there are government-supported trustmark schemes in Japan, South Korea, Taiwan, and Vietnam, and some operation of other commercial schemes in various countries, but no Asia-wide or sub-regional scheme. National schemes will be discussed in the chapters in Part II concerning those countries. The APEC CBPR system is discussed in Chapter 19.

The one commercial trustmark scheme that has some presence outside the USA, TRUSTe, was originally, in 1996, a non-profit spin-off of the Electronic Frontier Foundation (EFF), but by 1999 EFF concluded that the 'experiment is in many ways a failure'.[119] TRUSTe became a for-profit company in 2008, and is based in San Francisco with facilities in the Philippines. TRUSTe has various certification programmes (children's privacy, downloads, etc.) but its most general one, for 'TRUSTed Websites' has 'Minimum Program Requirements'[120] which include 'Privacy Practices' which have some resemblance to the OECD or APEC privacy principles. They are, at best, the weakest possible interpretation of those principles, but no analysis is attempted here of whether they could be argued to comply with those principles, as they are of no significance in Asian jurisdictions. TRUSTe's lack of enforcement of its own standards has been regularly and severely criticized by analysts of its practices such as Edelman[121] and Connolly.[122]

Trustmark schemes have rarely been regarded positively by those who have investigated them. In addition to Edelman and Connolly, Bennett and Bayley assert[123] that '[f]requently, privacy seals have been awarded without the kind of systemic and rigorous investigation and auditing characteristic of quality assurance programs' (the ISO-style technical privacy standards with which they contrast trustmarks). After discussion of a number of privacy seal or trustmark schemes (including TRUSTe and Japan's JIPDEC Privacy Protection Mark), Bennett and Raab[124] were dismissive of both the actual and potential value of such schemes:

> **(p.46)** None of these systems, however, has yet achieved general recognition and credibility. Ironically, the more privacy seal programs in existence, the more the consumer will be confused, and the more difficult it will be for any one system to achieve a reputation as the methodology by which privacy-protective practices can be claimed and assured. Moreover, each organization operates in a competitive marketplace. The more stringent the registration requirements, the higher the likely consumer confidence, but the lower the likelihood businesses will sign up.

6. Organizations of privacy-related authorities, and interest groups

Various global and regional associations of DPAs or other data privacy enforcement authorities (PEAs) are of increasing significance. Associations of broader human rights authorities are also considered here, as it is possible they may become more significant in privacy issues in future. Business and civil society groups involved in privacy in Asia are also mentioned briefly.

There are many organizations of DPAs across the world—global, regional, linguistic, and political[125]—but the most influential is the EU's Article 29 Working Party (EU-A29WP), both because it has a formal role under the EU Directive (in such matters as 'adequacy' assessments) and because of the quality and diversity of its collective Opinions on data privacy issues.[126] Its membership is the data protection authorities of all 28 EU member states, the world's most substantial body of expertise in data privacy. It is important to stress, to avoid confusion, that the APPA forum is not the Asia-Pacific equivalent of the EU-A29WP, and has no such significance, breadth of membership, institutional role, or willingness to make collective statements. Nevertheless, it serves a useful function. The closest Asia-Pacific equivalent to EU-A29WP is probably the ECSG APEC data privacy subgroup,[127] but this does not make policy statements, and is attended by a mix of government representatives, privacy authorities, and others. Its functions are now primarily to do with the APEC CBPR, and therefore it is discussed in Chapter 19.

6.1. International Conference of Data Protection and Privacy Commissioners

The International Conference of Data Protection and Privacy Commissioners (ICDPPC) is the grouping of data protection authorities of broadest scope and greatest longevity, having held annual conferences for 35 years. As Raab points out 'conference' is used not only to describe their annual meeting, but as a collective noun.[128] It has accreditation standards which govern which authorities can attend its closed meetings and vote on resolutions—these were originally quite strict but were simplified and possibly weakened in 2010.[129] The ICDPPC annual conference is open to all attendees (except for closed sessions) and has become the leading global data protection conference. Of the 85 countries which have data **(p.47)** protection authorities appointed under their data privacy laws, only 59 national DPAs are accredited to ICDPPC (70 per cent of current national data protection authorities).[130] The only Asian members of ICDPPC are the Hong Kong and South Korean DPAs.

The ICDPPC members adopt joint policy resolutions, but there is no central repository of these resolutions, although they now tend to be gathered together on the websites set up by each conference host.[131] In recent years they have included strong calls for an international data privacy agreement, discussed further in Chapter 19. The ICDPPC adopted a Resolution on International Standards of Privacy at its 2009 meeting, commonly called the 'Madrid Resolution'.[132] The content of the principles and the enforcement mechanisms it recommended are

discussed in the next chapter. Its adoption is not known to have had any effect. A Resolution adopted by the ICDPPC in 2008 also supported the Council of Europe's invitation to states, whether or not they are members of the Council of Europe, to ratify CoE Convention 108 and its Additional Protocol.

6.2. Asia-Pacific Privacy Authorities

The APPA is a 'forum' of Asia-Pacific national and sub-national privacy authorities. Its geographical boundaries are undefined except by the term 'Asia-Pacific', so it is uncertain, for example, whether all Asian DPAs, including those not necessarily within the normal meaning of 'Asia-Pacific', such as an Indian DPA (if created), would be eligible to join. It is at least as broad as APEC, including countries and provinces on the Pacific side of the Americas. APPA now has 16 members including four from Australia, two from Canada, Hong Kong, two from South Korea, Macau, Mexico, Colombia, Peru, New Zealand, and the USA.[133] Membership was previously limited to those DPAs that had been accredited to the ICDPPC.[134] However, APPA has reduced its standards, and now also accepts as members any 'privacy enforcement authorities' (PEA) as well as DPAs.[135] The Macau DPA was previously only an observer at its meetings, due to its continuing incomplete legislative basis and lack of formal independence, but is now a full member (via GPEN not APEC CPEA—see following parts). Neither Japan nor Taiwan are members due to lack of any plausible PEA. The Singaporean and Malaysian DPAs may join via first joining GPEN or APEC CPEA, since independence is no longer required. Singapore's DPA is an observer as of November 2013. The Philippines DPA has not yet been appointed.

APPA meets twice per year with the primary function of sharing experiences, but has also developed valuable standards on reporting and citing privacy decisions.[136] It has an **(p.48)** anodyne Statement of Objectives,[137] that includes fostering sharing of knowledge and resources, and supporting cross-border enforcement cooperation (although this would often be through CPEA or GPEN). It does not involve any commitment to take common actions, and the only common action seems to have been two letters by one DPA on behalf of APPA members, to Google concerning its merged Terms of Service.[138] APPA is expanding its membership (particularly in Latin America) and activities and will probably be more significant in future. It has a considerable and increasing overlap in personnel with the APEC data privacy subgroup, although that is technically a grouping of countries ('economies' in APEC-speak) whereas APPA is a grouping of DPAs and PEAs.

6.3. Global Privacy Enforcement Network

The Global Privacy Enforcement Network (GPEN) originated in a 2007 OECD Recommendation[139] which called for the establishment of an informal network of privacy enforcement authorities. GPEN membership is 'open to any public privacy enforcement authority that: (1) is responsible for enforcing laws or regulations the enforcement of which has the effect of protecting personal data; and (2) has powers to conduct investigations or pursue enforcement proceedings'.[140] GPEN has members from 32 jurisdictions, all of which have data privacy laws of one form or other, and most but not all of which are OECD members.[141] The Asian members of GPEN are the DPAs from Hong Kong SAR, Macau SAR, and South Korea. Macau's inclusion illustrates that Asian jurisdictions that are not part of APEC can only join GPEN, not APEC CPEA (discussed in section 6.4 of this chapter).

6.4. APEC Cross-border Privacy Enforcement Arrangement

As a result of the development of APEC CBPR there has been developed, separate from GPEN, a 'framework for regional cooperation' called the APEC Cross-border Privacy Enforcement Arrangement (CPEA)[142] in which '[a]ny Privacy Enforcement Authority in an APEC economy may participate in cross-border co-operation, enforcement and information sharing'.[143] The CPEA is therefore not exclusively concerned with the APEC CBPR (Chapter 19, section 2). Created in 2010, it has as members 'PE Authorities' (i.e. privacy enforcement authorities), the data protection authorities from only six of the 17 APEC economies which have data privacy laws (Australia, NZ, USA, Canada, Hong Kong, and Mexico), plus government departments from South Korea (but not their independent DPAs) and Japan. The separate membership of 15 Japanese government agencies indicates **(p.49)** the lack of central coordination in their law. APEC CPEA therefore has membership from relatively few APEC countries, and from only three Asian jurisdictions (Hong Kong SAR, South Korea, and Japan). CPEA's administration is shared between the APEC Secretariat, and the Australian, New Zealand, and US members. There is no indication on the CPEA website that it has yet done anything.

6.5. Asia-Pacific Forum of National Human Rights Institutions

The Asia-Pacific Forum of National Human Rights Institutions (APF-NHRI) aims to advance human rights in the Asia-Pacific through its member organizations, and to facilitate the formation and growth of national human rights institutions by providing training, networking, and resource sharing.[144] APF-NHRI started in 1996,[145] and now has nine full members, in compliance with the Paris Principles,[146] from the national human rights commissions of countries considered in this book: Afghanistan, India, Indonesia, Malaysia, Nepal, the Philippines, South Korea, Thailand, and Timor Leste. It also has associate members from Myanmar, the Maldives, Sri Lanka, and Bangladesh. It thus has a total of 14 members from Asia, plus seven members from other countries in the Asia-Pacific. APF-NHRI full members must comply with the Paris Principles, and may be expelled from membership if they cease to do so.[147] The Paris Principles require compliance before full membership is granted, and associate membership is often granted where candidates are not yet fully able to comply.[148]

It is clear that data privacy is a human right: privacy is included in ICCPR, Article 17; the UN HRC has set out data privacy rights stemming from Article 17 (see section 4.1 of this chapter). The Snowden revelations of unimagined levels of state surveillance privacy have made data privacy a UN and UNHRC issue once again (discussed in Chapter 19). It is now clear that privacy is central to human rights issues, so there are stronger reasons why human rights commissions should become involved in data privacy issues, and other privacy issues. The APF has not yet done so at a regional level. If human rights commissions were involved in these issues, the APF-NHRI membership would cover more countries in the region than is currently the case with APPA. It would also provide a valuable alternative regional voice on privacy issues.

6.6. Civil society, professional, and business organizations in Asia

There are no professional or business groups in Asia which have a particular focus on privacy issues. A number of global business groups, and particular companies, are a constant presence at conferences, APEC DPS meetings, APPA conferences, etc., as they have the necessary financial resources to travel to, and to subsidize, events put on by **(p.50)** relatively impecunious privacy authorities. International associations of privacy consultants and company privacy officers have not yet established regional or national branches in Asia.[149] There is a mutually suspicious relationship between these organizations and those of privacy advocates/non-governmental organizations (NGOs), and little membership overlap.

Civil society organizations involved in privacy have only a local, not a regional or sub-regional presence in Asia. There are local NGOs interested in privacy in many Asian countries, but none have a single or even a sustained focus on privacy issues, and usually become involved only when a major privacy issue arises. In his study of privacy advocates, Bennett did not identify any significant Asian organizations with a 'privacy centric' focus.[150] But, as he says is generally the case, it is true in Asia that there are 'a huge number of potential groups whose support could be

mobilized given the correct circumstances, the right issue, or the correct case of intrusive governmental or corporate behaviour', as well as some that have privacy protection as an explicit, though not primary, goal. The actions of some such NGOs to resist surveillance are discussed in the country chapters in Part II. London-based Privacy International (PI) has in recent years engaged in 'capacity building' meetings and training sessions with local NGOs interested in privacy in some Asian countries, and has often commissioned them to write reports as part of its 'Privacy in the Developing World' project,[151] possibly for submission as stakeholder reports to the UN Universal Periodic Review process. There is also an Asia-Pacific wide Asian Privacy Scholars Network,[152] which is not an advocacy organization but an information exchange network operating primarily between academics, via an email list and periodic conferences. However, as Bennett points out, such academic networks have always been a key component of privacy advocacy.[153]

Notes:

([1]) Simon Chesterman, 'Introduction and Chapter One: From Community to Compliance? The Evolution of Monitoring Obligations in ASEAN' (Cambridge University Press, 2014, forthcoming) <http://papers.ssrn.com/abstract_id=2347833>.

([2]) For an overview of ASEAN see 'Overview', ASEAN <http://www.asean.org/asean/about-asean/overview>.

([3]) *Charter of the Association of Southeast Asian Nations*, 20 November 2007.

([4]) Chesterman considers that 'an important tension in this transformation is the question of whether the "ASEAN way"—defined by consultation and consensus, rather than enforceable obligations—is consistent with the establishment of a community governed by law' (Chesterman, 'Introduction and Chapter One: From Community to Compliance?').

([5]) Supported by other instruments such as the Treaty of Amity and Cooperation in Southeast Asia (1976), and the ASEAN Protocol on Enhanced Dispute Settlement Mechanism (see art. 24 of the Charter).

([6]) Tae-Ung Baik, *Emerging Regional Human Rights Systems in Asia* (Cambridge, 2012), p. 202.

([7]) See Baik, *Emerging Regional Human Rights Systems in Asia.*

([8]) *Charter of the Association of Southeast Asian Nations*, arts. 1.7 and 14, respectively.

([9]) ASEAN Intergovernmental Commission on Human Rights (AICHR) <http://aichr.org/>.

([10]) *Terms of Reference of AICHR* (AICHR) <http://aichr.org/?dl_name=TOR-of-AICHR.pdf>.

([11]) *Terms of Reference of AICHR*, cls. 3–6.

([12]) United Nations International Coordinating Committee of National Human Rights Institutions (ICC), 'Principles Relating to the Status of National Institutions' ('Paris Principles') (UN ICC, 1991) <http://www.asiapacificforum.net/members/international-standards>.

([13]) Baik, *Emerging Regional Human Rights Systems in Asia*, p. 205.

([14]) Forum-Asia, 'Still Window Dressing: Performance Report on the AICHR 2011–12' <http://www.forum-asia.org/?p=16296>. They criticized the modus operandi of 'consultation and consensus' 'which results in the pursuit of the lowest common denominator, as illustrated in the drafting of the [ASEAN Human Rights Declaration]'. There is also a comprehensive lack of transparency about the financial aspects of AICHR, including its sources of funding and budget.

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

([16]) Human Rights Watch, 'Civil Society Denounces Adoption of Flawed ASEAN Human Rights Declaration', 19 November 2012 <http://www.hrw.org/print/news/2012/11/19/civil-society-denounces-adoption-flawed-asean-human-rights-declaration>. Among the criticisms are that '[i]n many of its articles, the enjoyment of rights is made subject to national laws, instead of requiring that the laws be consistent with the rights'; it 'fails to include several key basic rights and fundamental freedoms, including the right to freedom of association and the right to be free from enforced disappearance'; and that the rights it states are of a lower standard than those in equivalent declarations in Europe, Africa, or the Americas. Consequently, the civil society organizations state that they will not invoke it in their work 'except to condemn it as an anti-human rights instrument'.

([17]) Coordinated by Human Rights Watch and including among the international organizations the International Commission of Jurists and Article 19.

([18]) UN News Centre, 'UN Official Welcomes ASEAN Commitment to Human Rights, But Concerned Over Declaration Wording', 19 November 2012 <http://www.un.org/apps/news/story.asp?NewsID=43536#.UgiIOVP9ogI>.

([19]) Baik, *Emerging Regional Human Rights Systems in Asia*, p. 206.

([20]) Clause 5(e), *E-ASEAN Framework Agreement*, 24 November 2000 <http://www.asean.org/news/item/e-asean-framework-agreement>.

([21]) They are: '6. It is crucial to create a trustworthy environment for E-Commerce by creating and enforcing laws, regulations and guidelines pertaining to consumer and business rights to protect them from undesirable elements in the Internet' and '7. Establish framework for cross border complaints and dispute resolution to discourage fraud, encourage better customer service and improve online sales': *The ASEAN E-commerce Database Project* (Department of Trade and Industry, the Philippines, Ref. DTI/ASEANTELSOM/01 2010) <http://www.asean.org/archive/documents/ASEAN%20eCommerce%20Database%20Project.pdf>.

([22]) Chris Connolly, 'A New Regional Approach to Privacy in ASEAN' (Galexia, 2008) <http://www.galexia.com/public/research/articles/research_articles-art55.html>.

([23]) *ASEAN Framework Agreement on Services* art. XIV(1) provides that '[t]he terms and definitions and other provisions of the [General Agreement on Tariffs and Trade] GATS shall be referred to and applied to matters arising under this Framework Agreement for which no specific provision has been made under it' and art. IX(1) provides that '[t]his Framework Agreement or any action taken under it shall not affect the rights and obligations of the Member States under any existing agreements to which they are parties'.

([24]) SAARC website <http://www.saarc-sec.org/>.

([25]) Baik, *Emerging Regional Human Rights Systems in Asia*, p. 207.

([26]) SAARC Agreement on South Asian Free Trade Area (SAFTA) <http://www.saarc-sec.org/userfiles/saftaagreement.pdf>. All SAARC countries are parties except Afghanistan.

([27]) SAARC Agreement on Trade in Services, 2010; see discussion on SAARC website at <http://www.saarc-sec.org/areaofcooperation/detail.php?activity_id=46>.

([28]) The SAARC Charter of Democracy includes commitments to democratic institutions and the rule of law, but contains nothing about human rights beyond a recital '[r]eaffirming faith in fundamental human rights and in the dignity of the human person as enunciated in the Universal Declaration of Human Rights and as enshrined in the respective Constitutions of the SAARC Member States'. See SAARC Charter of Democracy <http://www.saarc-sec.org/SAARC-Charter-of-Democracy/88/>.

([29]) Baik, *Emerging Regional Human Rights Systems in Asia*, pp. 208–9.

([30]) For some sub-regional groupings, see Baik, *Emerging Regional Human Rights Systems in Asia*, pp. 199–200.

([31]) Baik, *Emerging Regional Human Rights Systems in Asia*, p. 199.

([32]) See T. Nakamura (Ed.), *East Asian Regionalism from a Legal Perspective* (Routledge, 2009). See also Wikipedia entry 'East Asian Community'.

([33]) Some are summarized in Baik, *Emerging Regional Human Rights Systems in Asia*, pp. 199–201.

([34]) *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD, Paris, 1981); adopted as a Recommendation of the Council of the OECD, 23 September 1980.

([35]) List of OECD Member Countries (OECD, 2013) <http://www.oecd.org/general/listofoecdmembercountries-ratificationoftheconventionontheoecd.htm>.

([36]) 'In May 2007, OECD countries agreed to invite Chile, Estonia, Israel, Russia and Slovenia to open discussions for membership of the Organisation and offered enhanced engagement to Brazil, China, India, Indonesia and South Africa' (OECD website). Chile, Slovenia, Israel, and Estonia have since become members. Russia is not yet a member.

([37]) 'While accepting certain restrictions to free trans-border flows of personal data, they seek to reduce the need for such restrictions and thereby strengthen the notion of free information flows between countries.'

([38]) For example, see Roger Clarke, 'Beyond the OECD Guidelines: Privacy Protection for the 21st Century' (unpublished, 2000) <http://www.anu.edu.au/people/Roger.Clarke/DV/PP21C.html>. This very detailed critique 'catalogues the deficiencies that were inherent in the "fair information practices" tradition that the OECD's 1980 Guidelines codified, together with the additional problems that have arisen since their formulation'.

([39]) Michael Kirby, 'Privacy Protection, A New Beginning: OECD Principles 20 Years On' (1999) 6 PLPR 25. The Guidelines were developed by an Expert Group chaired by Justice M.D. Kirby, then Chairman of the Australian Law Reform Commission.

([40]) *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* (O.J. L. 281, 23 November1995, pp. 31ff).

([41]) Christopher Kuner *European Data Protection Law: Corporate Compliance and Regulation* (2nd Edn., Oxford University Press, 2007) is the standard text. For a concise account, see Bygrave, 'International Agreements to Protect Personal Data', pp. 30–43.

([42]) Bygrave, 'International Agreements to Protect Personal Data', p. 32.

([43]) The most important additional principles in the EU Directive are described in Chapter 3 as: data export restrictions based on destination; minimal collection; 'fair and lawful processing'; 'prior checking'; deletion; sensitive data protections; automated processing controls; and direct marketing opt-out. Others could be added.

([44]) Article 29 Data Protection Working Party, 'Opinions and recommendations' <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm>.

([45]) CoE Convention 108 has included the same requirement since its 2001 Additional Protocol.

([46]) Graham Greenleaf and Lee Bygrave, 'Not Entirely Adequate but Far Away: Lessons from How Europe Sees New Zealand Data Protection' (2011) 111 Privacy Laws & Business International Report, pp. 8–9 <http://ssrn.com/abstract=1964065>.

([47]) Article 29 Data Protection Working Party, 'Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive', WP 12, DG XV D/5025/98, adopted 24 July 1998 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf>; Article 29 Data Protection Working Party, 'First orientation on Transfers of Personal Data to Third Countries: Possible Ways Forward in Assessing Adequacy', WP 4, XV D/5020/97-EN final, adopted 26 June 1997 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp4_en.pdf>.

([48]) See Bygrave, 'International Agreements to Protect Personal Data', p. 39 and Kuner, *European Data Protection Law* ch. 4-D 'Adequacy Decisions'.

([49]) Andorra, Argentina, Canada, Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, and Uruguay (and not Australia as a whole, despite the appearance to the contrary on the EC website).

([50]) See Kuner, *European Data Protection Law*, ch. 4-G 'Exceptions' for a full analysis.

([51]) European Commission, 'Model Contracts for the transfer of personal data to third countries' <http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm>.

([52]) Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council.

([53]) *Standard contractual clauses*, cl. 9.

([54]) *Standard contractual clauses*, cls. 3(1)–3(4).

([55]) See Lokke Moerel, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers* (Oxford University Press, 2012).

([56]) Australia, Brunei Darussalam, Canada, Chile, People's Republic of China, Hong Kong, Indonesia, Japan, Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, the Philippines, Russia, Singapore, Chinese Taipei, Thailand, United States, Vietnam: APEC Member Economies (APEC, 2012) <http://www.apec.org/about-us/about-apec/member-economies.aspx>.

([57]) Many Asian and South American countries were seeking APEC membership in 2008. When it refused India's application for membership, APEC decided not to admit more members until 2010, and this has not changed since.

([58]) APEC is the only intergovernmental grouping in the world operating on the basis of non-binding commitments, open dialogue, and equal respect for the views of all participants. Unlike the WTO or other multilateral trade bodies, APEC has no treaty obligations required of its participants. Decisions made within APEC are reached by consensus and commitments are undertaken on a voluntary basis. ('About APEC', originally published on the APEC secretariat website (no longer online), but since republished elsewhere <http://www.asia-studies.com/apec.html>.)

([59]) *APEC Privacy Framework* (APEC, 2004, completed 2005) <http://publications.apec.org/publication-detail.php?pub_id=390>.

([60]) The Framework originally consisted of Part III containing the principles, plus a Preamble and Scope note in Parts I and II. Part IV 'Implementation' included Section A 'Guidance for Domestic Implementation' but did not include Section B on the 'cross-border elements' (including data exports) until it was added in September 2005 and the Framework completed.

([61]) Preventing harm (I); notice (II); collection limitation (III); uses of personal information (IV); choice (V); integrity of personal information (VI); security safeguards (VII); access and correction (VIII); accountability (including due diligence in transfers) (IX).

([62]) For a full discussion, see Graham Greenleaf, 'Five Years of the APEC Privacy Framework: Failure or Promise?' (2009) 25 *Computer Law & Security Report*, pp. 28–43 <http://ssrn.com/abstract=2022907>.

([63]) See Greenleaf, 'Five Years of the APEC Privacy Framework', Part 2 'APEC Privacy Principles—A brief critique' for a discussion of each APEC principle. See ch. 16 for how APEC deals with 'publicly available information'.

([64]) See footnote 43 above for the most important additional principles in the EU Directive which are absent from the APEC Privacy Framework.

([65]) Including Hong Kong, Korea, Taiwan, Australia, New Zealand, and Canada.

([66]) These include principles concerning collection directly from the individual, data retention, notice of corrections to third party recipients, data export limitations, anonymity, identifiers, sensitive information, and public registers. See Greenleaf, 'Five Years of the APEC Privacy Framework', pt. 2.4 'Five bases for criticism', and for further details see Graham Greenleaf, 'APEC's Privacy Framework Sets a New Low Standard for the Asia-Pacific' in M. Richardson and A. Kenyon (Eds.), *New Dimensions in Privacy Law: International and Comparative Perspectives* (Cambridge University Press, 2005).

([67]) It has apparently been assumed in meetings of the APEC Privacy Sub-group that these should be included: Nigel Waters, 'The APEC Asia-Pacific Privacy Initiative—a new route to effective data protection or a trojan horse for self-regulation?' (2009) 6:1 *SCRIPTed* 75 <http://www2.law.ed.ac.uk/ahrc/script-ed/vol6-1/waters.asp>.

([68]) When the incomplete Framework was announced in 2004, it was assumed that data export limitations would be dealt with in pt. IV 'implementation' when it was completed. However, pt. IV said nothing on the subject.

([69]) Graham Greenleaf, 'The APEC Privacy Initiative: "OECD Lite" for the Asia-Pacific' (2004) 71 *Privacy Laws & Business International Newsletter*, pp. 16–18 <http://ssrn.com/abstract=510683>.

([70]) Greenleaf, 'Five Years of the APEC Privacy Framework', pt. 4 'Implementation—Exhortations only'.

([71]) Among the initial proposals under discussion when the APEC Framework was being negotiated was a New Zealand suggestion of an approach to APEC regional certification of when a jurisdiction had obtained 'substantial compliance' with the APEC Framework, but this proposal was rejected prior to the first draft of the Framework in 2004; see Greenleaf, 'The APEC Privacy Initiative: "OECD Lite" for the Asia-Pacific', 'APEC proposals for self-assessment and data export limits'.

([72]) APEC's website is supposed to have up-to-date reports from each economy on their progress in implementing the Framework, but it only has reports from 14 out of 21 economies, and of those only five are dated after 2006: 'Data Privacy Individual Action Plan' (APEC, undated)

<http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Data-Privacy-Individual-Action-Plan.aspx>.

([73]) 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>.

([74]) *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, opened for signature 28 January 1981, CETS No. 108 (in force 1 October 1985).

([75]) See Lee Bygrave, 'International Agreements to Protect Personal Data' in J.B. Rule and G. Greenleaf (Eds.), *Global Privacy Protection: The First Generation* (Edward Elgar, 2008), pp. 15–49.

([76]) CoE Convention 108 had its origins, in part, in early CoE concerns about 'electronic data banks' and the perception that there was insufficient impetus to encourage European states to enact laws to protect information privacy. Only eight European countries had done so during the 1970s. By the time drafting was under way, the OECD had set out on a similar task but from more of a trade, than human rights perspective.

([77]) Bygrave, 'International Agreements to Protect Personal Data', p. 27.

([78]) Bygrave, 'International Agreements to Protect Personal Data', pp. 15–49.

([79]) 'Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life [or criminal convictions], may not be processed automatically unless domestic law provides appropriate safeguards.'

([80]) *Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Data Flows*, opened for signature 8 November 2001, ETS No. 181 (entered into force 1 July 2004).

([81]) Turkey has signed but not ratified the Convention. San Marino has done neither. Belarus is not a CoE member because of human rights concerns, and the Vatican (Holy See) is not a member because it is not a democracy. The UK and other countries have acceded to the Convention on behalf of their self-governing territories. For details, see Council of Europe: Treaty Office, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data CETS No 108: Member States of the Council of Europe* (16 February 2014) Council of Europe Conventions <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=1&DF=&CL=ENG> for a list of states that have acceded to and ratified the Convention.

([82]) Four countries have not yet signed the Additional Protocol: Azerbaijan, Malta, San Marino, and Slovenia. There are 35 ratifications <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=181&CM=8&DF=&CL=ENG>. Nine European countries (Belgium, Denmark, Greece, Iceland, Italy, Norway, Russia, Ukraine, and the United Kingdom) and three UK territories have ratified the Convention but have not ratified the Additional Protocol. In almost all cases their failure to ratify the Additional Protocol does not matter a great deal because they are EU member states, or their laws have been found 'adequate' by the EU. Therefore they are already under the same obligations imposed by the Additional Protocol, for most purposes.

([83]) UN General Assembly, *Guidelines for the Regulation of Computerized Personal Data Files*, 14 December 1990 <http://www.unhcr.org/refworld/docid/3ddcafaac.html>.

([84]) Article 12 states: 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.'

([85]) Provisions with similar wordings are now found in the American Convention on Human Rights, art. 11, and the European Convention on Human Rights, Art. 8. The African Charter on Human and People's Rights 1981 has no equivalent provision. See for details 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 '2. Relevant provisions on the right to privacy in international human rights instruments'.

([86]) International Covenant on Civil and Political Rights, opened for signature 16 December 1966, 99 UNTS 171 (entered into force 23 March 1976) (ICCPR), Art. 17; First Optional Protocol to the International Covenant on Civil and Political Rights, opened for signature 16 December 1966, 999 UNTS 302 (entered into force 23 March 1976).

([87]) Bygrave, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties', pp. 247–84. This article, though mainly about Art. 8 of the ECHR, compares the ICCPR with the ECHR in relation to privacy protection.

([88]) UN Human Rights Committee <http://www.ohchr.org/EN/HRBodies/CCPR/Pages/CCPRIndex.aspx>. The Committee is separate from the UN Human Rights Council.

([89]) For current membership, see 'Membership' <http://www.ohchr.org/EN/HRBodies/CCPR/Pages/Membership.aspx>.

([90]) 'All States parties are obliged to submit regular reports to the Committee on how the rights are being implemented. States must report initially one year after acceding to the Covenant and then whenever the Committee requests (usually every four years). The Committee examines each report and addresses its concerns and recommendations to the State party in the form of "concluding observations"': 'Introduction—Human Rights Committee' (UN, 2014) <http://www.ohchr.org/EN/HRBodies/CCPR/Pages/CCPRIntro.aspx>.

([91]) Johannes Chan, 'The Hong Kong Bill of Rights: An Introduction' in *Annotations to the Hong Kong Bill of Rights Ordinance* (Butterworths, 1999), p. 4.

([92]) Afghanistan; Bangladesh; Cambodia; India; Indonesia; Japan; Lao People's Democratic Republic; the Maldives; Mongolia; Nepal; Pakistan; the Philippines; Republic of Korea; Sri Lanka; Thailand; Timor Leste; and Viet-nam. See Table of ICCPR Ratifications at <http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en>.

([93]) *Optional Protocol to the International Covenant on Civil and Political Rights* (table of accessions and ratifications) at <http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-5&chapter=4&lang=en>.

([94]) Derived from a search of UNHRC decisions (to 2010) on the WorldLII database 'United Nations Human Rights Committee' <http://www.worldlii.org/int/cases/UNHRC>. There was one complaint against Sri Lanka mentioning privacy, but it was an incidental mention in a building dispute. The UNHRC website <http://tbinternet.ohchr.org/_layouts/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=17>, does not support such searches.

([95]) Baik, *Emerging Regional Human Rights Systems in Asia*, p. 89.

([96]) UNHRC, *General Comment 15(32) on A17*, 1989.

([97]) Paragraph 9, *General Comment 15(32) on A17*, Doc. CCPR/c/21/Rev.1 19 May 1989.

([98]) Bygrave, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties', pt. 3, 'Article 17 of the ICCPR'.

([99]) Baik, *Emerging Regional Human Rights Systems in Asia*, p. 70.

([100]) Baik, *Emerging Regional Human Rights Systems in Asia*, p. 72.

([101]) For an analysis of ECtHR jurisprudence under Art. 8, to 1998, see Bygrave 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties', pp. 254–82.

([102]) For example, the similarities were evident in *Modinos v Cyprus* (1993) 16 EHRR 485, where the European Court of Human Rights held that a Cypriot statute that rendered male homosexual conduct in private between adults a criminal offence violated Art. 8 despite a policy of non-enforcement by Cypriot authorities. This was a case decided on facts almost identical to *Toonen v Australia* [1994] UNHRC 15; CCPR/C/50/D/488/1992 where the ICCPR reached a similar conclusion.

([103]) Bygrave, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties', pp. 282–4.

([104]) GATS further requires in art. VI (1) that '[i]n sectors where specific commitments are undertaken, each Member shall ensure that all measures of general application affecting trade in services are administered in a reasonable, objective and impartial manner'. There is also a need to comply with art. II (1) of GATS, requiring that '[w]ith respect to any measure covered by this Agreement, each Member shall accord immediately and unconditionally to services and service suppliers of any other Member treatment no less favourable than that it accords to like services and service suppliers of any other country'.

([105]) New Zealand Law Commission (NZLC), *Privacy Concepts and Issues: Review of the Law of Privacy, Stage One* (Wellington, New Zealand, 2008), para. 7.69.

([106]) Colin Bennett and Charles Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (MIT Press, 2006), p. 111.

([107]) G. Shaffer, 'Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of US Privacy Standards' (2000) 25 *Yale Journal of International Law* pp. 1–88.

([108]) Bennett and Raab, *The Governance of Privacy*, p. 111.

([109]) ISO website at <http://www.iso.org>.

([110]) For a fuller discussion to 2007, see Bennett and Raab, *The Governance of Privacy*, pp. 105–8; Colin J. Bennett and Robin Bayley, '"Saying what you do and Doing what you Say": Arguments and Prospects for an International Privacy Standard' 29th International Conference of Data Protection and Privacy Commissioners, Montreal, Canada, 25–28 September 2007.

([111]) ISO 17799 (Security standard), 2000, based on the information security practices of international businesses; also ISO 27000 series (Data Security).

([112]) ISO 24745 (Biometric Information Protection); ISO 24760 (Framework for Identity Management).

([113]) ISO 22307:2008 'Financial services—Privacy impact assessment'; H. Hamidovic, 'An Introduction to the Privacy Impact Assessment Based on ISO 22307', *ISACA Journal*, 2010, Vol. 4.

([114]) ISO/IEC 29100:2011, 'Information technology—Security techniques—Privacy framework' <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45123>. This is described by the ISO as a standard which 'provides a privacy framework which specifies a common privacy terminology; defines the actors and their roles in processing personally identifiable information (PII); describes privacy safeguarding considerations; and provides references to known privacy principles for information technology'. See also ISO 29101 (Privacy Reference Architecture).

([115]) It is described by the ISO in ISO/IEC 29100:2011 as 'applicable to natural persons and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where privacy controls are required for the processing of PII [personally identifiable information]'.

([116]) David Wright and Charles Raab, 'Privacy Principles, Risks and Harms' (unpublished, copy provided by authors, 2013).

([117]) ICDPPC, 'Resolution on Development of International Standards' (29th International Conference of Data Protection and Privacy Commissioners, Montreal, Canada, 25–28 September 2007), at <http://www.priv.gc.ca/information/conf2007/res_global_05_e.asp>.

([118]) R. Rodrigues, D. Wright, and K. Wadhwa, 'Developing a Privacy Seal Scheme (that Works)' (2013) 3(2) *International Data Privacy Law*, pp. 100–16 <http://idpl.oxfordjournals.org/content/early/2013/01/31/idpl.ips037.full>.

([119]) Slashdot, 'TRUSTe Decides Its Own Fate Today', 8 November 1999, <http://yro.slashdot.org/article.pl?sid=99/11/05/1021214>, cited by C. Connolly, 'Trustmark Schemes Struggle to Protect Privacy' (Galexia, 2008) <http://www.galexia.com/public/research/assets/trustmarks_struggle_20080926/trustmarks_struggle_public-Introduc.html>, p. 23.

([120]) TRUSTe, 'Minimum Program Requirements' at <http://www.truste.com/privacy-program-requirements/program-requirements>.

([121]) B. Edelman, 'Adverse Selection in Online "Trust" Authorities', Proceedings of ICEC'09 <http://www.benedelman.org/publications/advsel-trust.pdf>; B. Edelman, 'Coupons.com and TRUSTe: Lots of Talk, Too Little Action' <http://www.benedelman.org/news/031808-1.html>.

([122]) Connolly, 'Trustmark Schemes Struggle to Protect Privacy'.

([123]) Bennett and Bayley, 'Saying what you do and Doing what you Say', p. 7.

([124]) Bennett and Raab, *The Governance of Privacy*, p. 167.

([125]) For a global survey to mid-2013 see the section 'Data protection authorities (PDAs) and their associations' in Graham Greenleaf, 'Scheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories' (2014) 23(1) *Journal of Law & Information Science* <http://www.jlisjournal.org/abstracts/greenleaf.23.1.html>; also at <http://ssrn.com/abstract=2280877>.

([126]) Article 29 Working Party, 'Opinions and recommendations' (European Commission, 2014) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm>. They comprise 210 Opinions, Explanatory Documents, Working Papers etc. to 2014.

([127]) APEC Electronic Commerce Steering Group <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.aspx>.

([128]) For a history of ICDPPC, see C. Raab, 'Networks for Regulation: Privacy Commissioners in a Changing World' (2011) 13(2) *Journal of Comparative Policy Analysis: Research and Practice*, pp. 195–213.

([129]) G. Greenleaf, 'Independence of Data Privacy Authorities: International Standards and Asia-Pacific Experience' (2012) 28(1) *Computer Law & Security Review*, section 3.7.

([130]) Greenleaf, 'Scheherezade and the 101 Data Privacy Laws'.

([131]) For example, International Conference of Data Protection and Privacy Commissioners, 'Resolutions adopted at previous conferences' (35th ICDPPC, Poland, 2013) <https://privacyconference2013.org/Resolutions_and_Declarations>. These are also located in the WorldLII International Privacy Law Library database of ICDPPC Resolutions and Declarations <http://www.worldlii.org/int/other/ICDPPCRD/>.

([132]) International Conference of Data Protection and Privacy Commissioners, *International Standards on the Protection of Data Protection and Privacy* ('Madrid Resolution') (ICDPPC, 5 November 2009) <http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf>.

([133]) APPA members <http://www.appaforum.org/members/>.

([134]) C. Raab, 'Information Privacy: Networks of Regulation at the Subglobal Level' (2010) 1(3) *Global Policy*, pp. 296–7.

([135]) Members can be 'accredited to the International Conference of Data Protection and Privacy Commissioners (ICDPPC); or a participant in the APEC Cross-border Privacy Enforcement Arrangement (CPEA); or a member of the OECD Global Privacy Enforcement Network (GPEN)': APPA website at <http://www.appaforum.org/about/>.

([136]) APPA 'Case Note Citation' and 'Case Note Dissemination' on 'Common administrative practices' <http://www.appaforum.org/resources/common_practice.html>.

([137]) APPA 'Statement of Objectives', on APPA 'Resources' APPA 'Resources' <http://www.appaforum.org/resources/>.

([138]) APPA 'Google privacy policy changes—APPA Correspondence 2012' <http://www.appaforum.org/resources/correspondence/google_pp_index.html>.

([139]) OECD *Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy* <http://www.oecd.org/document/60/0,3343,en_2649_34255_38771516_1_1_1_1,00.html>.

([140]) Global Privacy Enforcement Network, *Action Plan for the Global Privacy Enforcement Network (GPEN)* (GPEN, adopted 15 June 2012; Part E amended 22 January 2013) <https://www.privacyenforcement.net/public/activities>.

([141]) Global Privacy Enforcement Network (GPEN) <http://www.privacyenforcement.net/about_the_network>.

([142]) Cross-border Privacy Enforcement Arrangement (APEC, 2010) <http://aimp.apec.org/Documents/2010/ECSG/DPS1/10_ecsg_dps1_013.pdf>. See also *CPEA Fact Sheet* (APEC, 2013) <http://www.apec.org/About-Us/About-APEC/Fact-Sheets/APEC-Cross-border-Privacy-Enforcement-Arrangement.aspx>.

([143]) APEC CPEA website <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.asp>.

([144]) Asia Pacific Forum <http://www.asiapacificforum.net>.

([145]) It was started by Commissions from Australia, India, Indonesia, and New Zealand.

([146]) The difference between Full and Associate membership is whether a national commission fully adheres to the standards set out in the Paris Principles developed by the United Nations to define the core attributes that all new or existing national human rights institutions should possess. The APF-NHRI adopts the accreditation decisions of the International Coordinating Committee of National Human Rights Institutions (ICC) to determine membership status: Paris Principles 1991 ('Principles Relating to the Status of National Institutions') <http://www.asiapacificforum.net/members/international-standards>.

([147]) Asia Pacific Forum Constitution, arts. 11.4(b) and 11.5(b).

([148]) Andrew Byrnes, Andrea Durbach, and Catherine Renshaw 'Joining the Club: The Asia Pacific Forum of National Human Rights Institutions, the Paris Principles, and the Advancement of Human Rights Protection in the Region' (2008) 14(1) *Australian Journal of Human Rights*, pp. 63–98 <http://ssrn.com/abstract=1397466>.

([149]) For example, there is an Australian and New Zealand branch, but no Asian branches, of the 'International Association of Privacy Professionals' (iapp) <http://www.privacyassociation.org/>.

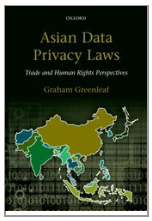
([150]) Colin Bennett, *The Privacy Advocates: Resisting the Spread of Surveillance* (MIT Press, 2008), particularly ch. 2 'The Groups'.

([151]) Privacy International, 'Privacy in the Developing World' (PI, 2014) <http://www.privacyinternational.org/projects/privacy-in-the-developing-world>.

([152]) 'Asian Privacy Scholars Network' (UNSW, 2014) <http://www.cyberlawcentre.org/privacy/apsn.htm>.

([153]) Bennett, ch. 6 'The Networks' in *The Privacy Advocates*.

University Press Scholarship Online
Oxford Scholarship Online



Asian Data Privacy Laws: Trade & Human Rights Perspectives
Graham Greenleaf

Print publication date: 2014
Print ISBN-13: 9780199679669
Published to Oxford Scholarship Online: December 2014
DOI: 10.1093/acprof:oso/9780199679669.001.0001

Standards by Which to Assess a Country's Data Privacy Laws

Graham Greenleaf

DOI:10.1093/acprof:oso/9780199679669.003.0003

[–] Abstract and Keywords

This chapter proposes standards against which national privacy protections can be assessed and compared. Contextual protections are the types of privacy protections, other than specialized data privacy legislation, which require comparison are protections arising from constitutions, treaties, human rights institutions, civil and common law, criminal and administrative laws, and self-regulation. The two main standards for comparison of sets of data privacy principles are the 'minimum' or first generation principles (OECD 1980 and Council of Europe 1981), and the 'European' or second generation principles (EU 1995 and Council of Europe 2001). Differences between 'efficiency' principles and 'surveillance limitation' principles are also important. The standards for assessment of effective enforcement mechanisms in a data privacy law are more difficult to determine. After considering the possible sources of such standards, the conclusion reached is that an approach based on 'responsive regulation' theories is the most useful.

Keywords: data protection, privacy, Asia, responsive regulation, standards, principles

1. Standards by which to assess a country's data privacy protections

Part II of this book aims to both describe and assess critically the data protection (data privacy) laws of the countries in Asia. Part III aims to make comparisons between them. It is therefore necessary to consider standards against which national data privacy laws can reasonably be assessed. Three types of comparisons, and thus standards, are necessary, considered here in the following order:

(i) *Contextual protections*—What types of privacy protections arising from aspects of a country's laws (other than specialized data privacy legislation) require consideration?
(ii) *Privacy principles*—What are the standards for comparison of sets of data privacy principles?
(iii) *Effective enforcement*—What are the standards for effective enforcement mechanisms in a data privacy law?

In Europe this is a more straightforward exercise than in Asia. A generally supportive and consistent context comes from European instruments such as the European Convention on Human Rights, and corresponding institutions such as its Court. While it is possible to argue about whether the standards set by the European Union Data Protection Directive, or Council of Europe (CoE) Convention 108 (and its Additional Protocol) can be improved, they nevertheless provide standards of both the second and third type, **(p.52)** standards to which national data privacy protections in Europe must comply and against which they may be assessed. However, in Asia there are no such regional (or sub-regional)

instruments providing guidance for such an assessment, so standards must be derived from a variety of international sources (including those used in Europe) as well as from first principle considerations of what privacy laws should achieve.

1.1. What is a 'data privacy law'?

All European countries except Turkey have data privacy laws that are required under European agreements. These laws must comply with the standards set by them, so the question of what is a data privacy law arises rarely. In Asia there are no such legal requirements (see Chapter 2), and it is a non-trivial question to ask at what point do a country's privacy protections (including non-statutory protections, sectoral laws etc.) amount to a 'data privacy law'. Part of the discourse on privacy protection since the 1980s has been to talk about how many countries have a 'data protection law' ('data privacy law'). It is valuable to have such a definition or standard (while accepting that any such binary distinction is to some extent arbitrary), so as to make meaningful comparisons between laws that so qualify (and are therefore *prima facie* similar); to measure the global or regional trajectories of their development; and to measure the implementation of international agreements. There is no settled academic or official consensus on the minimum standards required for a 'data privacy law'. I have proposed[1] as a brief definition, that a country[2] has a data privacy law[3] if it has legislation of 'comprehensive' national scope,[4] which provides a set of minimum data privacy principles,[5] to a standard at least approximating the minimum provided for by the international agreements of the early 1980s,[6] plus some methods of officially backed enforcement. The effectiveness of such laws is a separate matter. In this book the expression 'data privacy law' is used in this sense, and the laws of at least 10 Asian jurisdictions meet these criteria. Some important and quite general laws, falling slightly short of this definition, are also given detailed consideration, particularly in China, Indonesia, and Vietnam. Use of this definition shows that, as at the end of 2013, 101 countries around the world have data privacy laws.[7]

2. Assessing the legal context of a data privacy law

While the focus of this book is on specialized data privacy legislation, the effectiveness of data privacy protection in a country may depend to a significant degree on the legal context for protection of such rights. Consideration and comparison of the other main elements **(p.53)** influencing the effectiveness of privacy protection within a country must at least involve these six elements:

(i) Constitutional protection—Does the country's constitution expressly or impliedly provide protection to privacy? Beyond a simple 'yes' many subsidiary questions arise: how explicit, and how qualified is the protection; does the protection extend horizontally (to private sector actors), or is it only vertical (against the state); can constitutional protections be used to found an action, or only to invalidate legislation or state actions, or neither?
(ii) Treaty protection—Is the country a party to treaties that protect privacy? If so, will a ratified treaty become part of the domestic law of the country without further enactment? In Asia at present, the only possibly relevant treaty is the International Covenant on Civil and Political Rights 1966 (ICCPR). So the question is, whether the country is a party to the Optional Protocol to the ICCPR.
(iii) Human rights institutions—Does the country have human rights laws and institutions that may encompass privacy protection within their wider remit, and do they do so?
(iv) Civil law protection—Does the country's Civil Code, or its interpretation of the common law and equity, give any general protection to privacy interests?
(v) Criminal law and administrative laws—Do the country's criminal laws provide any general protection to privacy interests? Can breaches lead to civil remedies?
(vi) Self-regulation—Is there full self-regulation in relation to data privacy in such forms as voluntary industry codes or trustmark schemes? More common are industry codes, complaint resolution bodies, and trustmarks which are supported by and inter related with data privacy legislation (co-regulation).

All of these forms of protection, except self-regulation, are found in numerous Asian jurisdictions, and are important supplements to specialized data privacy laws. They are discussed in relation to each country in Asia in Part II, and compared in Chapter 17, section 2.

3. Standards for data privacy principles

Data privacy principles have been evolving for over 40 years since the first national data privacy laws in the early 1970s.[8] This evolution can be traced through the changing content of international data privacy agreements, and also in the content of national data privacy laws enacted across the globe.[9] The OECD Privacy Guidelines (1980)[10] (the 'OECD Guidelines') and the contemporaneous first version of the Council of Europe (CoE) Data Protection Convention 108 (1981)[11] ('CoE Convention 108') set modest but arguably reasonable standards for the 1980s. Most of the content of this minimum 'first generation' standard was adopted by the Asia-Pacific Economic Cooperation (APEC) Privacy **(p.54)** Framework (2004)[12] (the 'APEC Framework'). The European Union (EU) Data Protection Directive (1995)[13] (the 'EU Directive'), and the CoE Convention 108 Additional Protocol (2001)[14] (the 'CoE Protocol'), which brought CoE standards to approximate parity with the EU Directive, set a new and higher 'second generation' 'European standard' appropriate for a pre-Internet 1990s.

In order to explain the difference between these two levels of standards, it is first necessary to identify and differentiate (i) those elements which are common to all four instruments, and (ii) those elements which are found in the EU Directive (and generally in CoE Convention 108 plus CoE Protocol) but are not required by the OECD Guidelines or the APEC Framework. The difference between the two is the 'second generation' or 'European' principles, namely those elements that they do not share with the 'first generation' or 'minimum' principles.

3.1. 'Minimum' or first generation principles (OECD 1980 and CoE 1981)

The core of the OECD Guidelines are the eight 'basic principles of national application' in Part Two (principles 7 to 14). CoE Convention 108 included eight 'basic principles for data protection' in Chapter II, including all the OECD principles, plus others which anticipated the later 'European' principles.[15] The eight principles that they hold in common are set out below, with the title (as in the OECD Guidelines), followed by a summary of the principle and where it is found in each, with the full OECD wording footnoted.

1. *Collection limitation principle*—limited, lawful, and by fair means; with consent or knowledge (OECD 7; CoE 5(c), (d)).[16]
2. *Data quality principle*—relevant, accurate, up-to-date (OECD 8; CoE 5(a)).[17]
3. *Purpose specification principle*—at time of collection (OECD 9; CoE 5).[18]
4. *Use limitation principle*—uses and disclosures limited to purposes specified or compatible (OECD 10; CoE 5(b)).[19]
5. *Security safeguards principle*—through reasonable safeguards (OECD 11; CoE 7).[20]
6. *Openness principle*—concerning personal data practices (OECD 12; CoE 8(a)).[21]

(p.55) 7. *Individual participation principle*—individual rights of access and correction (Access: OECD 13; CoE 8(b); Correction: OECD 13; CoE 8(c), (d)).[22]

8. *Accountability principle*—data controllers accountable for implementation (OECD 14; CoE 8).[23]

Some of these principles can be broken down into sub-principles, giving a longer list than eight, such as the Individual Participation Principle, which can be divided into access and correction principles. It can also be argued that there is a principle of notice of purpose and rights at the time of collection implied by both the OECD Guidelines and the CoE Convention 108.[24] This gives 10 shared principles, and they can readily be broken down further to enable more precise comparisons, as is done in Chapter 17. These shared principles (whether 8, 10, or 15) were also included, with minor variations, in both the EU Directive and the APEC Framework. They can therefore be described as the 'minimum' principles common to all four international instruments (EU, CoE, OECD, and APEC).

The adoption of 'minimum' principles in national legislation

These minimum privacy standards are now universally accepted as part of any full 'data privacy law'. With only minor exceptions,[25] these elements (expressed in various ways) are always found in what is now over 100 national data privacy laws (plus many sub-national laws), nearly half of which are from outside Europe.[26] It is therefore reasonable to say that the joint influence of all of these international instruments in fashioning this 'common core' has been the single strongest influence on the content of data privacy laws around the world. These laws have a 'family resemblance' because of this joint influence. Historically, it was the simultaneous development of these elements in the OECD Guidelines and CoE Convention 108 that had the greatest causal effect on the shape of this family of laws, with the EU Directive subsequently borrowing from CoE Convention 108, and the APEC Framework subsequently borrowing from the OECD Guidelines. Perhaps common technological problems have been most significant in creating the need for some legal response, but these agreements have then shaped the form and content of that response (discussed further in Chapter 20, section 3.3).

3.2. 'European' or second generation principles (EU Directive 1995 and CoE Convention 2001)

From the early 1990s until its adoption in 1995, an extended set of principles were developed for the EU Directive,[27] but they were based on, and incorporated, the minimum principles **(p.56)** described above, plus some additional elements already found in CoE Convention 108. This occurred prior to the extensive use of the Internet by business, government, or consumers (from 1995), and therefore can be regarded as a 'pre-Internet' development. Then in 2001 it was the turn of the CoE Convention to adopt, via its Additional Protocol,[28] some further principles from the EU Directive, particularly the requirement to limit data exports. The following list[29] of the most significant differences in relation to privacy principles (or 'content principles') between these European instruments and the 'minimum' OECD/APEC instruments (informed in part by Bygrave[30]) is not comprehensive[31] but is sufficient to demonstrate the higher, stricter standards embodied by one or both of the EU Directive and the CoE Convention plus CoE Protocol.

None of the following eight elements is required, or even recommended, by the OECD Guidelines or APEC Framework. They are therefore eight 'European' principles that may be found in national privacy laws (10 including two enforcement principles):

1. *Data export restrictions based on destination*—Requirement of restrictions on personal data exports to countries which did not have a sufficient standard of privacy protection (defined as 'adequate') (EU Directive and CoE Convention 108).
2. *Minimal collection*—Collection must be the minimum necessary for the purpose of collection, not simply 'limited' (both EU Directive and CoE Convention 108).
3. *'Fair and lawful processing'*—A general requirement of 'fair and lawful processing' (not just collection) (both EU Directive and CoE Convention 108). Where a law outside Europe adopts the terminology of 'fair processing' and a structure based on other obligations being instances of fair processing, this is both indicative of influence by the Directive, and makes it easier for the law to be interpreted in a way which is consistent with the Directive.
4. *'Prior checking'*—Personal data systems which raise potentially high levels of risk should be identified and examined before they operate (EU Directive only).
5. *Deletion*—Destruction or anonymization of personal data after the purposes for which it is held are completed (both EU Directive and CoE Convention 108).
6. *Sensitive data protections*—Additional protections for particular categories of sensitive data (both EU Directive and Convention 108).
7. *Automated processing controls*—Data controllers should ensure that automated decision-making which significantly affects data subject is subject to human checking, and data subjects should be able to know the logic of such automated data processing (EU Directive only).
8. *Direct marketing opt-out*—Requirement to provide 'opt-out' of direct marketing uses of personal data (EU Directive only).

(p.57) They can therefore be described as 'European standards' in privacy principles.[32] In other words, the key additions to the two European instruments, the main differences between them and the OECD and APEC instruments, constitute the 'European' or 'second generation' privacy principles. Other international instruments are not significant in comparison, but the Commissioners' 'Madrid Resolution' (International Conference of Data Protection and Privacy Commissioners (ICDPPC), 2009, see Chapter 2, section 6.1) is largely consistent with these standards, and even the early UN Guidelines (1990) went beyond the 'first generation' minimum principles and included principles concerning deletion and sensitive data (see Chapter 2, section 3.5).

The adoption of 'European' principles in national legislation globally

These additional 'European' or 'second generation' data privacy principles have been adopted by all of the countries of the EU and by almost all of the non-EU countries of Europe which are members of the CoE. In addition, they have been adopted by many of the countries outside Europe that have enacted data privacy laws. Analysis of 39 countries outside Europe with data protection laws as at December 2011, showed that the 10, stricter, 'European' principles had been substantially incorporated into 33 of these non-European laws. On average they included seven out of the 10 principles.[33] Some of these additional 'European' principles occurred in more than 75 per cent of the 33 countries assessed, namely 'destination-based' data export restrictions (28/33); additional protection for sensitive data (28/33); deletion requirements (28/33); minimum collection (26/33); and two enforcement-related principles discussed in the following section. By the end of 2013 the number of non-European laws had increased to 46,[34] and these new laws seem to be at least as strong as those of previous decades. In addition, many existing laws are being strengthened to keep up with rising expectations of privacy protection, international agreements, and the examples set by other countries, and in the process these laws are becoming 'more European'.

The result is that there are at least 16 data privacy principles (8 'minimum' and 8 'European') derived from international agreements, that have become, to varying extents, standards, adopted in the overwhelming majority of data protection laws enacted globally. As such, they are a reasonable basis against which to compare the principles included in laws or proposed laws in Asian countries. Furthermore, we can compare laws on the basis of whether they only implement the first generation 'minimum' standard, whether they implement the second generation

'European' standard, or whether they implement something in between.

In some cases the question is whether Asian data privacy laws implement something even stronger than the second generation 'European' principles. The evolution of privacy principles has not stopped, except for the OECD and APEC standards. As discussed in Chapter 19, both European instruments are continuing to develop stronger principles.[35] Development of new principles in national laws across the globe also continues, including **(p.58)** in Asia, as discussed in Chapter 17. Development of most of these new 'content principles' has been spurred by Internet-related developments which had not happened when the second generation principles were drafted, so it may be appropriate to call them 'Internet principles' when their content becomes clear.

The principles required for 'adequacy'

The EU Article 29 Working Party's interpretation of what privacy principles must be implemented before a non-EU country's law can be regarded as 'adequate' in relation to the EU Directive[36] is an influential statement of standards for privacy principles, and is not exactly the same as the 'European' standards discussed in this chapter. The Article 29 Working Party criteria stress that a law should always include the following (stated briefly in the words of the Opinions): the purpose limitation principle; the data quality and proportionality principle; the transparency principle; the security principle; the rights of access, rectification, and opposition; and restrictions on onward transfers. There should also be additional principles for specific types of processing, namely sensitive data, direct marketing and automated individual decisions.

The lack of adoption of the three APEC principles—no 'APEC standard'

Compared with the widespread influence of the distinctive aspects of the 'European' principles, the three distinctive APEC principles have gained little traction (as set out in Chapter 2, section 3.3), except to some extent in relation to 'accountability' for data exports, which is discussed in the following section. However, data exports aside, it cannot be said that the APEC Privacy Framework represents an alternative standard to the existing 'minimum' and 'European' standards.

3.3. International data transfers—the most contested standards

One of the most-implemented 'European' principles outside Europe is 'Data export restrictions based on destination', which could also be named the 'adequacy requirement' for data exports. It is also clearly the most controversial privacy principle, and the only one on which there is a degree of direct conflict between international standards.

It is commonplace, not controversial, for international data privacy agreements to require free flow of personal information to other countries, but this is only ever required in specified circumstances. The OECD Guidelines require that member countries do not impede the free flow of personal information to other OECD countries that do 'substantially observe' the Guidelines. The CoE Convention 108 does similarly in relation to member states of the Convention. The EU Directive requires free flow of personal information to other EU countries, on the basis that they are all required to implement the standards of the Directive in their national laws. This is the positive aspect of international data transfer requirements. The APEC Framework is alone in having no such requirement.

(p.59) The more significant differences arise in the approaches in these agreements to restrictions on data exports:

(i) The OECD Guidelines explicitly set out three situations when data export restrictions were *allowed*,[37] restrictions based on the state of the law of the importing country (including that it does not 'substantially observe' the OECD standards).
(ii) The EU Directive's novel development was that it also *required* member countries to prohibit personal data exports to non-EU countries unless the standards required by the Directive for personal data exports were met. The only standard applying to a country as a whole is the 'adequacy' standard under Article 25 of the Directive (see Chapter 2, section 3.2). Other provisions in the Directive allowing exports require assessment of the exports on a transaction-by-transaction basis, under Article 26, or the use of binding corporate rules or standard contract clauses. The CoE Protocol added similar 'adequacy' requirements (using that term) to CoE Convention 108.
(iii) APEC's Privacy Framework 'accountability' principle IX (see Chapter 2, section 3.3) impliedly allows data exports to any country, requiring only that the exporter will 'exercise due diligence and take reasonable steps to ensure that the recipient…will protect the information consistently with these Principles'. If due diligence is exercised, no further liability is imposed on the exporter. The 2013 OECD Guidelines change the Guidelines in the direction of the APEC Framework, but considerable ambiguity remains (see Chapter 19, section 3.1).

There is, therefore, a conflict between the 'European standard' (the EU Directive and CoE Convention 108 plus Protocol) and the APEC Framework standard which has departed from the 1981 'minimum standard' (with the 2013 OECD Guidelines being similar but ambiguous). Other sources of international standards allow restrictions on data exports similar to the OECD Guidelines: the UN Guidelines (see Chapter 2, section 3.5) allow restrictions if 'there are no reciprocal safeguards'; and the ICDPPC 'Madrid Resolution' (see Chapter 2, section 6.1) is closer to the European standard in providing that transfers 'may be carried out' where the state of the destination 'affords, as a minimum, the level of protection' in the Resolution (and specifying other modes of exception). The APEC Framework is alone in not recognizing any legitimacy in destination-based restrictions on transfers.

There is a very large literature arguing about what standards for restrictions on data exports are justifiable or will have the greatest utility, and it is beyond the scope of this work to make a fundamental contribution to that debate. Kuner provides the most comprehensive analysis[38] of the issue, and concludes that the situation of international data flow regulation is and will continue to be one of 'legal pluralism', where 'there is no over-riding top level norm' which can resolve disputes. No single international agreement is likely to be agreed (or imposed) to produce a complete solution, so incremental answers will continue to develop through negotiations and politics.[39] Kuner puts forward seven 'suggestions for an improved regulatory framework', the normative basis of which is to reject a geographical basis (like 'adequacy') for restrictions, in favour of an 'organisational approach' (of which **(p.60)** binding corporate rules would be an example). He proposes elements of a model law on such a basis, supported by a 'mutual recognition' between states. Kuner is sensitive to the fact that such approaches need to improve protection to data subjects, and makes proposals to that effect,[40] but they stop short of full legal liability on exporting data controllers. His proposals are a valuable basis, not necessarily for the purposes of adoption, but as a means of providing a basis for more sophisticated critiques of existing or proposed laws.

Analysis of regulation of international data flows

Regulation of international flows of personal data is not only about data export restrictions, it is a complex of interrelated issues, some of which also affect purely domestic processing of personal data. Four issues require consideration, only the first of which is the standard 'data export

restrictions' issue:

(i) Under what conditions are data exports to a foreign jurisdiction allowed?
(ii) Does the law of the controller's jurisdiction assert extraterritorial operation? (including related issues of applicable law).[41]
(iii) Can the data subject enforce a contract against the recipient of exported data? (including issues of privity of contract doctrines).
(iv) Are there special rules for controller-to-processor transfers? (including whether the controller has vicarious liability liable for breaches by a foreign processor).

These issues are not dealt with directly by the first and second generation privacy standards, except that the EU Directive and the laws that have developed under it do provide some widely used responses to issue (i). The ways in which various data privacy laws in Asia deal with these issues is compared in Chapter 17.

Another question which must be asked when a foreign-based processor imports personal data into a country for processing, is whether the processor jurisdiction's law exempts outsourced processing (in full or part)? If there is such an 'outsourcing exemption' to a country's data privacy law, this will presumably have a negative impact on the country's law being assessed as 'adequate' by the EU (see section 3.2, Chapter 2), because it will deny protection to Europeans whose personal data is sent to the Asian country concerned for processing.

3.4. 'Efficiency' principles vs surveillance limitation principles

A more critical and political view of privacy principles looks at them from the perspective of what effect they have on the operation and expansion of information surveillance systems. Privacy principles can be divided into 'efficiency' principles, which help make information systems operate more fairly in the interests of both data controllers and data subjects, and 'surveillance limitation principles' which go beyond 'efficiency' and limit the surveillance capacity of information systems in ways that are not necessarily in the commercial or administrative interests of data controllers. By adopting this approach, the disputes over privacy laws and policy since the 1980s have been mainly about how strong the surveillance limitation aspects of privacy laws should be made.

(p.61) This approach originates with Rule and colleagues, writing in 1980 before the 'minimum' privacy principles were crystallized by the OECD Guidelines and CoE Convention 108. They identified the 'official response' to data privacy problems, from the US Fair Credit Reporting Act of 1970 onwards through US and early European laws, as 'the efficiency criterion'—in other words, the view that privacy protection is satisfied by laws and principles that ensure the 'efficiency' of surveillance systems:[42]

> By this ['efficiency'] criterion, surveillance is considered acceptable provided that four conditions are met: *first*, that personal data are kept accurate, complete, and up to date; *second*, that openly promulgated rules of 'due process' govern the workings of data systems, including the decision-making based on the data; *third*, that organisations collect and use personal data only as necessary to obtain 'legitimate' organisational goals; *fourth*, that the persons described in the data files have the right to attest adherence to these principles.

In these early sets of 'fair information principles', the only limits on collection and use of personal data are 'legitimate' (or lawful) organizational goals, not goals limited by the purpose for which the information is collected. As Rule and colleagues conclude, these 'efficiency' provisions are a most opportune definition of 'privacy protection' if you are an organization interested in surveillance:

> By these criteria, organisations can claim to protect the privacy of those with whom they deal, even as they demand more and more data from them, and accumulate ever more power over their lives.

However, the OECD Guidelines and contemporaneous CoE Convention 108 of 1980/81, all subsequent international agreements, and almost all of the 101 national laws to 2013, have added one other vitally important ingredient that goes beyond 'efficiency': the requirement that organizations may only use or disclose the personal information they collect for the purpose for which they collected it, with defined exceptions (of very varying breadth in different laws and agreements). This 'finality' limitation, as it is sometimes called, goes beyond 'efficiency': if enforced it means that organizations cannot change their minds about the uses they (or others) wish to make of personal information, after the event of collection. This is a significant limitation on the surveillance capacity of organizations. However, it is only of significance if organizations are required to narrowly define the purpose of collection in the first place, and then restrict their collection of data by that defined purpose. Otherwise, by planning ahead, they can avoid problems that 'finality' may cause. One of the most significant threads in the post-1980 history of data privacy laws has been a series of disputes and divergences over how tightly limitation on collection, use, and disclosure should be tied to the original purposes of collection.

These questions are still fundamental after 30 years, and still asked too infrequently: to what extent do and should data privacy principles and laws go beyond attempting to ensure the 'efficiency' of personal information systems, and provide means to limit and control the expansion of surveillance systems?[43]

(p.62) Of the eight minimum principles embodied in the international agreements of the early 1980s (see section 3.1 of this chapter), five are 'efficiency' criteria: data quality; security safeguards; openness; individual participation; and accountability. The collection limitation, purpose specification, and use limitation principles, mild as they were in allowing 'compatible' uses and disclosures, and only placing unspecified limits on collection and vague requirements of notice and consent, nevertheless introduced the essential elements of 'finality', based on initial purpose of collection. These 'finality' concepts continue to place limits on the expanded re-use of already collected information, and the development of new surveillance systems. They can be considered to be the 'surveillance limitation' elements of the minimum principles.

These 'surveillance limitation principles' were expanded by the subsequent 'European' principles[44] added by the EU Directive and the CoE Additional Protocol (see section 3.2 of this chapter) in 1995–2001. All eight of the European principles embody 'surveillance limitation' rather than 'efficiency' criteria. Of these, minimal collection, deletion, and data export limitations based on destination, are the most significant surveillance limitation principles, because they extend 'finality'.

4. Standards for enforcement mechanisms, and 'responsive regulation'

It is more difficult to determine standards for appropriate or sufficient enforcement of a data privacy regime than to describe standards for the privacy principles that such regimes should implement. Nevertheless, some objective standards are needed if the data protection regimes considered in Part II are to be analysed critically, and then compared in Part III.

A distinction needed at the outset is between compliance and enforcement. In Part II, the available evidence of enforcement of national laws is considered, including statistics and case studies (both formal decisions and complaint summaries). The extent of compliance with each law (as distinct from enforcement of it) by companies or agencies is a different matter, and generally little or no information is available because few sociological studies of compliance are done. The limits of this book will generally be the consideration of the extent of enforcement, not the extent of compliance.

Two broad approaches to enforcement standards can be taken. The first is to look for internationally accepted standards specific to privacy enforcement, from such sources as international agreements, peer-determined standards set by organizations of data protection authorities (DPAs), or suggestions made by expert commentators. The second is to consider the more general standards by which regulatory regimes are assessed, of which the most relevant to data privacy enforcement is 'responsive regulation' theory.

4.1. International standards for data privacy enforcement mechanisms

This section will consider what international instruments provide; what data protection Commissioners recommend; and what leading authors propose.

Standards required by international data protection instruments

International data privacy agreements embodying only the 'minimum' privacy standards have little or nothing of value to say about standards for enforcement. The OECD privacy **(p.63)** Guidelines are non-prescriptive in relation to enforcement, encouraging both legislation and self-regulation, 'reasonable means' for individuals to exercise their rights, 'adequate sanctions and remedies', and no unfair discrimination against data subjects.[45] CoE Convention 108 in 1981 only required that state parties provide 'appropriate sanctions and remedies' (although its Additional Protocol in 2001 requires more, to align it with the EU Directive). The APEC Privacy Framework is equally non-prescriptive,[46] and does not require any particular means of implementation of the Privacy Principles, stating instead that the means of implementing the Framework may differ between countries, and may be different for different principles, but with an overall goal of compatibility between countries. Under the APEC Framework, anything ranging from complete self-regulation unsupported by legislation, through to legislation-based national privacy agencies, is acceptable.[47]

The instruments embodying 'European standards' do include some enforcement standards. CoE Convention 108's Additional Protocol requires one or more supervisory authorities which must function in 'complete independence' (DPAs), and their decisions must be able to be appealed to the courts. They must have powers to hear complaints; investigate and intervene; to engage in legal proceedings or bring matters to the attention of the courts; and to cooperate with other supervisory authorities. The EU Data Protection Directive requires all of CoE Convention 108's enforcement measures, plus additions. Data subjects must have a 'judicial remedy', and be able to obtain compensation for damage. The supervisory authority must be able to carry out prior checking of processing posing particular risks, and to keep a register of notified processing. These European requirements are the most concrete enforcement requirements in international agreements, but are not shared with the OECD and APEC agreements. Both European instruments may strengthen in future.[48] Despite the lack of direction from the OECD and APEC instruments, the study of 33 non-European data privacy laws as at 2010 mentioned previously (see section 3.2 above) showed that those laws provided for recourse to the courts in 26/33 laws, and for a specialist data protection agency in 25/33 laws.[49] Requirement for availability of compensation payments, or for rights of appeal against DPA decisions, were not measured, and possibly may have been less frequently found.

The EU Article 29 Working Party's interpretation of what types of enforcement mechanisms and levels of effectiveness constitute 'adequate' enforcement in relation to the EU Data Protection Directive[50] is another influential statement of enforcement **(p.64)** standards. The requirements can be summarized as follows (with quotations from the 1998 Opinion):[51]

> (i) *Delivery of a 'good level of compliance'* with the content rules (data protection principles): 'A good system is generally characterised by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them. The existence of effective and dissuasive sanctions can play an important [role] in ensuring respect for rules, as of course can systems of direct verification by authorities, auditors, or independent data protection officials.'
> (ii) Provision of *support and help to individual data subjects* in the exercise of their rights: 'The individual must be able to enforce his/her rights rapidly and effectively, and without prohibitive cost. To do so there must be some sort of institutional mechanism allowing independent investigation of complaints.'
> (iii) Provision of *appropriate redress* to the injured party where rules are not complied with: 'This is a key element which must involve a system of independent adjudication or arbitration which allows compensation to be paid and sanctions imposed where appropriate.'

This approach focuses on the results to be achieved, not on particular enforcement mechanisms. This makes good sense, because of the wide varieties of legal systems, national legal cultures, and levels of economic and technical development in the countries to which it is addressed, which make it unrealistic to consider that mechanisms regarded as necessary in European countries are necessarily appropriate. The approach of the Article 29 Working Party is in many ways consistent with the 'responsive regulation' approach discussed later in this chapter.

We can conclude that standards derived from international data privacy instruments are far less precise in relation to data privacy enforcement than they are in relation to data privacy principles, but there is once again a higher 'European' standard with more precision.

Standards proposed by DPAs collectively

The ICDPPC in 2009 made the Madrid Resolution,[52] Part VI of which, on 'Compliance and Monitoring', proposed that data privacy laws should include numerous measures under a categorization which can be summarized as follows:

> (i) Encouragement through domestic law of *proactive measures* by data controllers—procedures to prevent and detect breaches; data protection officers; training programmes; audits; design of information systems; privacy impact assessments; binding codes of conduct with measures of compliance; and response plans in the event of breaches.
> (ii) *Monitoring* by independent supervisory authorities—powers to investigate and intervene to ensure compliance; judicial oversight of administrative remedies (such as DPA decisions); and direct recourse to the courts by data subjects.
> **(p.65)** (iii) *Cooperation and coordination* between supervisory authorities nationally and internationally.
> (iv) *Liability* of data controllers for pecuniary and non-pecuniary damage caused by breaches (unless the data controller can demonstrate the liability cannot be attributed to him)—data subject to have legal rights to seek such compensation; and liability to be without prejudice to any penal, civil, or administrative penalties provided.

This collective proposal by DPAs deserves attention as 'peer review' of the compliance and enforcement provisions that a data privacy law should contain. It unambiguously states that a right to seek compensation should exist, and that both direct recourse to the courts and a right of appeal against DPA decisions should be provided. However, it does not specify what mix of compensation, compliance orders, civil/administrative penalties, or criminal/penal provisions should be provided, or say anything about the role of publicity (transparency) in relation to breaches and remedies.

Standards suggested by commentators

Most leading authors in the field of data privacy have given only limited consideration to the question of the desirable standard for enforcement mechanisms in a data privacy law. Kuner[53] does not provide any general theory of what constitutes effective enforcement, but does provide many examples of enforcement actions by DPAs and courts in European jurisdictions, which he classifies under the headings of (i) order to take action or not to take action (i.e. injunctive relief), (ii) audits and inspections, (iii) fines, and (iv) criminal penalties. He does not mention payment of compensation, although one of his examples includes such payments (in Denmark). Bygrave[54] does not categorize 'sanctions and remedies', but in his discussion of them mentions compensation (noting the Directive's requirements), 'judicial remedy' (as required by the Directive), appeals against DPA actions, class complaints (mainly in reference to Hong Kong and Australia), and the importance of 'public disclosure' (but without mention of complaint reporting).

Bennett and Raab give the most detailed analysis,[55] starting from the 'major problem that there exists no satisfactory way of evaluating or measuring the approximation of regulatory laws and mechanisms to the goal of protecting privacy'.[56] They discuss many different approaches to measuring the achievement of the goals of privacy protection, and of the performance of privacy regulators, and the considerable difficulties they all involve, particularly if there is overreliance on empirical measures. In particular, they caution about the dangers of confusing output indicators (such as the number of complaints an agency investigates each year) with measures of outcomes indicating greater privacy protection. Their conclusion is that it is necessary to focus on 'the data protection system as a whole' 'as a system of interacting parts', and not isolated components of it. They stress the interdependence of factors such as public awareness of privacy rights, remedies and dangers; the extent to which privacy regulators publicize their work; the extent to which the data privacy legislation enables a regulator to be effective; and the extent to which data **(p.66)** controllers are assisted in their efforts to comply. Clearly, they are not evaluating a law on paper only, but including all matters associated with enforcing it and encouraging compliance with it. Without suggesting any recipe, they say 'a highly efficacious data protection system would comprise' (in summary): a strong law; an assertive regulatory authority; data controllers committed to compliance; market incentives to comply; a vigilant and activist citizenry; and use of privacy-enhancing technologies.[57] The result is 'a process that involves organizational change and learning, and that involves an elaborate implementation network of persons and organizations engaged in the collaborative, albeit often conflictual, production of data protection'.[58] The complexity of this process is such as to make overall 'performance measurement' so difficult that 'the only reliable subjects for evaluation seem to be procedural, involving rules, codes, sanctions and decisions that may lead to protection of privacy but do not themselves represent privacy as such':[59] proxies for privacy, so to speak. They are right that this is a matter of measuring outputs, not outcomes (privacy), but some proxies are closer to 'the real thing' than others, although usually only *ex post facto*. The amounts of compensation paid; employment or credit restored; apologies published; and invasive systems or processes that are terminated.

There is one enforcement mechanism that Bennett and Raab definitely support: they regard the existence of a DPA as 'the sine qua non of good privacy protection inasmuch as laws are not self-implementing and the culture of privacy cannot securely establish itself without an authoritative champion'.[60] They classify DPA functions as ombudsmen, auditors, consultants, educators, negotiators, policy advisers, and enforcers, but do not attempt to enumerate what DPA powers are desirable for optimal enforcement.

Conclusions

Consensus on how to measure effective enforcement of data privacy principles, and therefore provide a standard against which privacy laws and authorities can be measured (or, more optimistically, aim to achieve) is clearly more elusive than stating the competing standards for data privacy principles. However, considered broadly, the systemic approach proposed by Bennett and Raab and the approach of the Article 29 Working Party are quite consistent. There is also a high level of consensus, though not universal agreement, that such a 'data protection system' at least requires a dedicated DPA, and the rights of individuals to obtain compensation for breaches and to bring matters before a court if they need to.

These approaches are very valuable, but they do not tell us what interrelationships between the components of a 'data protection system' are necessary for the internal dynamics to be effective. Bennett and Raab give some examples of the interactions that are needed, but not how to achieve them. In my view, the theory of 'responsive regulation' is best able to explain key elements of how the necessary dynamic can be achieved.

4.2. Responsive regulation theory and data privacy regulation

The theory of 'responsive regulation' provides one of the best ways to describe the complexity of the relationships between achievement of objectives and provision and use of appropriate enforcement mechanism. In doing so, it also (in effect) recommends how **(p.67)** regulators can best use the powers they have, in order to achieve their regulatory objectives. Ayres and Braithwaite first encapsulated in 1992[61] the best-known element of what has come to be known as responsive regulation theory, the centrality of a hierarchy of sanctions:[62]

> it is contended that the achievement of regulatory objectives is more likely when agencies display both a hierarchy of sanctions and a hierarchy of regulatory strategies of varying degrees of interventionism. The regulatory design requirement we describe is for agencies to display two enforcement pyramids with a range of interventions of every-increasing intrusiveness (matched by ever-decreasing frequency of use). Regulators will do best by indicating a willingness to escalate intervention up those pyramids or to deregulate down the pyramids in response to the industry's performance in securing regulatory objectives.
>
> Finally, it is argued that the greater the heights of tough enforcement to which the agency can escalate (at the apex of its enforcement pyramid), the more effective the agency will be at securing compliance and the less likely that it will have to resort to tough enforcement. Regulatory agencies will be able to speak more softly when they are perceived as carrying big sticks.

In fact responsive regulation has always involved much more than a pyramid of sanctions, and in more recent work[63] Braithwaite has stressed that there is both a pyramid of sanctions, and a pyramid of supports, as illustrated in Figure 3.1.[64]

The theory posits that regulators should prioritize the pyramid of supports as the least costly way of achieving large-scale regulatory compliance,

and only 'when that fails to solve specific problems sufficiently, the regulator moves to the right…and starts to move up a pyramid of sanctions'.[65]

Braithwaite also stresses that responsive regulation contains a 'storytelling orientation' where stories about the implementation of each level of the enforcement pyramid—both successes and failures—are made known to the various classes of stakeholders in the regulatory system. These include those who are regulated, the intended beneficiaries of this, and those responsible for assessing its effectiveness. Braithwaite says[66] that one test of responsive regulation is how good a system is in 'bubbling up' stories of its successes and failures, provided these stories have credibility as being representative, and that this applies to privacy regulation. Use of each level of sanction must be visible to those regulated, and to consumers or citizens affected by privacy breaches. Publication of details of decisions and other enforcement activities by regulators is therefore essential for responsive regulation to occur. In this book, this is referred to as part of the transparency element of enforcement.

Applying responsive regulation theory to data privacy regulation

There are many elements of responsive regulation theory,[67] only some of which are of direct relevance to privacy regulation. Some very basic elements of the theory (trivial to those familiar with it, but worth stating for those not so familiar) which focus only on the sanctions pyramid, can be summarized in five propositions: **(p.68)**

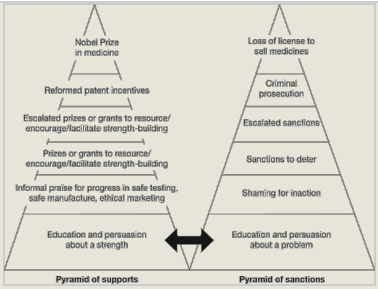


Figure 3.1 Pyramids of supports and sanctions being developed in John Braithwaite's current work on the regulation of medicines, with Graham Dukes and James Maloney.

1. Effective regulation requires *multiple types of sanctions* of escalating seriousness.
2. It is an enforcement *pyramid*: sanctions at the top get used far less than the cheaper bottom layers.
3. All forms of sanctions must be *actually used* when necessary, for credibility to be retained.
4. Use of each level of sanction must be *visible* to those regulated, consumers and the representatives of both.
5. The higher levels are *incentives* for those who are regulated to make the lower levels work.

In summary, responsive regulation theory posits a pyramid or hierarchy of enforcement options, credible use of the whole pyramid of options, and various types of transparency and feedback mechanisms. It is readily adapted to the context of data privacy regulation in many respects. However, in the area of data privacy, where all laws are significantly complaint driven, it is necessary to distinguish two pyramids of sanctions, one comprising the reactive sanctions appropriate to responding to complaints (or 'own motion' investigations of individual instances of suspected breaches), and a second pyramid of systemic enforcement sanctions which are not complaint driven. As described further in the next section, it would only cause conceptual and descriptive confusion to combine the two.

Responsive regulation theory, as developed by Ayres and Braithwaite, has received a range of criticisms.[68] In the context of data privacy regulation a relevant criticism is **(p.69)** Kingsford-Smith's argument that 'responsive regulation seems to have been less successful in regulatory environments with large populations of regulatees and insufficient resources for visits, inspections, or other regular checks, and where detection of non-compliance is difficult'.[69] She is discussing regulation of the Australian financial sector (except the prudentially regulated banking and insurance sectors), but her description fits a privacy regulator who is regulating the whole or most of the businesses in the private sector, and often the public sector as well.[70] She argues that 'the regulatory circumstances do not provide the bridge for contact between the regulator and firm, which allows a relationship to develop which supports responsive action'.[71] However, her argument is that the classic approaches of responsive regulation do not work *as well* in these circumstances, not that they do not work at all or that the theory is defective. To say that privacy regulation is difficult and very often marked by its absence and ineffectiveness would surprise no one familiar with the field. Perhaps the lesson to be drawn from Kingsford-Smith's caution is that responsive regulation of a very large population of diverse data controllers will need to emphasize different aspects of the responsive regulation 'toolbox' than would be the case with, say, the regulation of nursing homes, coal mines, or telecommunications providers. In particular, the visibility of the use of sanctions has to be achieved much more actively where there is no tightly knit industry to communicate with, new intermediaries such as Privacy Officers may play a more important role, requirements for 'privacy by design' and 'privacy by default' may reduce the face-to-face regulatory burden and so on. These are familiar debates in relation to data privacy, but putting them into the context of responsive regulation may increase our understanding.

Responsive regulation, standards, and comparisons

The practical benefit for this study is that responsive regulation theory, when applied to privacy regulation (building on Bennett and Raab's approach), provides a number of ways of analysing and comparing the enforcement aspect of laws in Asian countries. First, we can ask in relation to each country whether the range of sanctions (both reactive and systemic) and supports provided by the law, provide a sufficient range of each to make responsive regulation possible, including not only different types but sufficient high upper ends ('big sticks'). Different 'mixes' may achieve this, allowing for the wide differences of legal and administrative traditions between these countries. Second, we can at least compare the track record of each country's regulator in providing the transparency of enforcement which is particularly necessary for data privacy regulation. Third, if there is sufficient transparency in relation to remedial outputs, this may make possible assessment of whether all types (and degrees) of sanctions are being utilized. While these are only proxies for privacy protection, as Bennett and Raab noted, they may be the best measure of evaluation—and comparison—available.

4.3. Pyramids of enforcement mechanisms in use in Asian data privacy laws

It would be possible to construct an enforcement pyramid of ideal and universal enforcement mechanisms, against which Asian data privacy laws could be compared, but its value **(p.70)** would be limited. The approach needed to achieve successful responsive regulation is always context

dependent, and depends upon such factors as the types of industries being regulated, the nature of the principles being enforced, and the resources available to regulators and others given the state of development of the country concerned.[72] To these we can add differences in legal, bureaucratic, and business cultures.

However, a more realistic approach may be to start with the enforcement mechanisms and sanctions already included in the data privacy laws of Asian countries, which would give a regional rather than universal standard of comparison. This is in effect what is done in Chapter 18, and the comparative table of enforcement mechanisms in the 10 most comprehensive current data privacy laws in Asia. If these sanctions (including the gradations of penalties available) are sorted into an approximate order of seriousness of sanctions we obtain a hypothetical 'pyramid of sanctions' found in Asian data privacy laws. These are used in Part II and Chapter 18 to conclude whether particular laws are comparatively strong or weak, in the Asian context, in the range of sanctions that they provide.

The mechanisms through which the objectives of enforcement can be achieved in the field of data privacy,[73] fall into two main categories: reactive measures (responses to individual instances of potential breaches of data privacy principles or legal requirements) and systemic measures (proactive steps aimed at preventing breaches or detecting situations likely to result in breaches). In addition to these separate pyramids of reactive and systemic sanctions, there are positive measures (education and training, information services, awards, etc.) which support those who are trying to comply with the regulatory goals.

Reactive sanctions

In Asia, reactive sanctions have been and still are the primary mechanism by which compliance with data privacy laws has been encouraged. The range of severity of each sanction may vary greatly, say from a US$100 administrative fine to hundreds of thousands of dollars (as in Singapore), sometimes called an escalation model. Taking into account that the same sanction can escalate, a possible pyramid of reactive enforcement sanctions, including only what is possible under at least one current Asian data privacy law, could involve a pyramid of well over 20 steps.[74] Of course, the exact ranking of sanctions by **(p.71)** degree of seriousness can be a matter of reasonable disagreement, and will also vary between countries depending on cultural perceptions. Nevertheless, a very wide range of sanctions is available under the data privacy laws of Asian countries, and an individual country's laws can be considered against what is in use elsewhere.

Systemic sanctions

The preventive and deterrent objectives of enforcement can often be best achieved through systemic mechanisms which are not used in reaction to any single complaint. These can include: registration systems (general, or more often selective); audits and inspections; appointment of data protection officers; design or default requirements in information systems; and privacy impact assessments. Quite a few types of systemic enforcement measures are already in use in Asian jurisdictions (as demonstrated in Chapter 18).[75] Such systemic measures also need to be ranked in rough order of highest cost (and resulting infrequency of application) at the top of the list, with those placed at the bottom being measures where it is possible to spread the cost burden across a wide range of respondents (businesses/agencies). Systemic compliance measures can therefore also be thought of as a pyramid, with the most costly and selectively applied at the top, and those capable of more generic application at the bottom. As with reactive sanctions, the more variety of systemic sanctions a data privacy regulator has at its disposal, the stronger is the potential effectiveness of its enforcement system. Most systemic measures can also be described as 'proactive' measures.

Supportive measures in relation to sanctions

Separate from sanctions are a wide variety of legislative provisions that are not in themselves sanctions but their presence or absence either supports or constrains the effective use of a sanction. Many are currently in use, and these are compared in Chapter 18.[76]

Supportive measures in relation to compliance—incentives

A different form or supportive measure, the importance of which is stressed by Braithwaite and other responsive regulation theorists, is that there are many types of support that regulators can give to those data controllers or processors (or their advisers) who 'wish to do the right thing'. Numerous 'compliance supports' are provided in Asian jurisdictions by DPAs or ministries.[77] Responsive regulation also places a high value on consumers/citizens knowing of their rights and responsibilities in relation to privacy protection, and in various **(p.72)** Asian jurisdictions similar support facilities are sometimes provided for both adults and schoolchildren, including educational materials, prizes and awards, and even television dramatizations about privacy. These measures can also be described as 'incentives' or more colloquially as 'carrots' (as opposed to 'sticks').[78]

Transparency and responsive regulation

Responsive regulation requires transparency in the use of sanctions: use of each level of sanction must be visible to those regulated, consumers, and the representatives of both. Without the right forms of publicity/transparency, in the context of privacy regulation, data controllers/processors and their advisers will not obtain market signals about the costs of non-compliance, and thus will have no incentive to institute steps to improve compliance, or settle complaints of non-compliance in the most non-adversarial manner possible. Also, data subjects, and their advisers, will not get the message that they can utilize data privacy laws to vindicate their rights, and that it may be worthwhile considering privacy litigation. Without transparency, there is unlikely to be effective regulation.

Two types of transparency can be argued to be most useful in relation to achieving these objectives in data privacy regulation: publication of illustrative complaints resolutions by DPAs; and publication of statistics concerning penalties and remedies. In few, if any, jurisdictions are many data privacy conflicts elevated to the level of a court decision, or that of a quasi-judicial tribunal, or even that of the formal enforceable decisions of a regulator (DPA). While the publication of all such decisions at these three levels is essential to transparency, they usually do not exist in sufficient numbers to make it clear how much of the detail of the law is in practice being interpreted, or what remedies (if any) are being received by individual complainants. These matters are hidden in the anonymous resolution of complaints, usually by mediation, carried out by DPAs. These are too numerous (and typically too trivial) for detailed complaint summaries to be worth publishing of all of them, and the cost and administrative burden on the DPA would be unjustifiable. Preparation and publication of a selection of such case summaries is what is needed, sufficient in number to illustrate major interpretations of the legislation by the DPA, and to indicate the typical remedies that may result from a range of complaint types. Some DPAs in Asia achieve this, to a level of 20–30 complaint summaries per year, and with a recommended standard form of citation for their summaries. None have yet taken the further step of making a commitment to establish objective criteria for selection of which complaints to summarize.[79] Such transparency overlaps, but should be distinguished from, the publicizing of breaches by identified respondents ('name and shame') as a sanction in itself. Complaint statistics, usually included in annual reports, often only indicate the subject area of complaints, numbers of complaints received compared with numbers resolved, and 'outcomes' in the sense of the numbers of complaints found justified, dismissed without investigation, etc. However, the most valuable statistics are rarely provided, such as how many complainants

received how much compensation, the numbers of complaints resulting in apologies, or changes to practices, or other remedies. Such statistics can cover the bulk of complaints that do not result in summaries, and can give as good an objective measure of an enforcement system as it is realistic to expect.

(p.73) Conclusion—looking for an appropriate range of sanctions, supports, and transparency

In conclusion, the approach that will be taken throughout this book, and which is proposed as the most realistic and useful way to assess and compare the enforcement aspects of data privacy laws, is an approach emphasizing the need for (i) a wide range of types of enforcement measures, including those enabling data subjects to take independent enforcement action; (ii) a range of possible severity of penalties (from 'slap on the wrist' to 'big stick'); (iii) regulators who demonstrably use all sanctions, and all levels of severity; and (iv) transparency. An effective regulatory system in relation to privacy requires all four dimensions.

4.4. Standards requiring existence and independence of data privacy authorities

There was no requirement for a coordinating supervisory body (let alone an independent one) in the original privacy instruments of the 1980s, and there is also no such requirement in the APEC Framework or the 2013 revised OECD Guidelines. A supervisory body with powers to administer and enforce the data privacy law, separate from the departments or ministries of the State, and with independence from them, was, however, required by the EU Data Protection Directive, and by the Additional Protocol to CoE Convention 108, so this is part of the European standard for data privacy laws. In other words, the European standard is to require both a separate DPA and one that is independent. Globally, the *de facto* standard, in countries that have data privacy laws, is to follow the European requirements. In more than 90 per cent of these countries their data privacy laws include the establishment of a specialized DPA,[80] and in almost all cases a DPA has been appointed.

What is a 'DPA'? This is a question which must be answered before addressing the question of independence, best illustrated by contrast with the model of 'ministry-based enforcement' which is still relatively common in Asia (Japan, Taiwan, China, and India) but rarely found elsewhere. Differences between the two models include: (i) a DPA is able to investigate and report in relation to all possible breaches under a law, not only those in one industry sector; (ii) a DPA does not have the conflicts of interest of also being the general regulator of an industry sector; (iii) a DPA can ensure that the same standards are applied across all industry sectors (and usually, the public sector as well). In some countries (e.g. South Korea) both independent DPAs and ministries have significant enforcement roles, so there is no sharp distinction between the two models. One of the questions that this book addresses is whether a ministry-based enforcement model can provide data privacy protection as effectively as a specialized DPA.

The separate question of what is required for a DPA to be able to claim 'independence' is complex. There are seven international agreements and standards relevant to data privacy, five of which require a DPA be 'independent' in some way,[81] except for OECD and APEC **(p.74)** which do not require a DPA at all. Nevertheless there is no simple definition of what 'independence' means. An analysis[82] of these seven international instruments, and the writings of expert authors, identifies 12 factors as relevant,[83] five being required more frequently than the others: DPA established by legislation; legislation gives power to investigate free of direction; fixed term of office; defined reasons for removal; and powers to report directly to Parliament or the public. Although there is no full agreement on which criteria are necessary for independence, they provide an international standard by which to measure the independence of Asian DPAs. The criteria are applied to Asian laws in Chapter 18, section 2.2.

However, an issue not dealt with in any of the instruments requiring independence in a DPA, is whether it makes any difference if the DPA has jurisdiction only over the private sector and not the public sector. This is probably because bodies that developed the criteria have only contemplated DPAs covering both sectors, as is the case everywhere other than in Asia. However, the recently established DPAs in Singapore and Malaysia are the only two among the 90 existing DPAs[84] with jurisdiction over the private sector only. They are not 'watchdogs on government', unlike other DPAs. While there are strong and obvious reasons why DPAs which have part of their functions preventing abuses by a government must be independent of that same government (reasons which apply to all other DPAs across the world), they do not apply with the same strength in Singapore and Malaysia, or perhaps in relation to future DPAs to be created in Asia. Here we are dealing with the regulation of industry by a government agency, and while there are always arguments for and against the use of independent regulators, the position of these DPAs as semi-independent regulatory bodies is nothing unusual. Whether they are independent enough of the private sector to avoid 'regulatory capture' is a separate question.

Consequences of a lack of independence, or lack of a DPA

The are three main consequences of the lack of an independent DPA to an Asian country: (i) 'appropriate autonomy and independence' is a condition for membership of the ICDPPC, a reduced and ambiguous requirement since 2010;[85] (ii) lack of an independent DPA is a negative factor in an 'adequacy' assessment by the European Commission (see Chapter 2, section 3.2); and (iii) lack of an independent DPA is likely to be a negative factor in an application by a non-European country to become a party to CoE Convention 108 (see Chapter 19, section 3.2). The extent to which the Asia-Pacific Privacy Authorities (APPA) will continue to require independence of a DPA for accreditation is now uncertain **(p.75)** since they no longer follow the accreditation standards of the ICDPPC. Whether the Singaporean and Malaysian DPAs will apply for APPA membership via first applying to join ICDPPC, or will do so via first joining the Global Privacy Enforcement Network (GPEN) or APEC Cross-border Privacy Enforcement Arrangement (CPEA), will reveal whether 'independence' of DPAs will continue to have significance outside Europe.

Notes:

([1]) Graham Greenleaf, 'Scheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories' (2014) 21(1) *Journal of Law & Information Science* <http://www.jlisjournal.org/abstracts/greenleaf.23.1.html>; also at <http://ssrn.com/abstract=2280877>.

([2]) Here 'countries' means 'separate legal jurisdictions' whose privacy laws are not subject to another jurisdiction's law. Thus Hong Kong and Macau SARs and Taiwan are included.

([3]) 'Legislation' is needed, not only a voluntary code of conduct or a trustmark scheme.

([4]) Laws must cover most economically significant aspects of the operation of the country's private sector. A few countries also have national 'public sector only' laws.

([5]) General constitutional protections, or a civil actions (tort), or criminal law prohibitions, to protect privacy are not sufficient.

([6]) It would be too strict to require compliance with every one of 15 sub-principles into which the privacy principles in the OECD Privacy Guidelines (1980) and the Council of Europe (CoE) Data Protection Convention 108 (1981) can be divided. The conclusions reached were that

the minimum requirements are (i) access and correction rights ('individual participation'), (ii) some 'finality' principles (limits on use and disclosure based on the purpose of collection), (iii) some security protections; and (iv) overall, at least 11 of the 15 sub-principles.

([7]) Greenleaf, 'Scheherezade and the 101 Data Privacy Laws', and accompanying table.

([8]) Growth started with Sweden's Data Act in 1973, and a number of sectoral and other developments in the USA. See Greenleaf, 'Scheherezade and the 101 Data Privacy Laws', section 'The global diffusion of data privacy laws over 40 years: Growth by decade'.

([9]) For a history which is particularly valuable in incorporating early non-legislative versions in the USA and elsewhere, see Robert Gellman, 'Fair Information Practices: A Basic History' (Version 2.02, November 11, 2013) <http://bobgellman.com/rg-docs/rg-FIPshistory.pdf>.

([10]) *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD, Paris, 1981); adopted as a Recommendation of the Council of the OECD, 23 September 1980. The Guidelines were revised in 2013 and that version is referred to as the 'revised OECD Guidelines 2013': see Chapter 18.

([11]) Council of Europe, *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.

([12]) *APEC Privacy Framework* (APEC, 2004, completed 2005) <http://publications.apec.org/publication-detail.php?pub_id=390>.

([13]) *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* (O.J. L. 281, 23 November 1995, pp. 31ff).

([14]) Council of Europe, *Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Data Flows* (ETS No. 181, opened for signature 8 November 2001, entered into force 1 July 2004).

([15]) These included requirements of deletion and special treatment for sensitive data.

([16]) OECD Guidelines: '7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.'

([17]) OECD Guidelines: '8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.'

([18]) OECD Guidelines: '9. The purposes for which personal data are collected should be specified not later than at the time of collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.'

([19]) OECD Guidelines: '10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [Guideline 9] except: (a) with the consent of the data subject; or (b) by the authority of law.'

([20]) OECD Guidelines: '11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.'

([21]) OECD Guidelines: '12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.'

([22]) OECD Guidelines: '13. An individual should have the right: (a) to obtain from the a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; and (iv) in a form that is readily intelligible to him; (c) to be given reasons if a request made under sub-paragraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.'

([23]) OECD Guidelines: '14. A data controller should be accountable for complying with measures which give effect to the principles stated above.'

([24]) The APEC principles are more explicit on this point.

([25]) The elements most often missing from national legislation are the following: the 'fair means' aspect of the collection principle; the openness principle; and notice not required on change of purpose under the use limitation principle.

([26]) See section 1.1 in this chapter.

([27]) *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* (O.J. L. 281, 23 November 1995, pp. 31ff).

([28]) Council of Europe, *Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Data Flows* (ETS No. 181, opened for signature 8 November 2001, entered into force 1 July 2004).

([29]) This was first argued in 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>. The analysis there also included two 'European' enforcement requirements, so was put in terms of how many out of 10 principles a law embodied.

([30]) Lee Bygrave, 'International Agreements to Protect Personal Data' in James B. Rule and Graham Greenleaf (Eds.), *Global Privacy Protection: The First Generation* (Edward Elgar, 2008), pp. 15–49, 19–38.

([31]) Other 'European' elements could be added to the list, for example the right to prevent further processing, but it was decided to keep the list to a manageable size. A choice was then made of the most important distinguishing elements.

([32]) Greenleaf, 'The Influence of European Data Privacy Standards Outside Europe'.

([33]) Greenleaf, 'The Influence of European Data Privacy Standards Outside Europe'. In that study, two further elements related to enforcement (not 'content principles') were included, giving a total of 10 principles. They were the requirements of a data protection authority, and recourse to the courts.

([34]) Based on the 101 laws identified in Greenleaf, 'Scheherezade and the 101 Data Privacy Laws'.

([35]) Revisions under way of the EU Directive (in the form of a proposed Regulation) and the CoE Convention 108 and Additional Protocol (called 'modernization') are likely to contribute to the evolution of a third and higher international data privacy standard, as discussed in Chapter 19.

([36]) Article 29 Working Party 'Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive' (WP 12, DG XV D/5025/98, 24 July 1998), <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf>; Article 29 Working Party 'First orientation on Transfers of Personal Data to Third Countries: Possible Ways Forward in Assessing Adequacy' (WP 4, XV D/5020/97-EN final, 26 June 1997), <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp4_en.pdf>.

([37]) Export restrictions were allowed where the importing country does not 'substantially observe' the OECD Guidelines; where re-export would circumvent domestic laws (in effect, where the receiving country does not have its own data export prohibitions); and to protect sensitive data not similarly protected overseas (Guideline 17).

([38]) Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press, 2013).

([39]) Kuner, *Transborder Data Flows and Data Privacy Law*, pp. 157–65.

([40]) Kuner, *Transborder Data Flows and Data Privacy Law*, 'Continuing accountability of data controllers', pp. 173–4.

([41]) See Dan Svantesson, *Extraterritoriality in Data Privacy Law* (Ex Tuto Publishing, 2013); Kuner, ch. 6 'Applicable law, extraterritoriality and transborder data flows' in *Transborder Data Flows and Data Privacy Law*.

([42]) James Rule, Douglas McAdam, Linda Stearns, and David Uglow, *The Politics of Privacy* (New American Library, 1980), p. 93.

([43]) See Graham Greenleaf and Roger Clarke, 'A Critique of the Australian Law Reform Commission's Information Privacy Proposals' (1986) 2(1) *Journal of Law, Information and Science*, p. 83 at part 3.1 <http://www.austlii.edu.au/au/journals/JlLawInfoSci/1986/6.html>; Graham Greenleaf, 'Stopping Surveillance: Beyond "Efficiency" and the OECD' (1996) 3 *Privacy Law & Policy Reporter*, p. 148 <http://www.austlii.edu.au/au/journals/PrivLawPRpr/1996/69.html>.

([44]) Data export limitations based on destination; minimal collection; fair and lawful processing; prior checking; deletion; sensitive data protections; automated processing controls; and direct marketing opt-out.

([45]) OECD Privacy Guidelines, Art. 19. 'In implementing domestically the principles set forth in Parts Two [Basic Principles of National Application] and Three [Basic Principles of International Application], Member countries should establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data. Member countries should in particular endeavour to: a) adopt appropriate domestic legislation; b) encourage and support self-regulation, whether in the form of codes of conduct or otherwise; c) provide for reasonable means for individuals to exercise their rights; d) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; and e) ensure there is no unfair discrimination against data subjects.'

([46]) APEC Privacy Framework Part IV Section A ('Guidance for domestic implementation'), provisions I–VI, particularly II. The APEC Cross-Border Privacy Framework may differ: see Chapter 19, section 2.

([47]) Graham Greenleaf, 'Five Years of the APEC Privacy Framework: Failure or Promise?' (2004) 25 *Computer Law & Security Report*, pp. 28–43.

([48]) The proposed EU Regulation and 'modernized' CoE Convention may include improved means to exercise rights, but that is a matter for the future (see Chapter 19).

([49]) The two enforcement-related principles in that study were: 9. DPA required—Requirement of an independent Data Protection Authority as the key element of an enforcement regime (EU Directive, and Additional Protocol to Convention 108); and 10 Recourse to the courts—Requirement of recourse to the courts to enforce data privacy rights (EU Directive, Convention 108, and, more explicitly, the Additional Protocol to Convention 108).

([50]) Article 29 Working Party 'Transfers of personal data to third countries' (1998); Article 29 Working Party 'First orientation on Transfers of Personal Data to Third Countries' (1997).

([51]) This statement is derived from joint work with Lee Bygrave for the European Commission.

([52]) International Conference of Data Protection and Privacy Commissioners, *International Standards on the Protection of Data Protection and Privacy* ('Madrid Resolution') (ICDPPC, 5 November 2009) <http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf>.

([53]) Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (2nd Edn., Oxford University Press, 2007), part 1 G 'Enforcement of the Law', pp. 50–6 and Appendix 13.

([54]) Lee Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer, 2002), ch. 4 'Monitoring, supervisory and

enforcement regimes', pp. 70–84.

([55]) Colin Bennett and Charles Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (MIT Press, 2006), ch. 9 'The Evaluation of Impact', pp. 235–68.

([56]) Bennett and Raab, *The Governance of Privacy*, p. 239.

([57]) Bennett and Raab, *The Governance of Privacy*, pp. 263–4.

([58]) Bennett and Raab, *The Governance of Privacy*, p. 265.

([59]) Bennett and Raab, *The Governance of Privacy*, p. 266.

([60]) Bennett and Raab, *The Governance of Privacy*, p. 134.

([61]) Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press, 1992), pp. 35–52.

([62]) Ayres and Braithwaite, *Responsive Regulation*, pp. 5–6.

([63]) John Braithwaite, 'The Essence of Responsive Regulation' (Fasken Lecture) (2011) 44 UBC LRev 475.

([64]) Diagram from Braithwaite, 'The Essence of Responsive Regulation', p. 482.

([65]) Braithwaite, 'The Essence of Responsive Regulation', p. 481.

([66]) John Braithwaite, comments in an address to an APEC Privacy seminar, Canberra, January 2007.

([67]) Braithwaite in 2010 reformulated it in nine propositions, only one of which refers directly to the pyramid of sanctions: Braithwaite, 'The Essence of Responsive Regulation', p. 476.

([68]) For a summary, see Dimity Kingsford-Smith, 'A Harder Nut to Crack: Responsive Regulation in the Financial Sector' (2011) 44 UBC LREv, pp. 705–9.

([69]) Kingsford-Smith, 'A Harder Nut to Crack', p. 695.

([70]) Enforcement of data privacy laws does not involve an easily defined set of subjects of regulation, because such laws are usually equally applicable to all private sector organizations ranging from small businesses to the largest global conglomerates, and in most countries all public sector agencies as well.

([71]) Kingsford-Smith, 'A Harder Nut to Crack', p. 696.

([72]) John Braithwaite, 'Responsive Regulation and Developing Economies' (2006) 34(5) *World Development*, pp. 884–98.

([73]) The enforcement measures in use (whether reactive, systemic, or supportive) can be categorized into 10 general types: (i) choice of enforcement authority (DPA or/and ministry-based enforcement); (ii) varieties of complaint investigations; (iii) investigative powers and procedures; (iv) orders and remedies available from DPA/ministry; (v) offences; (vi) rights of court action (including appeals from DPA/ministry decisions); (vii) data breach notification requirement; (viii) transparency of enforcement (publication of statistics and cases etc); (ix) 'accountability' measures within a data controller; and (x) inspection measure external to a data controller. There are a considerable variety of options within each. For example, orders and remedies available from a DPA or ministry could include compliance orders or injunctions, administrative fines, compensation payments, etc. The inspection measure external to a data controller could include registration systems or audits, with each able to operate at different specific levels. Requirements to carry out privacy impact assessments are external, but carrying out the PIA may be internal.

([74]) For example, the following 22 steps, from most serious to least serious sanctions: termination of business licence to operate; offences with high level fines and/or jail sentences; class actions before courts, with high levels of compensation; administrative penalty by DPA for breach of principles, with high level fines; personal liability of corporate officers for offences; disciplinary action against government officers; suspension of business licence to operate; offence to breach any principle, with medium level fines; offence to breach ministry/DPA order, with medium level fines; individual right of action in court for compensation; award of compensation by separate tribunal; data breach notification to DPA/ministry; data breach notification to individual; publication of identified DPA decisions authorized ('name and shame'); administrative penalty by DPA for breach of principles, with medium level fines; award of compensation by DPA; rectification orders by DPA/ministry; compliance orders by DPA/ministry to prevent breaches; award of compensation by agreed mediation; publication of enforcement statistics by DPA; use of ADR (mediation) facilitated by DPA; warning letters by DPA/ministry.

([75]) These include, from most costly to least costly: privacy impact assessments required; DPA inspection/audit of personal data systems; data user registration and publication ('sensitive' systems only); data protection officer (DPO) required; 'accountability' requirements by a data processor; and openness of data processing procedures.

([76]) The following 'supports' for effectiveness of sanctions are in at least one current Asian data privacy laws: existence of a separate data protection authority (DPA) (i.e. not only ministry-based enforcement); DPA has enforcement powers on own motion investigations; class complaints permitted; onus of proof is on data user; right of appeal against DPA decisions; time limits on DPA decision; no need to prove breach ab initio in court; and DPA can intervene in court cases.

([77]) These include: training courses; freely accessible training/educational materials; non-compulsory guidelines; compliance advisory services; assistance in conducting voluntary audits and PIAs; compliance seals and marks; and compliance prizes and awards.

([78]) The notion of 'nudges' to support compliance is related to this approach: For an overview, see 'Nudge theory' (Wikipedia) <http://en.wikipedia.org/wiki/Nudge_theory>.

([79]) Graham Greenleaf, 'Reforming Reporting of Privacy Cases: A Proposal for Improving Accountability of Asia-Pacific Privacy Commissioners' <http://ssrn.com/abstract=512782>.

([80]) Greenleaf, 'Scheherezade and the 101 Data Privacy Laws', at section 'The prevalence of DPAs'. The DPAs are named in the table. By December 2013, of the 101 countries with data privacy laws, 90 require separate DPAs of some type, and 86 have appointed them.

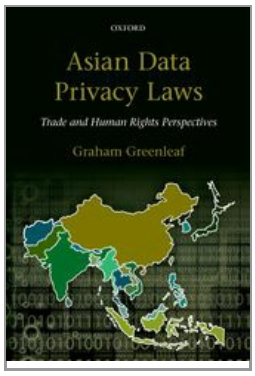
([81]) (i) The Paris Principles (1991) on national human rights institutions; (ii) European Union Data Protection Directive (1995) and its interpretation; (iii) CoE Convention 108 as amended by Additional Protocol (2001); (iv) ECOWAS data protection Supplementary Act (2010); (v) Commonwealth model Privacy Act (2002); (vi) International Conference of Data Protection and Privacy Commissioners (ICDPPC) accreditation requirements (2001); (vii) Association of Francophone Data Protection Authorities (AFAPDP) Resolutions (2011): see Graham Greenleaf, 'Independence of Data Privacy Authorities: International Standards and Asia-Pacific Experience' (2012) 28(1) & (2) *Computer Law & Security Review* <http://ssrn.com/abstract=1971627>.

([82]) Greenleaf, 'Independence of Data Privacy Authorities: International Standards and Asia-Pacific Experience'.

([83]) (1) Establishment of DPA by legislation rather than any executive order or delegated legislation; (2) independence established by legislation (usually, ability to investigate and report free of direction or permission from any other political or governmental authority); (3) a fixed term of office, so as to avoid a Commissioner being at the whim of executive dismissal (including remuneration also independent of the executive); (4) removal from office only for defined reasons (inability, neglect of duty, or serious misconduct), and with procedural safeguards; (5) powers and duties to report directly on issues to either the Parliament and/or the public; (6) immunity against personal lawsuits relating to performance of official duties; (7) resources of the DPA determined independently of the Executive; (8) positive qualification requirements for Commissioners; (9) prohibition of Commissioners undertaking other concurrent positions; (10) prohibition of appointment of Commissioner from specified backgrounds which could cause conflicts of interests, or requirement of the disclosure of interests; (11) DPA decisions being subject to a right of appeal; and (12) appointment of Commissioner by the Legislature rather than by the Executive.

([84]) Greenleaf, 'Scheherezade and the 101 Data Privacy Laws', at section 'The prevalence of DPAs'.

([85]) Greenleaf, 'Independence of Data Privacy Authorities', pt. I, section 3.7.



Asian Data Privacy Laws: Trade & Human Rights Perspectives
Graham Greenleaf

Print publication date: 2014
Print ISBN-13: 9780199679669
Published to Oxford Scholarship Online: December 2014
DOI: 10.1093/acprof:oso/9780199679669.001.0001

Hong Kong SAR—New Life for an Established Law

Graham Greenleaf

DOI:10.1093/acprof:oso/9780199679669.003.0004

[–] Abstract and Keywords

The focus of this chapter is on Hong Kong's Personal Data (Privacy) Ordinance of 1995, the first comprehensive data privacy law in Asia. It sets out the context of a common law system with the constitutional protection of privacy through the Basic Law. The Ordinance also established Asia's first data protection authority (DPA), the Privacy Commissioner for Personal Data (PCPD). The Ordinance is analysed in detail, drawing on the largest body of reported complaints, appeals, and judicial decisions in any Asian jurisdiction. It has been strengthened considerably by reforms in 2012. The chapter concludes that Hong Kong's law includes principles stronger than the minimum international standards, and that since 2012 they are capable of being enforced more effectively, and that the system operates with a high level of transparency.

Keywords: data protection, privacy, Asia, Hong Kong, China, Privacy Commissioner, data protection authority

1. Introduction and context

Hong Kong's Personal Data (Privacy) Ordinance of 1995 (the PDPO or the 'Ordinance') was the first comprehensive data privacy law in Asia. Following the re-incorporation of Hong Kong into China in 1997 as the Hong Kong Special Administrative Region (SAR), the Hong Kong SAR and the Macau SAR are the only regions of China which have comprehensive data privacy laws. For 18 years, administered by four Privacy Commissioners for Personal Data (PCPDs), the Ordinance lacked sufficient powers for the Commissioners to fully enforce its privacy principles. Major reforms to the Ordinance in 2012, an activist approach to enforcement by the fourth Commissioner, and some pro-privacy tribunal decisions, have started to overcome these limitations and give this established law a 'new lease of life'.

1.1. Historical context

Hong Kong Island was ceded to Britain by the 1842 Treaty of Nanjing (the first of the 'unequal treaties'), having been seized in 1840 after the First Opium War. Further war and cession added the Kowloon peninsula, and the New Territories were added in 1898 by a lease from China for 99 years.[1] During 150 years of colonial rule to 1997, Hong Kong developed a very prosperous economy, based on finance, trade, and manufacturing, becoming the world's twelfth largest trading economy. By the Sino-British Declaration (1985), China and the UK reached a constitutional settlement by which the UK agreed to 'restore' sovereignty to China in 1997, in order to realize Deng Xiaoping's concept of 'one country, two systems' for Hong Kong.[2]

1.2. Constitutional, legislative, and political context

Hong Kong's privacy protection has a unique constitutional context. Hong Kong is a

Special Administrative Region of the People's Republic of China (PRC), established in accordance with the PRC Constitution.[3] The 'one country two systems' approach instituted in Hong Kong is prescribed in Hong Kong's Basic Law[4] (a law of the PRC which applies to **(p.81)** and is part of the law of Hong Kong). It allows the exercise of a 'high degree of autonomy'[5] by Hong Kong in matters apart from foreign affairs and defence, and the content and ultimate interpretation of the Basic Law.

The legislative and executive systems involve only limited democracy.[6] The Chief Executive is appointed by the Central Government of the PRC, with a limited role for democratic input.[7] The members of his 'cabinet', the Executive Council, are all appointed by him. Legislation is enacted by a 70-member Legislative Council (LegCo), increased from 60 in 2010, of whom half are elected by direct elections from geographical constituencies and the other half from specified occupational groups and industries called 'functional constituencies'. The Basic Law states that 'the ultimate aim is the election of all the members of the Legislative Council by universal suffrage',[8] but uncertainty continues as to when this may occur. The consent of the Chief Executive is required before Bills relating to government policies may be introduced. Non-government Bills, or amendments to government Bills, require a majority vote by each of the geographical and functional constituencies, and are therefore more difficult to enact. LegCo is much more than a consultative body, but short of being a fully democratic institution.

1.3. The legal and judicial system of Hong Kong

Under British colonial rule, the common law of England and the rules of equity were made applicable to Hong Kong insofar as they were appropriate to the circumstances of the colony. The Basic Law provided for Hong Kong's previous legal system to be maintained.[9] The Basic Law gives Hong Kong independent judicial powers, with the judicial power of 'final adjudication' vested in Hong Kong's Court of Final Appeal (replacing the Judicial Committee of the Privy Council).[10] Hong Kong courts exercise the normal powers associated with a common law approach to the rule of law, including judicial review of administrative power and review of legislation for its consistency with the Basic Law.[11]

While Hong Kong's courts have the conjoint power to interpret and apply the Basic Law, this is subject to an overarching power of interpretation of the Basic Law vested in the Standing Committee of the National Peoples Congress of the PRC, which is a legislative and political rather than a judicial body. So, although Hong Kong's common law legal system is preserved by the Basic Law, interpretation of the Basic Law can be ultimately subordinated to the very different legal system of the PRC.[12] This makes for a difficult area of constitutional construction.[13] The PRC power of interpretation has only been exercised in a few instances, none directly affecting privacy issues arising from the Basic Law.

(p.82) 1.4. State surveillance in Hong Kong

Hong Kong residents do not experience omnipresent or oppressive surveillance. Their experience in this regard is probably most similar to citizens of a European state where

government agencies have a relatively high degree of basic information about all citizens though a centralized ID system, but where public and private sector bodies keep personal information collected for different purposes segregated because of privacy laws.[14]

The information systems built around the Hong Kong ID card have the most pervasive effect. Previous photo-ID cards were replaced (2003–2009) by a multipurpose 'smart' (i.e. chip-based) ID cards which may also replace drivers' licences and library cards. The ID card and the number on it can be required 'in all dealings with government'. Extensive use of the ID card and number by the private sector for identity verification is also allowed but controlled by the privacy Ordinance (discussed in section 5.5 of this chapter). Extensive data matching between government agencies based on the ID number is controlled by the Ordinance. Hong Kong residents normally carry their ID cards and are accustomed to disclosing their ID number. Although the legislative controls around the 'smart ID card' system allow much leeway for expansion of its functions ('function creep'),[15] after a decade of operation this has not occurred.

In the private sector, Hong Kong did not have a comprehensive consumer credit reporting system until the late 1990s, when the Hong Kong Monetary Authority, in the wake of the Asian financial crash, put pressure on all financial institutions to join the existing credit reporting system. Since 2003, credit reporting has been allowed not only on credit defaults but also on the regularity of payments and level of indebtedness of all individual debtors, so details of the credit transactions of all Hong Kong consumers and small businesses are now held by Hong Kong's privately owned credit reporting agency. Reporting of 'positive' data on the number of mortgages held has been allowed since 2011. However, access to personal information about credit practices is still largely confined to the credit industry and this information is not accessible to employers, insurers, or other parties who are not credit providers. Workplace surveillance is extensive in Hong Kong.

Hong Kong has taken a relatively relaxed view of anonymity in transport systems. The Octopus card is a pervasive stored-value card, which is anonymous by default (but with an option to be identifiable), which can be used in most forms of public transport. Cash can be paid (with inconvenience) on all tollways and tunnels in Hong Kong, so some travel within Hong Kong remains anonymous. Cash purchases of SIM cards for mobile phones can be made at convenience stores, and these can be used without further identification to the network (in contrast with many other countries). Although public authorities, no doubt, have other methods of more selective surveillance, pervasive surveillance of movements or telecommunications is absent.

(p.83) 1.5. Social attitudes to privacy in Hong Kong

In considering social attitudes to privacy in Hong Kong, it is necessary to distinguish between public opinion, the extent of public activism, and the views of policy elites.[16] Hong Kong residents continue to rate privacy as one of the social policies of most concern to them. Data users also have a generally positive attitude toward privacy

protection, according to surveys commissioned by the Privacy Commissioner. While public *attitudes* toward privacy as a value rate it highly, public *activism* in relation to privacy has usually been low, and Hong Kong has had few major public confrontations over privacy issues. An example was in 2004 when opposition by the public, some legislators and businesses caused cancellation of police and business association plans for blanket CCTV surveillance of Lan Kwai Fong (an area in Hong Kong with a dense mix of bars, restaurants, and shops). On issues such as the privacy impact of the 'smart' ID card and the introduction of 'positive' credit reporting, where strong public opposition would be expected in many other countries, there was little public challenge to the approach advocated by government and business elites. Similar proposals have been regarded as major privacy issues in other countries. However, those living in Hong Kong are not inherently acquiescent when they perceive infringements of civil liberties. In June 2003, only a couple of months after the ID legislation was passed, an estimated half a million people from a population of 6 million took to the streets to protest against attempts by the government to introduce a 'security' law. The government claimed that Hong Kong's Basic Law required it to introduce this law, which many saw as threatening freedom of speech and association. The government was forced to abandon the law. No such dramatic events have yet been triggered by privacy concerns.

Hong Kong has not developed an organized civil libertarian constituency interested in privacy issues in Hong Kong, with the non-governmental organizations (NGOs) involved in promoting human rights giving little attention to privacy. This is paradoxical, because Hong Kong has had for two decades as high a concentration of experts on privacy law and policy as could be found in any comparably sized jurisdiction in the world. The work of these academic and professional experts has resulted in the Law Reform Commission's series of reports on privacy issues, which is the equal of any in the world,[17] and a high quality body of academic and professional literature.[18] In terms of effectiveness, an extraordinary exception is the role of the maverick legislator 'Long Hair' (Leung Kwok-hung) and his activist colleague Koo Sze Liu who, with support from the legal profession, successfully challenged the whole police and security apparatus, government and constitutional structure of the SAR in a number of 2005–06 court decisions on surveillance (discussed in the next section). They are a stellar example of the difference that individuals can make through privacy activism.

(p.84) 1.6. Constitutional protections in Hong Kong

Constitutional protection of privacy occurs in three different ways in Hong Kong. First, the Basic Law (1990) provides for the continued application of the International Covenant on Civil and Political Rights 1966 (ICCPR). These rights include both a general right of privacy and the right to protection of the law against 'unlawful interference with…privacy, family, home or correspondence'. Because Hong Kong is not a party to the First Optional Protocol to the ICCPR, and China has not ratified it on behalf of Hong Kong, its residents do not have any direct right of appeal (communication) concerning breaches of the ICCPR to the UN Human Rights Committee (UNHRC). However, the Hong Kong government has now made three reports to the UNHRC (1999, 2005, and 2013).[19] The only privacy-related issue raised by the UNHRC in its 2013 Concluding Observations was 'the

increasing number of arrests of, and prosecutions against, demonstrators, and (c) the use of camera and video-recording by police during demonstrations', and it recommended that the government make clear and public 'guidelines for police and for records for the use of video-recording devices'.[20]

Second, the ICCPR provisions have been replicated in local legislation in Hong Kong's Bill of Rights Ordinance (BORO, 1991), but its provisions are subject to amendment or repeal by the Legislative Council (LegCo), unlike those of the Basic Law. The BORO is binding only on government authorities and cannot be used by individuals to seek protection against actions by businesses or other private bodies (called 'horizontal effect'). There are as yet no significant privacy cases under the BORO, other than brief *obiter dicta* indicating that the BORO privacy protection does not have horizontal effect.[21]

Third, the Basic Law specifically provides in relation to privacy that 'The homes and other premises of Hong Kong residents shall be inviolable' and that 'arbitrary or unlawful search of, or intrusion into [such homes and premises] shall be prohibited'; that 'The freedom and privacy of communication of Hong Kong residents shall be protected by law'; and that 'No department or individual may…infringe upon the freedom and privacy of communications of residents except that the relevant authorities may inspect communication in accordance with legal procedures to meet the needs of public security or of investigation into criminal offences'. These Basic Law protections cannot be amended by the local legislature.

This third constitutional protection finally became a major public issue in 2005–06. It was used by litigants to force Hong Kong's administration to enact a Communications and Surveillance Ordinance and thus to end a constitutional crisis. The Ordinance repealed the previous power of the Chief Executive to authorize interception and introduced a requirement for judicial authorization of both interception of communications, and the more intrusive types of other covert surveillance by law enforcement bodies, while allowing law enforcement agencies to sanction their own use of less intrusive forms. It also provided for the appointment of a Commissioner on Interception of Communications. As a result, Hong Kong moved from being a jurisdiction with only nominal controls over surveillance, to one with a relatively high degree of accountability and transparency.[22]

(p.85) The constitutional protections of privacy were therefore shown to be of substance, even though rarely used as yet. The Basic Law protections have the potential to play a role in Hong Kong analogous to the role that Article 8 of the European Convention on Human Rights plays in European countries, or at least in those such as the United Kingdom which do not otherwise provide constitutional protection of privacy.

1.7. Common law protections in Hong Kong

The Basic Law guarantees that Hong Kong remains a common law jurisdiction, and so its courts are free to adopt principles developed in the courts of other legal systems of British origin. If the common law protected privacy, constitutional provisions and legislation would not be so important. Hong Kong courts have not made any significant decisions on the existence of a tort of invasion of privacy, but it is likely that they would

follow the UK approach in rejecting any general common law right of privacy (a general privacy tort).[23]

It is possible that Hong Kong's courts may give greater protection to privacy in future by expanding the law of breach of confidence (or a tort of misuse of private information[24]), in line with the recent UK approach exemplified by the *Campbell Case*,[25] partly in response to the UK's European treaty obligations to protect privacy, which have textual similarities to Hong Kong constitutional provisions (see section 1.6 of this chapter). However, this has not yet occurred. Of the two instances of litigation in Hong Kong in the past decade which could have resulted in an extension of breach of confidence law to protect privacy, one was settled. The other remains incomplete but appears to be proceeding as a traditional breach of confidence action.[26]

However, the Court of First Instance, following the lead of the lower court in Singapore, has held that there is a tort of harassment in Hong Kong.[27] Anthony Chan J, following the approach taken in Singapore,[28] held that harassment was (non-exhaustively) constituted by:

> a course of conduct by a person, whether by words or action, directly or through third parties, sufficiently repetitive in nature as would cause, and which he ought reasonably to know would cause, worry, emotional distress or annoyance to another person.

He noted that, as with other torts, there must be 'a mental requirement of the wrongdoer as well as damage to the victim in order to constitute the tort of harassment', but that recklessness will suffice without need for intention.[29] Despite this slight authority, the position in Hong Kong is uncertain.[30]

Statutory action for interferences with privacy

The Hong Kong Law Reform Commission (HKLRC) has recommended legislation for new privacy rights of civil actions for public disclosure of private facts and intrusions **(p.86)** into privacy,[31] but the government has ignored the proposals to date. In 2006 magazine publication of pictures of a pop star in a state of undress, which had been taken by a hidden camera, led the then Chief Executive to state that the HKLRC proposals would be used as the basis for exploring new measures to guard against press intrusion into privacy, but nothing has come of this. The Privacy Commissioner has since found that some such actions breach the Ordinance (see the discussion of unfair collection practices in section 4.1 of this chapter). The HKLRC also recommended in 2006 both a criminal offence of harassment (which has been enacted in Singapore in 2014, see Chapter 10, section 1.4) and a tort action,[32] but the government has taken no action on either.

2. The Privacy Ordinance and the Commissioner

The most important legislation concerning information privacy is the Personal Data (Privacy) Ordinance 1995, which covers both the public and private sectors. The Ordinance also established the first data protection authority in Asia, the Privacy Commissioner for Personal Data (Privacy Commissioner or 'PCPD'). It is also the longest-

established law in Asia dealing comprehensively with the private sector, and one of the earliest outside Europe to do so. It is pioneering legislation, but after 17 years, was showing its age before reforms in 2012 (the '2012 reforms') which came into effect in 2012 and 2013.

2.1. Origins of, and influences on, the Ordinance

The Ordinance's enactment was not prompted by any significant public demands or major controversy, but was led by the then colonial administration, influenced by local elite opinion. It was a positive and not a reactive process, influenced by European developments and their potential effect on trade with Hong Kong. The history of the Ordinance's development[33] shows that the Hong Kong government was concerned about possible limits on personal data flows from Europe as early as the 1981 Council of Europe Data Protection Convention, but heightening in the early 1990s as the European Union (EU) Data Protection Directive developed. From 1989 the HKLRC was given a very broad reference on privacy protection, and following public consultations published recommendations for data protection legislation,[34] the majority of which were embodied in the 1995 Ordinance.

In the closing years of the British administration, the Hong Kong government had a mixed record on initiatives to protect human rights, balancing carefully which human rights related measures it felt able to adopt, in light of relations with the mainland government. The Ordinance was a human rights-related initiative. But it also had an economic selling point, safeguarding the free flow of personal information to Hong Kong, making it difficult to characterize it as part of a British plot to destabilize Hong Kong in advance of the 'hand-over'. The content of the Ordinance clearly reflected both the OECD Guidelines and EU Directive, but not as any direct pressure from abroad, rather as a long-term protection of the trading position of Hong Kong and as an aspiration of policy-makers to be in keeping with international best practice.

(p.87) 2.2. Privacy Commissioner for Personal Data

The Ordinance provides for the establishment of the office of the Privacy Commissioner for Personal Data (PCPD) as an independent statutory authority[35] to monitor and promote compliance with the Ordinance. Appointment is by the Chief Executive of Hong Kong, for an initial period of five years with eligibility for one reappointment. There have been four Commissioners: Stephen Lau, a senior computing executive (1996–2001); Raymond Tang, a lawyer (2001–2005); Roderick Woo, a lawyer and former Law Society head (2005–2010); and Allan Chiang, a retired civil servant who was the previous Postmaster General (since 2010).

The functions of the Commissioner are broad,[36] and include supervising and promoting compliance with the Ordinance, promoting awareness and understanding of the Ordinance, examining proposed legislation that might affect individual privacy, carrying out inspections of personal data systems, and undertaking research. The budget of the Commissioner's Office, provided by the Executive, is currently under HK$65 million per year (US$8.37 million), for an establishment of 82 staff. The budget and staffing has not

increased substantially in a decade.[37]

2.3. Reform of the Ordinance, 2009–12

Since its enactment in 1995, all provisions of the Ordinance have been brought into effect, save section 33 concerning cross-border transfers which is still not in effect. It stayed largely unaltered since its enactment for the next 14 years. A consultation paper on reform was issued in 2009.[38] Following a two-year consultative process, during which the Privacy Commissioner expressed dissatisfaction with the limited nature of proposed reforms, but supported others, the Personal Data (Privacy) (Amendment) Bill was introduced into LegCo in July 2011, and passed in 2012 (hereinafter 'the 2012 amendments'). The 2012 amendments came into effect on 1 October 2012, except for the provisions concerning direct marketing and the provisions concerning the legal assistance scheme (both in effect 1 April 2013). The history of these long-delayed amendments to the Ordinance shows that although reform initiatives were progressing slowly from 2006–10, the key factor resulting in the introduction of legislation by mid-2011 and its enactment a year later, was the major scandal in early 2010 concerning revenue-generation from customer details by the Octopus group of companies, the operator of Hong Kong's transit card, in which the Hong Kong government is a major shareholder. The scandal was 'a human rights lesson for the Hong Kong community', which demonstrated the lack of effective powers in the Ordinance, and resulted in intense political upheaval and which, in October 2010, forced the Administration to announce that it would expedite amendment of the Ordinance. As the Commissioner has observed, a political crisis outside the government's control resulted in this reform, whereas other reforms proposed by the HKLRC, on matters such as a 'privacy tort' and stalking, have languished because the government has not been proactive in the absence of a scandal forcing its hand.[39]

(p.88) 2.4. Asia's most mature legislation—a wealth of interpretations

The meaning of Hong Kong's Ordinance has been elaborated by the Commissioner, appeals tribunal, and the courts, far more extensively than any other data privacy law in Asia. Since 1997, successive Commissioners have published nearly 300 complaint case notes,[40] usually of a few hundred words and including details of the relevant legislative provisions, 37 much more detailed investigation reports under section 48(2),[41] and a very unusual and revealing book-length analysis of the privacy principles in the Ordinance.[42] The Administrative Appeals Board (AAB) has decided 108 appeals against the Commissioner's decisions, and they are now readily available.[43] Previously they were only known to a narrow circle of specialists in Hong Kong. They are a significant source of interpretation of the Ordinance, particularly in light of the small number of judicial decisions. There are at least 13 court decisions where the Commissioner was a party,[44] 7 at First Instance, and 6 in the Court of Appeal.

Long-term studies of the enforcement activities (and their outcomes) of data protection authorities are rare. Cheung has published[45] an evaluation of not only the Commissioner's enforcement actions, but also the results of appeals to the AAB against the Commissioner's decisions, and appeal and judicial review actions in Hong Kong's

courts, over the life of the Ordinance from 1996 to 2011. During that time, the number of complaints increased 25-fold. Among her general findings are that there has been a 'growing reliance on and trust' of the Commissioner, and that his decisions have been upheld by the AAB in 87 per cent of cases (from 191 appeals). Decisions of the courts have also upheld decisions by the AAB or the Commissioner in over 60 per cent of cases (from 21 cases dealing with 'major issues').

Compared with most other jurisdictions, Hong Kong has a relatively rich history of administrative tribunal and court interpretations of the Ordinance, plus extensive publication of the Commissioner's own interpretations, giving all interested parties valuable guidance to the Commissioner's practices and (in some cases) authoritative precedents. It is therefore not possible for a single chapter to do justice to the details of the Ordinance's interpretation, and only the most important aspects will be covered, with many important practical and procedural aspects glossed over. The complaint and case-law resources mentioned earlier should be consulted, as should the Commissioner's guide to the principles. **(p.89)**

3. Scope of the Ordinance

The Ordinance is comprehensive, covering 'data users' in both public[46] and private sectors, with very few exceptions compared with data protection legislation in many jurisdictions. It does not distinguish between automated and non-automated data or processing, covering both equally. 'Personal data' must relate to a living individual, and the Ordinance does not therefore cover legal persons or deceased persons.

3.1. The data regulated—'personal data', 'data', and 'documents'

The scope of the Ordinance depends on the meaning of 'personal data', 'data', and 'document'. 'Personal data' must relate directly or indirectly to a living individual, and from which it is 'practicable' for the individual to be identified, directly or indirectly, and must be in a form allowing access or processing (except in relation to the security principle).[47] 'Data' is defined as 'any representation of information, including an expression of opinion, in any document'.[48] A 'document' is defined as including such things as a disc, tape, film, or other device in which data or visual images are embodied and capable of reproduction. Photos are included.[49] Both manual and automated records are included. Information therefore only counts as 'data' if it has been held in a document by the data user at some point, and not merely held in someone's memory. For example, where a woman disclosed her personal information to a member of staff at a housing estate office, and this information was passed on to others, her complaint failed because the information about her was never written down.[50] The same result is reached in privacy laws of most other jurisdictions.

The requirement of 'practicability' of identifying a person from particular data was illustrated by a complaint that indicator lights came on and a bell sounded whenever a holder of a concessional senior citizen transport card ('Octopus card') placed the card on a toll gate reader. Any person could purchase such a card, and the same sound and light indicators occurred for both under-12s and over-65s. The AAB upheld the

Commissioner's decision that no personal data about the individual was disclosed.[51] Nor did the Octopus card identify that person. We could also say that the circumstances did not enable the holder of the card to be identified. The situation may have been different if the individual had held a personalized Octopus card, which would have displayed his age when placed on the reader, but this was not considered.[52]

Whether data is 'related' to an individual received a narrow interpretation in the UK in *Durant v Financial Services Authority* [2003] EWCA Civ 1746, which held that in order to be 'personal data' information must be 'biographical' to a significant extent and with the individual as its focus. The Hong Kong Court of First Instance, upholding an AAB decision, took a similarly restrictive approach to that in *Durant* in allowing redactions from documents because they dealt with other matters, not strictly data concerning specific individuals.[53] The AAB has done likewise in cases concerning invoices and minutes of **(p.90)** meetings.[54] The PCPD considers that complaints concerning data that only 'relate' to the complainant 'in none but a trivial sense', could be dismissed by the Commissioner on the ground of triviality.[55] The judicial interpretation of 'collection of personal data' (see section 4.1 of this chapter in relation to 'collection') is in effect also a significant restriction on the meaning of 'personal data'.

A narrow view of 'personal data' in relation to email addresses and IP addresses has also been taken by the AAB in the *Yahoo! HK Case*.[56] Shi Tao was convicted by a court in the PRC of violating PRC criminal law by disclosing state secrets sent via his email account while he was in Hunan Province, China. He was sentenced to 10 years' imprisonment. Evidence in the case showed that staff of the Beijing office of Yahoo! China disclosed to PRC investigative authorities details of email transactions sent from a particular email account, including the IP address from which a person had logged in to send the relevant emails. Yahoo! China was a business owned by a foreign company registered in the PRC that was owned in turn by a Hong Kong company, Yahoo! Hong Kong (YHHK). The question before the AAB was whether YHHK had (though its agent) disclosed 'personal data'. The AAB found that it had not, because an IP address is not necessarily associated with an individual, and there was in this instance no evidence that Shi Tao had opened the relevant email account under his name (thereby enabling it to be used to indirectly identify the IP address with him), rather than under an alias. Consequently, it had not been demonstrated by the complainant that YHHK had disclosed personal data from which it was practicable to identify Shi Tao. The AAB noted that Yahoo! was not in the position of an Internet Service Provider (ISP), which would normally be able to associate a person's identity with an IP address or email account.

3.2. Data users, data processors, and vicarious liabilities

Almost all obligations under the Ordinance are imposed on a 'data user', defined in much the same way as a data controller under European laws as a person controlling processing of personal data.[57] In the *Yahoo! HK Case*,[58] the AAB held that even when a company is forced to disclose personal data under the compulsion of a foreign law, to a foreign government (in this case the mainland's State Security Bureau), it still retains control of the information both before and after disclosure and is a data user. A party

who is only processing the data as agent for another person[59] (a processor) is not a data user. However, the 2012 amendments provide in effect that a processor has a separate statutory obligation to delete personal data once the purpose of processing is completed, not only a contractual obligation under data protection principle (DPP) 4(2).[60]

3.3. Exemptions

Individuals can be data users but data held by an individual are exempt if '(a) concerned only with the management of his personal, family or household affairs; or (b) so held only **(p.91)** for recreational purposes' (domestic purposes).[61] There is no general exemption for 'non-commercial' purposes, unlike some laws, so clubs and societies are generally bound to comply. The Central Authorities of the Central People's Government of the PRC and most of its subordinate organs with activities in Hong Kong are exempt. No other classes of data users have a general exemption. The near-comprehensive coverage of data users is complemented by the relatively narrow and specific exemptions from particular DPPs, giving the Ordinance more universal application than data protection legislation in many jurisdictions.

There are exemptions from the principles of use limitation, and of subject access, where it is considered necessary to protect various public and social interests such as security, defence, international relations, the prevention and detection of crime, and the remedying of unlawful conduct (see Part VIII of the Ordinance). The exemptions only apply where complying with the DPPs would prejudice the interests concerned.[62] 'Unlawful' in this context includes civil wrongs. For example, witness statements collected for the purpose of possible criminal proceedings were permitted to be disclosed to plaintiffs in a civil suit.[63]

There are some narrow exemptions relating to employment,[64] in contrast (for example) with the very broad exemption for employment-related personal data in the Australian private sector legislation. Lastly, there are exemptions from the subject access requirements where compliance would breach legal professional privilege;[65] or would be likely to cause serious harm to an individual's physical or mental heath.[66] There is also an exemption from the use limitation requirements in relation to personal data used for research or the preparation of statistics where the results that are made available do not identify any of the individuals concerned.[67]

In the 2012 Amendments there are new exemptions from parts of the Ordinance, including very broad exemptions for personal data held by a court, magistrate, or judicial officer in the course of performing judicial functions,[68] and exemptions to permit the transfer of personal data to carry out due diligence exercises,[69] for the purpose of emergency rescue or relief,[70] and to the Government Records Service for archive purposes.[71]

News media exemption

The media are exempt from many aspects of the Ordinance until after publication.[72] The exemption applies only to data users whose business consists of 'news activity', which is

given a broad definition as 'any journalistic activity' and including gathering and preparing news and current affairs information, and disseminating it or observations on it. A person cannot request access to personal data held by a news media data user until after a story is published. The Commissioner cannot investigate complaints until after publication, and cannot commence 'own motion' investigations at any time, in relation to news activities.

There is a further significant and unusual exemption from DPP 3 (limiting uses and disclosures to the purpose of collection) of personal data which is disclosed to a data user engaged in news activities, where the disclosing party (e.g. a 'whistleblower' or other media informant) reasonably believes this to be in the public interest.[73] 'Public interest' is not **(p.92)** defined. Media sources, not only the news media themselves, therefore have a 'news activity' exemption in Hong Kong. Further, once such a 'public interest' disclosure is made, the news activity use then made of it by a journalist is similarly exempt from DPP 3.

The news media exemptions are therefore not comprehensive, but the Ordinance has had little enforcement against the media.[74] The *Eastweek* case excluded from the scope of its application images collected by data users where they were not interested in the identity of the person appearing in an image. The prohibition on 'unfair collection' practices has, however, been applied to 'paparazzi' style photo-journalism (see section 4.1 of this chapter). The limits on the DPP 3 exemption are shown in a complaint upheld by the Commissioner where a newspaper was directed to delete from an article the ID number and name of a complainant to the police, on the basis that he had not consented to publication of this information, and that its publication would not serve the public interest.[75] However, a finding by the Commissioner that publication by a newspaper of an assault victim's address was a breach of DPP 4 (the security principle), from which there are no news activity exemptions, was reversed by the AAB on the grounds that DPP 4 deals with unauthorized or accidental disclosures only, and not with intentional publication.[76]

4. Hong Kong's data protection principles

Hong Kong's six data protection principles (DPPs) are broadly consistent with the OECD Privacy Guidelines, as the Law Reform Commission (HKLRC) recommended in its 1994 report,[77] but are stronger in some important respects. The government intended that the Ordinance would give 'statutory effect to internationally accepted data protection principles'.[78] This intention echoed the HKLRC's recommendation that the OECD Guidelines should be adopted in the legislation. Nevertheless, the eight OECD Guidelines were not adopted verbatim in the Ordinance. Instead, they were reformulated in a set of six broadly stated DPPs in Schedule 1,[79] which will now be examined.

Although 'processing' is defined (non-exhaustively) as including 'amending, augmenting, deleting or rearranging the data, whether by automated means or otherwise',[80] the concept of 'processing' is not central to the Hong Kong Ordinance. The DPPs are primarily expressed in terms of more specific concepts such as 'collection', 'use', and 'disclosure', with only the security principle referring to processing.[81] The Ordinance is therefore closer in its expression to the OECD Guidelines than are, for example, the

Macau or Malaysian laws.

4.1. Collection limitations on personal data

DPP 1 limits the collection of personal data to that necessary for a lawful purpose directly related to a function of the collector. The data must also be 'adequate but not excessive in relation to that purpose'.[82]

(p.93) The *Eastweek* case and the meaning of 'collect'

There is an important restrictive judicial interpretation of 'collection of personal data' in Hong Kong, which has not yet been followed in other jurisdictions. In the *Eastweek* case [83] in 2001 a majority of the Court of Appeal held that where a person collects data of an unidentified individual with no intention to identify that individual, this is not collection of personal data and falls outside the Ordinance (and therefore could not be in breach as 'unfair'). In that case a newspaper's photo of a woman in a public place, which was used to illustrate the bad dress sense of Hong Kong women, was held by the Court of Appeal not to be collection of personal data. This was because the newspaper was not interested in the woman's identity, even though her friends and colleagues could identify her from the published photo. The case decided that:[84]

> It is…of the essence of the required act of personal data collection that the data user must thereby be compiling information about an identified person or about a person whom the data user intends or seeks to identify.

The Commissioner also places importance on the statement in the decision that the identification of the person must be 'known or sought…as an important item of information'.[85] This stress on 'importance' as necessary for collection has some similarities to the UK approach in *Durant*.

As the Commissioner notes, the conditions in *Eastweek* 'seem to infuse a subjective element into the notion of collection of personal data'.[86] It is difficult to see how the court's interpretation in *Eastweek* could have been the general intention of the legislation when it defines personal data by reference to objective tests while the approach of the majority judges makes the definition of personal data (at the time of collection) subject to such subjective tests, viz. the knowledge or intention of the collecting party. Nevertheless, it is the law in Hong Kong, although not in other jurisdictions.

The Commissioner has indicated[87] that he will apply *Eastweek* to narrow the scope of the Ordinance quite considerably. None of the DPPs (e.g. rights of access and correction, security requirements) will apply if the data was not collected as personal data. For example, unsolicited personal information will not become 'personal data' upon receipt, but only when the data user decides to keep it as part of a compilation of information about the data subject.[88] However the Commissioner has refused to apply *Eastweek* in the extreme way proposed by a university, which argued that the marking sheets and cover sheets of assignments and examination booklets were not personal data because the identity of a student did not influence what marks were given. The Commissioner rejected this, stressing the university's capacity to identify the student.[89]

Excessive collection

In 2005, a local newspaper reported that Hongkong Post had installed pinhole cameras in the working areas of a Post Office, supposedly to detect the theft of stamps by employees. The Commissioner found that the potential loss of stamp revenue was out of proportion **(p.94)** to the extent of the surveillance, and thus excessive in relation to its functions, breaching DPP 1(1).[90] In another example, a company required a woman's ID card number and her date of birth before she could enter a 'lucky draw' competition. The Commissioner found that this was excessive collection because collection of the month of birth was enough to send people birthday gifts. Random lucky draw numbers together with names and addresses and sighting of ID cards was sufficient to identify winners without collection of ID numbers, so that was also excessive given the sensitivity of ID numbers.[91]

Where an employer required employees on their first day of employment to be fingerprinted for the purposes of recording attendance, the Commissioner also held that this was excessive collection contravening DPP 1(1).[92] Among the factors taken into account were that the information was not being used for security purposes, that alternative methods of ensuring accurate attendance recording were available, and that fingerprints were 'sensitive' information (even though there are no special rules in the Ordinance for 'sensitive' data). If staff had been given a genuine choice of methods of recording attendance, it may have been acceptable for fingerprinting to be one of the choices.

Unfair collection practices

Collection must also be by lawful means, which are 'fair in all the circumstances of the case'.[93] Intention to use personal data in an unfair manner is relevant to this.[94] In the *Hongkong Post* complaint, the surveillance was carried out in an unfair manner since the need for covert surveillance (particularly of unlimited duration) was not demonstrated. The PCPD notes numerous other instances of unfair data collection[95] including a hidden camera in a university hostel,[96] a teacher's secret audio recording of a conversation with his supervisor,[97] and 'blind' advertisements soliciting job applications to undisclosed data users where the purpose of collection is not in fact for employment recruitment. However, an airline's requirement that cabin crew disclose their full medical records for the previous year relevant to any extended sick leave, failing which disciplinary action would be taken, was found on appeal from an AAB decision not to be unfair collection. This was because, where a requirement is properly mandatory (as it was under civil aviation requirements), the consequences of non-compliance must be communicated.[98] The Commissioner considers this decision is confined to analogous situations of statutory justification for such demands.[99]

DPP 1(2) does not explicitly refer to 'intrusive means' of collection, but the Commissioner interpreted 'fair' to include 'not intrusive' in two 2012 complaints. The use of hidden cameras is a common practice in Hong Kong journalism.[100] Each complaint concerned 'paparazzi' style photo-journalism using systematic surveillance and telescopic lens photography to take clandestine photographs of TV personalities within their private

residences, **(p.95)** over a period of three to four days.[101] *Sudden Weekly* took long-distance photographs of a male TV star, undressed, within his flat on a high floor of a building not exposed to public view. *Face Magazine* published pictures of acts of daily life and intimacy between two unmarried TV personalities within a flat which faced a hillside some distance away. The Commissioner found both respondents in breach of DPP 1(2), and served enforcement notices directing the magazines to remedy their contraventions and the matters occasioning them. The AAB dismissed all five grounds of appeal by each of the respondents.[102] On the principal substantive issue of whether the taking of the photographs was fair in the circumstances, the appellants argued in the *Face Magazine* case that it was in the public interest for them to do so. They contended that public interest includes 'preventing the public from being misled by some statements or actions of an individual, and the interest of the public in knowing the truth', relying principally on *Campbell v MGN* 'for the proposition that where a public figure chooses to make untrue pronouncements about his or her private life, the press will normally be entitled to put the record straight'.[103] The AAB distinguished *Campbell* on three grounds: Campbell had 'gone out of her way' to deny her drug addiction to the media, whereas the TV personalities here had not done so, and had only denied cohabiting when pressed by the media; possession and use of illegal drugs is 'entirely different in nature' from cohabitation; and the captions on the photographs in *Face Magazine* made no mention of denials of cohabitation. The AAB agreed (as had the Commissioner) that public interest is one factor to consider as to whether or not the collection of personal data is unfair, but also that being in an occupation bringing a person to public notice 'is not in itself enough to make his private life a matter of public interest'. The AAB agreed that under these circumstances, the collection of the personal data was unfair. In Hong Kong, 'public figures' are therefore able to protect some aspects of their private lives.

Notice required on collection

When personal data is collected directly from the data subject, he or she must be given notice of standard matters including the purpose of collection, consequences of non-provision, the usual recipients of disclosures of the data, and access and correction rights and procedures.[104] Notice is not required where personal data is collected from third parties, or collected by observation of the data subject, or provided unsolicited by the data subject. Compliance with this notification obligation is also not required where this would prejudice purposes such as the prevention or detection of crime, for which an exemption from DPP 6 is provided (see section 3.3 of this chapter).

4.2. Use and disclosure limitations on personal data

The 'finality' principle is embodied in the requirement in DPP 1 that collection of personal data is limited to where it is necessary for a lawful purpose directly related to a function of the collector. Principle 3 then limits the use or disclosure[105] of personal data to the **(p.96)** purposes for which the data were to be used when they were collected, or a directly related purpose, unless the subject voluntarily gives 'prescribed' (express) consent to other uses. Disclosure 'includes disclosing information inferred from the data'.[106]

Hong Kong therefore takes a narrow view of allowable secondary uses and disclosures, by only allowing those that are directly related to the purpose of collection, or with express consent. This apparent strictness is mitigated by the Commissioner's willingness to take a broad view of the primary purpose of collection. For example, a social worker's purpose of collection of client data was considered to implicitly include compliance with any legal obligation to provide information to a court.

'Consent' is not defined, but 'prescribed consent', '(a) means the express consent of the person given voluntarily' and '(b) does not include any consent which has been withdrawn by notice in writing served on the person to whom the consent has been given…'.[107] Various provisions of the Ordinance require that the prescribed consent of the data subject must be obtained. Part VIA (direct marketing) has separate requirements of 'consent' defined to include 'an indication of no objection'.[108] The requirement that consent to other uses be 'prescribed consent', strengthens the purpose limitation principle, although its application is not always clear.[109] For example, a tutorial centre invited one of their students who had excelled in a public examination to come in to receive an award of HK$2,000 and be interviewed and photographed by a magazine, asking her to bring her examination notice with her as proof of examination.[110] They then used her examination notice (including personal information such as her ID number), which they copied without informing her, and her photo, in an advertisement for their tutorial centre, apparently a common practice. The Commissioner found that both uses of her information were breaches of DPP 3 because, even if such advertisements were a known practice, they did not have her voluntary and express prescribed consent. Implied consent is not sufficient.

When considering whether purposes are 'directly related' to the original purpose of collection, the Commissioner takes into account 'the nature of the transaction giving rise to the need for using the personal data and the reasonable expectation of the data subject'.[111]

The data user's purpose of collection, which should be stated when personal data is collected from the data subject, is not necessarily definitive of the allowed uses of the data. It may not be definitive if the discloser of the information imposes more narrow conditions,[112] or if (as the Commissioner puts it) the statement is so broad as to 'exceed its lawful function and activities and the reasonable expectation of the data subject', and numerous examples of the application of these criteria are available.[113]

Publicly available ('public domain') information

Hong Kong does not have any general exception from the use limitation principle for 'publicly available information', unlike countries such as Australia, and so DPP 3 applies to **(p.97)** use of information collected from such sources as public registries or Internet sites. In an example from 2002, a company contracted with a government department to obtain data from a public register relating to property transactions, then used the data for a purpose unrelated to the purpose for which they were collected by the government department, and without data subject consent to any broader use. The company was

prohibited from using the information for the broader purpose even though the personal information was (as the Commissioner put it) 'in the public domain'.[114]

The applicability of DPP 3 to publicly available information was reiterated in a 2013 investigation of an application for smartphones ('app') named 'Do No Evil' (the 'DNE app').[115] The database accessed by the DNE app contained the information from public registers and websites provided by Hong Kong public authorities including court hearings, bankruptcies, and company returns. The app allowed all of these sources to be searched simultaneously by a person's name, or part of their name, or other data. The Commissioner's decisions outlines 'a myriad of privacy concerns', but the breach of DPP 3 was because it was not the company's purpose of data collection that was the determining factor, but the purpose for which the government bodies made the data available. This purpose can be explicitly stated by the public body or 'is stated in the relevant legislation, either explicitly or implicitly'. The personal data may only be used for that purpose or a directly related purpose. The expectations of the government departments, and the data subjects, were relevant to determining what was a directly related purpose, but did not support the uses made here. The respondent stopped providing the app, and there was no appeal to the AAB, despite disquiet from some in Hong Kong.[116]

4.3. Data quality obligations and advising third parties

Principle 2[117] requires that all practicable steps be taken to ensure accuracy in relation to personal data (having regard to purpose of use and any directly related purposes), and to erase or not use inaccurate data. 'Inaccurate' is defined as 'incorrect, misleading, incomplete or obsolete'.[118] Inaccuracy is not in itself a breach, if the necessary 'practicable steps' have been taken to avoid it. The Commissioner may issue enforcement notices requiring systemic improvement if such steps are not in place. Data subjects may request correction of inaccurate information.[119] Where third parties have received 'materially' inaccurate data, the data user must, where practicable, inform the third party of this and such particulars as will enable them to rectify the data.[120]

4.4. Erasure (deletion) of data

Non-retention is effectively provided for in DPP 2(2), which requires that 'personal data shall not be kept longer than is necessary for the fulfillment of the purpose (including any directly related purpose)' for which the data are used or are to be used in future. The **(p.98)** provision is not explicit as to whether some form of de-identification of data may satisfy the requirement that 'personal data should not be kept'. However, there is a separate obligation to 'erase' such data, subject to exceptions where erasure is prohibited under law or its retention is in the public interest, including historical interest.[121] The Commissioner provides guidance on how these obligations may be carried out.[122] A deletion obligation is not found in the 1981 OECD Guidelines. Since Hong Kong allows 'prescribed consent' to collect data to be withdrawn, this also implies a right to block the use of data originating from the data subject, but not other data.

The Commissioner found that Hang Seng Bank had been retaining its customers'

bankruptcy data for 99 years, and that this contravened DPP 2(2) and section 26(1) of the Ordinance.[123] The bank undertook not to retain customers' bankruptcy data for more than eight years from the date of the declaration of bankruptcy and to erase older data already held, and this was accepted.

4.5. Data security obligations

Principle 4[124] on security of personal data requires that all practicable steps be taken to protect personal data against 'unauthorised or accidental access, processing, erasure, loss or use', having regard to factors including the kind of data, their physical location, the potential harm (that could result from such unauthorized or accidental access, processing, erasure, loss, or use), the security measures incorporated, and the measures to ensure the integrity of persons having access to the data. The Ordinance does not generally require special treatment of any class of 'sensitive data' (unlike European laws), but DPP 4 requires regard to be had to the kind of data, which would include consideration of the sensitivity of the data where increased harm would be likely to result from security breaches.

Only a few examples can be given here.[125] Security flaws in online billing systems are a frequent source of complaint, and are one area where the Commissioner seems to have succeeded in obtaining systemic changes by telephone companies, such as more secure password requirements. A hacker was able to access mobile phone subscribers' account records, including all details of their calls, by intentionally making five unsuccessful attempts to log in, knowing that the password would be automatically reset to a fixed number (e.g. 123456), which was applicable to all customers. The phone company had failed to provide adequate security by using a fixed instead of random password reset.[126] A subscriber to a mobile phone service provided personal documents to an agent of a dealer, and they were lost in the course of transfer to the dealer and then to the phone service operator. The dealer had breached the security principle by not having adequate procedures to ensure that the same documents left its agents as were provided to them.[127] Further examples are given in section 5.5 of this chapter in relation to ID numbers.

(p.99) Data breach notification

The 2012 Amendments do not include any data breach notification requirements, and the government's 2009 Consultation Paper merely said 'we consider it more prudent to start with a voluntary breach notification system'. This conclusion seemed at odds at the time with the very high levels of large-scale data breaches in both the public and private sectors in Hong Kong for at least the preceding three years. Hong Kong government agencies and companies continue to experience frequent episodes of data security breaches. In his 2011–12 Annual Report the Commissioner noted with alarm the apparently recurrent data leakage incidents in the public sector (50 cases) particularly those involving the police (7 cases) and public hospitals (6 cases). Hong Kong's public sector authorities have now reached agreement with the Commissioner that any data breach incidents will be promptly reported to the PCPD. Where an agency or company fails to notify the PCPD, and its customers or clients, of a significant data breach as quickly

as is appropriate, the Commissioner's only sanction would appear to be adverse publicity. In a December 2012 press release the Acting Privacy Commissioner expressed concern that a hospital had lost the registration cards of 174 patients but had failed to report the matter to the Commissioner, naming the particular clinic involved.

A mandatory scheme covering the private sector is probably unlikely for some time, but a voluntary scheme now operates for both sectors. The Commissioner has 'strongly advised' data users 'to give formal data breach notification ("DBN") to the affected data subjects, the Commissioner and any other relevant parties after a data breach has occurred',[128] noting that data breaches may well involve a beach of DPP 4. The PCPD received 61 voluntary DBNs in 2012–13 (32 from the public sector and 29 from the private sector, involving 17,451 individuals). In all cases the PCDP undertook a compliance check (see section 9.3 of this chapter) as a result.

4.6. 'Openness' concerning practices

Principle 5[129] requires data users to take all practicable steps to ensure that any person (not only data subjects) can ascertain their policies and practices with respect to personal data, the kinds of personal data they hold, and its main purposes of use. This OECD-derived 'openness' principle could be used by the media and others to investigate the operation of personal data systems but has not been so used as yet.

The main use of DPP 5 has been to enable the Commissioner to require Hong Kong organizations to publish a privacy policy statement (PPS). In the *Hongkong Post* complaint, the absence of a PPS was a breach of DPP 5, and the enforcement notice required it to formulate a general privacy policy on video monitoring activities, and communicate it regularly to staff. The AAB upheld a decision by the Commissioner that the Equal Opportunities Commission had breached DPP 5 but the Commissioner did not issue an enforcement notice because it subsequently issued a PPS.[130] There is flexibility in how a PPS may be published.[131]

Surveys conducted for the Privacy Commissioner show that 97 per cent of government organizations had prepared the legislatively required written privacy policy statements and personal information collection statements, but only 46 per cent had done so in the private **(p.100)** sector. Between 80 per cent and 90 per cent of respondents considered that compliance was beneficial to their organization in various ways, from a better public image to improved record keeping. Compliance was least likely from small organizations.[132]

5. Types of processing of special concern

Hong Kong has no general provisions dealing with processing of sensitive data, but particular types of processing are subject to special provisions within the Ordinance, including direct marketing, interconnection of files ('data matching'), ID cards, and numbers. Credit reporting has already been discussed.

5.1. Direct marketing (2012 Amendments)

The pre-2012 Ordinance required direct marketers to give consumers an ability to opt

out of further communications, as in many other jurisdictions. This has been held to apply to government agencies promoting government services. The use of personal data for direct marketing was allowed as an exception to DPP 3, subject to the 'opt-out' provision (section 34(1) of the Ordinance).[133] Direct marketing has always been one of highest sources of complaints to the Privacy Commissioner.[134] Hong Kong already has specific anti-spam legislation, with a 'do not call' register.[135]

A sweeping new Part VIA inserted into the Ordinance by the 2012 Amendments, in force since 1 April 2013, governs the use of personal data and the provision of personal data to others for use in direct marketing. The amendments are somewhat different from the 2011 Bill that was introduced into LegCo.[136] Where a data user intends to use personal data for its own direct marketing uses, the data subjects must be informed (either orally or in writing) of the data user's intention. The data subject's consent is required for this to occur.[137] The data subject must be informed of the kinds of personal data to be used, and the classes of 'marketing subjects' to be used (classes of goods, facilities or services to be offered, or purposes of donations or solicitations). This applies irrespective of the source of the personal data (whether collected from the data subject or not). Data subjects must be provided with a 'channel' through which they can communicate their consent (in writing or otherwise), but there is no requirement that they use that channel to so communicate. It is an offence for a data user to make use of personal data for its direct marketing unless it complies with these provisions. Liability on conviction is a fine up to HK$500,000 (US$64,500), or imprisonment for up to three years. A data user has a defence if they can prove that they 'took all reasonable precautions and exercised all due diligence' to avoid commission of an offence. There are 'grandfathering' provisions for previously collected **(p.101)** data,[138] but the data user has the burden of proving that they apply.[139] Data subject consent may be either general or selective.[140] If the consent is given orally, the data user must send a written confirmation within 14 days (with additional offences applying). The provision of fines up to HK$500,000 (or imprisonment for three years) for almost all breaches of these provisions, in comparison with the previous maximum of HK$10,000 is a major change.

Where a data user intends to provide personal data to another data user for the direct marketing purposes (only) of that separate data user, analogous provisions apply.[141] However, the notice of intention must be in writing, stating the intention to disclose, and must also include the classes of persons to whom the personal data is to be disclosed. The user's consent must also be in writing. If the data is provided for gain, the fine may be up to HK$1 million (US$129,000) or imprisonment for five years. The notice must also state that the data user intended to provide the data for gain (sale or other gain).[142]

Under either of these provisions, data subjects must be informed, again by the data user, the first time their personal data is used for direct marketing, that they may, without charge, require the data user to cease using their data for direct marketing.[143] This also applies to 'grandfathered' data[144] So there is both a pre-use opt-in and a post-use opt-out.

Data subjects may require a data user to 'cease to use' their data for direct marketing.[145] While it appears that this would allow anyone in Hong Kong to give pre-emptive 'do not market' notices to each data user, this is unnecessary because consent must be obtained before direct marketing occurs, or the grandfathering provision may be used.

Provisions in the 2011 Bill which allowed personal data to be sold for purposes other than direct marketing, and requiring data subjects to opt-out from direct marketing (rather than opt-in, as is now required), are no longer included.[146] The legislative process therefore strengthened the 2012 Amendments considerably.

5.2. Sensitive data and 'sensitive processing'

Hong Kong has no special provisions for processing of defined categories of 'sensitive' data. Nor does the Ordinance have special provisions for defined types of 'sensitive processing', except in relation to data matching and direct marketing, discussed separately in this part. There are no special provisions relating to automated decisions. The 2009 government Consultation Document considered 'classifying biometric data (such as iris characteristics, hand contour reading, and fingerprints) as sensitive personal data', but only to limit the collection of what is deemed 'sensitive'. This did not proceed.

Criminal records

Arrest and conviction records are not treated as public records in Hong Kong, and access to them is generally tightly controlled. However, Hong Kong follows the approach of other common law countries in that court decisions, although only from the higher courts, are published with the parties being identified, including for public access on the Internet. Hong Kong has had a special law concerning old convictions, the Rehabilitation of Offenders Ordinance, since 1986. Where it applies, it allows individuals to claim that **(p.102)** they have not had a previous conviction, and for such convictions not to be held against them in some other proceedings. However, the Ordinance has a very narrow scope, applying only where a person has no previous convictions, where an offence involves a sentence of less than three months' imprisonment (even if suspended) or a fine less than HK$10,000 (US$1,300), and only after a further three-year conviction-free period.[147]

5.3. Interconnection of files ('data matching')

The Ordinance regulates data matching. A 'matching procedure' is defined as the automated matching of personal data with respect to 10 or more individuals collected for different purposes with the aim of producing or verifying data that may result in the taking of adverse action against any of the individuals concerned.[148] Apart from matching of data collected for the same purposes, all matching is regulated.[149]

Such a matching procedure may not be carried out unless the data subject has consented, or there is other statutory permission, or the matching procedure has been consented to by the Privacy Commissioner under section 32.[150] The Commissioner is required to assess applications for data-matching approvals according to criteria set out

in Schedule 5,[151] which includes whether the matching is in the public interest, the likely adverse consequences to individuals, the safeguards in the procedures to be employed, and whether there are practical alternatives to the procedures. These criteria are an appropriate basis for decisions, but there is no requirement that the Commissioner consult any other parties (e.g. representatives of those likely to be affected) in making his decision, and no evidence in his reports that he does so.

Data matching is used extensively by agencies of Hong Kong's public sector, and is made technically much easier (and probably more accurate) by the near universal collection of ID card numbers as identifiers by other agencies, and by many private sector organizations as well. The only systematic public source of information on such practices is the brief details of each matching procedure approved (or re-approved) by the Privacy Commissioner, as noted in his annual reports.

In 2003–04 the Commissioner re-approved 28 matching requests (all from the public sector), involving six types of procedures.[152] In 1998–99, the Privacy Commissioner re-approved 22 matching procedures that were consented to in the previous year and gave consent to four new ones. All consents were in relation to matching procedures carried out in the public sector, such as matching to check eligibility for housing benefits. In 2012–13 the Commissioner received 56 applications, all between public sector bodies, of which one was refused (details are not given), two were withdrawn, and one was still under assessment at the time of writing, and the rest approved. Some applications have been found 'not to be a matching procedure'. There are no instances of private sector bodies seeking approval. **(p.103)** Matching of personal data is no doubt prevalent in the private sector, but it would generally fall outside the definition of data matching because it does not meet the 'different purposes' requirement.

5.4. Use of publicly accessible data (including 'public registers')

Hong Kong does not have special provisions concerning 'public registers' (government databases of personal data accessible to the public), but neither does it have any special exemptions from the DPPs for 'publicly available information'. The operation of the Ordinance on public registers must therefore be inferred from its general terms. DPP 3's use and disclosure limitations are of particular importance, as discussed in the Commissioner's 'Do No Evil' decision (see section 4.2 of this chapter). Other DPPs will also apply to public registers, such as access and correction rights, subject to any overriding provisions in the Ordinance governing a particular register. Operators of public registers should advise data users of the purposes for which it is legitimate to use data from a particular register, but the extent to which they do is not known.

5.5. Identity information—ID cards and numbers

Since its introduction at the end of World War II there has been general acceptance in Hong Kong of an ID card as a means of dealing with illegal immigration and border security. All persons over the age of 11 residing in Hong Kong are required to obtain an ID card, which includes a unique identification number. By law, a person 'in all dealings with government' must provide the ID number where required, notwithstanding any

other law to the contrary.[153] Prior to the 1996 privacy Ordinance, in the absence of any law that prevented this, the card and number were also required by a wide range of private sector organizations. In 1997 the Commissioner issued a Code of Practice on the ID number,[154] as required by the Ordinance.[155] The Code specifies, as a rebuttable matter of law, how the Ordinance applies to the ID number. The then Commissioner did not consider that a major 'roll back' of existing card and number uses was a viable option in the absence of specific statutory direction or a strong body of public support, and particularly because of the obligation to provide the number to government. However, the Code did achieve a degree of 'ringfencing' of existing uses, and continues to impose limits on excessive or careless card and number use in both sectors. The introduction of a chip-based 'smart' ID card in 2003[156] has had relatively little effect on this situation. The legislation has potential for 'function creep' in relation to uses of the ID card and ID number,[157] but this potential has not been abused in the decade since its passage.[158]

In the public sector, the Code does not impose limits on the collection of ID numbers by government agencies, and allows the ID numbers to be used as a multipurpose internal identifier by any organization.[159] The controls the Commissioner can impose on data matching (see section 5.3 of this chapter) are of increased significance because it is **(p.104)** technically so easy for Hong Kong agencies to collect and use ID numbers for matching purposes. In the private sector, the Code allows collection of ID numbers by an organization that requires some reliability of identification in order to avoid non-trivial losses[160] (but not in other situations) and allows their use as internal identifiers. The difficulty of collecting ID numbers by automated means imposes some practical limits, but these are diminishing. Copies of cards (e.g. by fax) may be required to verify identity remotely. ID numbers may be shared with other private sector organizations 'a purpose shared by both', but if the disclosure is for purposes of 'data matching', separate permission from the Commissioner is necessary.

The breadth of use of the ID card and number in Hong Kong is illustrated by complaints about them reported by the Commissioner. These also illustrate that, despite the breadth of uses allowed by the Code, both it and the DPPs underlying it are frequently breached, and that successive Commissioners continue to try to stop unnecessary and careless uses. An account of these complaints from 1997–2008, published elsewhere,[161] also illustrates the wide range of 'day to day' unspectacular events that are the typical substance of data privacy. Wrongful intentional disclosures in breach of DPP 3 make up the majority of ID complaints, in relation to both public sector and private sector bodies. Where actions cause inadvertent disclosures, or make it easier for disclosures to others to occur, this is treated as a breach of the security principle,[162] not the disclosure principle. Excessive collection[163] is a source of ID complaints despite the Code's liberal acceptance of collection of ID numbers, but does occur where collection has no bearing on protecting the interests of the collector but is merely convenient, and thus considered excessive. Personal identifiers are still the third highest category of complaint,[164] and continue to feature in major investigations.[165] The PCPD's continuing vigilance has at least prevented the use of the ID number and card being completely out of control in Hong Kong.

5.6. Provisions relating to the Internet

The Ordinance does not include any specific provisions relating to the Internet, and it shares the potential limitations of other data protection statutes drafted prior to the widespread uptake of Internet services. As discussed above, in the *Yahoo! Case* the AAB took a narrow approach to 'personal information' in relation to email and IP addresses.

Interferences with privacy which arise from the use of social network service (SNS) have few clear answers under the Ordinance. Where SNS operators are located outside Hong Kong, the lack of data export provisions and the uncertainty concerning the extraterritorial operation of the Hong Kong Ordinance (see the following section) makes any enforcement by data subjects against SNS operators very unlikely to succeed. Alternatively, individuals can be data users. Personal data held by an individual and concerned only with the management of that person's personal, family, or household affairs, or held only for recreational purposes, are exempt from the provisions of the DPPs.[166]

(p.105) This raises the question of whether personal data about others located on a SNS user's home page are 'held' by that individual. Since 'data user' means a person who 'either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data', it would seem likely that both the individual and the SNS operator are data users. But the individuals will be exempt if, say, they do not put appropriate security settings on embarrassing personal information about others. The Hong Kong situation is therefore typical in not doing anything about individual-to-individual invasions of privacy in the SNS setting.

6. International data transfers from Hong Kong

Various related issues must be considered, not only the lack of restrictions on data exports.

6.1. Territorial scope of the Hong Kong Ordinance

The extraterritorial scope of the Ordinance is uncertain. Normally, acts done by an agent are considered to be the acts of the (exporter) principal,[167] but if the agent is located overseas, then its acts occurring overseas will not be a breach unless the Ordinance has extraterritorial effect. The exporting data user will therefore only be liable if the Ordinance has extraterritorial scope. Starting with the general principle that LegCo can legislate extraterritorially against any conduct that is contrary to the 'peace, order and good government' of Hong Kong,[168] it would be necessary to find some express legislative intent of extraterritorial application, or that the subject matter of the Ordinance implied such a purpose.[169]

The only significant litigated instance to date is the AAB decision in the *Yahoo! HK Case*[170] (see section 3.1 of this chapter). Even though all the information flows and entities were situated entirely within the PRC, it was arguable that the Hong Kong Ordinance applied to the personal data involved because YHHK was legally able to control the data processing from Hong Kong. The Privacy Commissioner concluded that YHHK, in relation to this

disclosure, was not liable under the Ordinance, one of the grounds being that the Ordinance had no extraterritorial application. The AAB simply stated that section 39(1)(d) of the Ordinance, which empowers the Commissioner to refuse to carry out or continue an investigation when the case had no connection with Hong Kong is 'not a provision dealing with extra-territorial application of the Ordinance'. The extraterritorial extent of the Ordinance is therefore not clarified.

6.2. Data exports from Hong Kong

The restriction the Ordinance places on the transfer of personal data outside Hong Kong[171] is the only one of its provisions that has not been brought into force by the Secretary for Home Affairs.[172] Hong Kong does not, therefore, have at present any explicit restrictions on cross-border transfers.

(p.106) The position if section 33 of the Ordinance was in force

Section 33, which is not currently in force, requires that data users must not transfer to a place outside Hong Kong, any personal data the collection, holding, processing, or use of which takes place in Hong Kong, or was controlled by a data user whose principal place of business is in Hong Kong, unless one of five specified conditions was met:

> (a) the place is on a 'whitelist' prepared by the Commissioner (on the same grounds as (b) following);[173]
> (b) the user has reasonable grounds for believing that the place has in force 'law which is substantially similar to, or serves the same purpose' as the Ordinance;
> (c) the data subject has given written consent;
> (d) the transfer is reasonably believed to be for the benefit of the data subject, but whose consent cannot practicably be obtained; or
> (e) the data user has taken reasonable precautions and exercised due diligence to ensure that the data would not be processed etc. in ways which would be contraventions if occurring in Hong Kong.

This last condition would permit the use of contractual arrangements to achieve a comparable level of protection for the personal data that are to be transferred.[174] One problem with such contracts is that Hong Kong retains the doctrine of privity of contract, so it will not assist the data subject that there is a contract between the exporter and the overseas recipients, even if it does include provisions for the data subject's benefit. Only the exporter can enforce such a contract. However, the Hong Kong government is considering reform of the law concerning third party benefit contracts.[175]

The requirement in (a) and (b) of 'law' would not permit the transfer of personal data to a place where the only protection afforded is that of a non-statutory industry or sectoral codes of practice, and it is also questionable whether (e) would allow this. In this respect, section 33 may possibly be more strict than articles 25 and 26, the analogous provisions in the EU Directive. It is a separate question whether a patchwork of sectoral laws could have the same scope as the Ordinance.

The current position

The government's failure to bring section 33 into force has allowed extensive offshore processing of Hong Kong personal data[176] to continue without any protections being provided to data subjects, and as the current Commissioner says, 'the current protection for personal data transferred overseas is weak and far from comprehensive'.[177] There are a number of likely reasons for section 33 not being brought into force. It applies to data exports to 'a place outside Hong Kong', which includes mainland China. It is unusually extensive in scope because where a data user's principal place of business is Hong Kong, the restrictions apply whether or not Hong Kong is the place from where the data are transferred. Furthermore, there may be significant consequences for international trade **(p.107)** depending on which countries are included in a 'whitelist' prepared by the Commissioner. In case the section is brought into force, the current Commissioner has 'completed in 2013 a survey of 50 jurisdictions and developed a white list of places which have in force a data protection law which is substantially similar to, or serves the same purpose as the Ordinance.' He has provided a copy to the government,[178] but has not made it available to the public.

7. Rights of data subjects in Hong Kong

In Hong Kong, the data subject's rights of 'individual participation' are primarily the rights to seek access to or correction of their own personal data, plus some rights of notification. Rights to object to (opt-out from) direct marketing are supplementary to a consent-based (opt-in) approach.

7.1. Notices confirming processing

At the time of collection of personal data from the data subject, that person is required to be given notice of the purposes etc. of collection (see section 4.1 of this chapter). Where personal data is to be used for direct marketing, additional notification obligations arise (see section 5.1 of this chapter). There are no rights for a data subject to be notified of disclosures of their personal data as disclosures occur, except where disclosure for direct marketing use is intended. These are the only occasions on which data subjects have a right to be notified about aspects of processing.

7.2. Rights to object to forms of processing

Data subjects have the right to object to direct marketing by any data user, and in most cases must give consent before such marketing can occur (see section 5.1 of this chapter). Some other forms of processing require consent. There are no rights to object to other forms of processing, which are either within the terms of the Ordinance, or in breach of it, except as arise from data correction rights.

7.3. Access to and correction of data

Principle 6 provides rights of access to and correction of personal data. Individuals can also insist that 'their version' of events be put on file even if the data user does not agree to change a record.[179] Hong Kong does not have freedom of information legislation in the public sector, so the Ordinance provides the only legal rights of access to information. There are very detailed compliance requirements not dealt with here.[180]

An individual can ask a data user whether it holds personal data of which that individual is the subject, and to be supplied with a copy of such data,[181] but this does not extend to obtaining a list of documents held.[182] Either or both requests may be made.[183] Access requests are not required to be made in writing, and there is no express requirement for a **(p.108)** response to be made in writing,[184] except that where 'copies' are requested, documents must be provided if they exist.[185] The data subject is required to make clear what personal data is requested, and provide clarifying information if requested.[186] The Commissioner and the courts aim to prevent access requests being used for purposes of harassment or to indirectly achieve the purposes of other litigation.[187]

Where personal data is exempt from access it is also exempt from correction even if the data user has reasons to suspect its accuracy, because only data supplied as a result of an access request is subject to correction.[188] This is a deficiency in the Ordinance. Details of corrections made must be provided within 40 days.[189] Reasons for refusal of access or correction must be recorded in a logbook, which the Commissioner may inspect.[190] Such inspections are not known to occur.

If the data that are the subject of the refusal consist of an expression of opinion (including an assertion of fact that is unverifiable or not practicable to verify), and the data user is not satisfied that the opinion is inaccurate, the data user may refuse to comply with the request but is required to attach a note to the data, recording the matters that the requestor considers to be inaccurate.[191] A correction request must be made in writing, not verbally,[192] as must the corrections.

A significant addition to the usual OECD rights is that, if the data have been disclosed to a third party within the preceding 12 months, the data user is required to provide a copy of the corrected data to the previous recipients with a notice in writing stating the reasons for the correction, unless the data user has reason to believe the party concerned has ceased to use the data, or the data were obtained by the party from a public register.[193]

A data user may charge a reasonable fee for complying with a data access request, but not for complying with a data correction request, or for a refusal to comply with either an access or correction request.[194] 'Excessive' fees for complying with a data access request are prohibited, but not defined. The Commissioner has held some fees to be excessive.[195] For example, a bank set up a new fee structure intending to charge all customers a flat-rate fixed fee of HK$200 (US$25) for complying with a data access request to obtain copies of their personal data in the custody of the bank. The Commissioner considered that a data user is permitted to recover only the labour costs and actual out-of-pocket expenses incurred in locating, retrieving, reproducing, and sending the requested data to the requestor based on the work involved being done by a clerical or administrative staff. The bank failed to establish it had taken this approach, and was found to have imposed a fee structure that was liable to be excessive. The Bank abandoned the proposed fee structure before implementing it.[196] The Commissioner has issued guidance on appropriate fees.[197] Access and correction **(p.109)** requests are

involved in around 10 per cent of complaints received by the Commissioner.[198] No figures exist concerning how many people use these rights each year.

8. Reactive enforcement—remedies in individual cases

Prior to the 2012 Amendments, the Hong Kong Ordinance had a very limited and defective enforcement regime compared with many other data privacy laws. In summary, the Commissioner had no powers to award any remedies, and could only issue enforcement notices if continuing breaches of the Ordinance were likely. The criminal penalties for breaches were too trivial to be dissuasive, and the provisions for complainants to seek compensation from the courts were never used. Some Commissioners made good use of what powers they had, but there were limits to what they could achieve.

The amended Ordinance makes considerable improvements in relation to all these deficiencies but it remains to be seen whether the Commissioner, complainants, prosecutors, and the courts will make effective use of these new powers. The Commissioner's powers are still very limited, even after the 2012 reforms. In summary, he still cannot initiate prosecutions himself, or issue administrative fines (for minor breaches), or provide compensation to complainants. In effect, his most important powers are limited to ordering data users to comply with the provisions of the Ordinance, recommend prosecutions if they do not do so, and assisting complaints to pursue compensation claims. Since the 2012 reforms, he can serve an enforcement notice irrespective of whether the contravention will continue or be repeated.

8.1. Investigation of complaints—powers of the Commissioner and types of investigation

The Commissioner enforces the requirements of the Ordinance through his power to investigate suspected breaches and serve enforcement notices.[199] The power of investigation may be exercised either on complaint from an individual who alleges a breach in relation to his or her personal data, or on the Commissioner's own initiative or 'own motion'.[200] Any powers the Commissioner has can be exercised as the result of an own motion investigation, not only as the result of a complaint.

A form of 'class complaint' is possible. Where two or more individuals could each make a complaint about the same matter, any one of them may do so 'on behalf of all those individuals', and the provisions of the Ordinance (which otherwise do not specify any procedures to be followed) 'shall be construed accordingly'.[201]

The Commissioner has extensive investigative powers including powers to enter onto premises[202] and to require the furnishing of information and production of documents,[203] which are sometimes (if rarely) used. If, after investigating, the Commissioner concludes that a data user is contravening or has contravened a requirement of the Ordinance, he may serve an enforcement notice on the data user directing it to take the steps considered necessary to remedy the contravention.[204] The 2012 amendments deleted the requirement that the contravention must be likely to continue or be repeated, thus greatly strengthening the Commissioner's enforcement

powers. The 2012 Amendments give the Commissioner **(p.110)** more powers to disclose matters coming to his attention in the course of inspections and investigations.[205]

The Commissioner completed 1,502 complaint cases in 2011–12, but of those only 24 resulted in formal findings of contraventions of the Ordinance (approximately 2 per cent).[206] During the course of the complaint investigation process most complaints are withdrawn, not proceeded with, found unsubstantiated, or transferred to other authorities. More than 10 per cent (169) were 'resolved through mediation during preliminary enquiries' (but no details are given); 87 (6 per cent) were resolved after formal investigation, but of these, half (44) were discontinued when complainants decided not to proceed, and in 19 there was found to be no contravention. Of the 24 cases where contraventions were found, 21 resulted in remedial actions taken by the data user plus either warning notices by the Commissioner or undertakings given by the data user to remedy the contravention. The remaining three resulted in enforcement notices, discussed in the following part.

8.2. Enforcement notices

The Commissioner can issue an enforcement notice when he finds following investigation that a data user 'is contravening or has contravened' a requirement of the Ordinance (including a DPP).[207] The notice must specify steps needed to 'remedy' the contravention 'including ceasing any act or practice' and to 'prevent any recurrence'. This is stated in more specific terms than before the 2012 Amendments, but still does not unambiguously allow the Commissioner to specify any additional steps which may be needed to provide justice to the individual complainant(s). However, in dismissing the appeals in the *Face Magazine* and *Sudden Weekly* decisions, the AAB held that the Commissioner's powers[208] to give directions in an enforcement notice are not exceeded by including a requirement to the media organizations to prepare guidelines for their staff on how to comply with the Ordinance in relation to systematic monitoring and long-distance photography, to his satisfaction within 21 days. Such directions are able to be 'forward looking', dealing with possible contraventions that may occur in future, and requiring specific steps to be taken.

A breach of one of the principles is not by itself a criminal offence, but a breach of any other requirement in the Ordinance, such as contravention of an enforcement notice, is an offence.[209] So the Commissioner can enforce the principles by the threat of criminal sanction implied in an enforcement notice.[210] In what the Commissioner describes as 'making full use of the authority of the PCPD', 11 enforcement notices were issued in 2012 (prior to the Amendments coming into force), directing correction of non-compliant practices, compared with one enforcement notice issued in 2011. In 219 cases warning letters, and advice or recommendations to data users complained against, were sent. In addition, the Commissioner conducted 12 self-initiated formal investigations 2012, compared with 11 in 2011. In some cases these resulted from data breaches which came to the PCPD's attention via the press.

The 2012 Amendments therefore make modest changes to enforcement notices, allowing

them to be issued as a formal sanction whenever the Ordinance has been breached, without the previous need for the Commissioner to be of the opinion that the contravention will continue or be repeated (explained in the following section), and clarifying the specific steps that the Commissioner can require to be taken by data users. **(p.111)** This change does little in itself to provide compensatory remedies to complainants, nor to deter data users from future contraventions by punishment, but those improvements are found in other provisions.

The problem prior to 2012

A major limitation on the effectiveness of enforcement notices prior to 2012 was that they could only be served where the contravention was likely to be continued or repeated by the data user.[211] So, while valuable to protect other data subjects against continuing or future contraventions, such notices provided only a limited remedy to the complainant. Where a breach was not due to any systematic deficiency in the practices of the data user but had nevertheless already resulted in damage to the complainant's reputation, feelings, or finances, the only remedy provided by the enforcement notice was protection against a repeat or continuation of the breach. There were many instances prior to 2012 where, if a data user complied with the Ordinance after being notified that they were in breach, and there was no reason to consider that future non-compliance was likely, the Commissioner could not even issue an enforcement notice, and could do little other than 'name and shame' the data user by issuing a section 48(2) report (see section 8.6 of this chapter) naming them. This was the case in the Octopus scandal in 2010.[212] In relation to the police complaints 'data spill', despite the remedial steps that the Independent Police Complaints Commission (IPCC) had taken, the Commissioner was not convinced that the IPCC had yet taken all steps to make it unlikely that contraventions would be continued or repeated, so he did issue an enforcement notice. In the *Face Magazine* decision the AAB supported a similar approach by the Commissioner regarding when an enforcement notice was appropriate.[213]

8.3. Injunctive relief

Individuals have no explicit right to go directly to the courts to seek enforcement of the DPPs by injunctions against existing or proposed practices, only to complain to the Commissioner. Explicit statutory rights to seek injunctions do exist elsewhere, such as in section 98 of the Australian Privacy Act 1988. However, since a breach of a DPP is unlawful as a civil wrong (though not in itself an offence), it is very likely that a threat to breach, or a continuing breach, would be amenable to an application for an injunction where damages would not be an adequate remedy.

8.4. Offences

As a deterrent to future breaches, prosecutions following failure to observe enforcement notices were of little value prior to the 2012 Amendments. This is because they have occurred so infrequently and because the maximum statutory penalties were ridiculously **(p.112)** small, particularly in the context of the scale of commerce in Hong Kong. Cheung notes that of 44 referrals for prosecution in 1998–2009, only 9 convictions resulted.[214]

In 2012, the PCPD referred 15 cases to the police for consideration of prosecution, a 25 per cent increase compared to 2011. There were two convictions resulting from such referrals in 2011. 'In one case, the data user complained against was convicted of contravening sections 34(1) and 64(10) of the Ordinance for sending repeated direct marketing material despite the complainant's opt-out requests. In another case, a staff [member] of the data user complained against was charged with the offence of obstructing the Commissioner in serving summonses to the staff of the data user in the course of investigating a complaint, thus contravening section 64(9) of the Ordinance.'[215] The 2011–12 Annual Report notes that of the two cases resulted in convictions, the fines were for HK$1,000 (US$130) and $2,500 (US$320). Obviously these are very small fines, and the real financial penalty was probably the respondent's legal costs. Three convictions in one year is some progress, but the trivial nature of the fines defeats the deterrent message.

A large percentage of previous prosecutions arose from breaches of (pre-amended) section 34, which requires data users to cease further contact with the individual if the individual chooses to opt out from further such contact, and contraventions are an offence.[216] For example, a Hong Kong credit card company was convicted and fined HK$7,000 (US$900) in 2007, and a telecommunications company was fined HK$4,000 (US$515) in 2006, for continuing with email and telephone marketing (respectively) after the customers exercised their opt-out.

Offences of repeated contraventions and repeated non-compliance with enforcement notice

Contravention of an enforcement notice remains an offence (maximum HK$50,000 fine (US$6440)) but enforcement notices can now be issued without the Commissioner having to be of the opinion that continuing or repeated contraventions are likely. If the offence continues, there is a daily penalty of HK$1,000 (US$130). However, on a second conviction, these fines escalate to a maximum of HK$100,000 (US$13,000) and a daily penalty of HK$2,000 (US$260).[217] There is a defence of due diligence in complying with the notice.[218]

Another new offence deals with repeated contravention of a requirement under the Ordinance under the same facts, and so avoids the need for the issuing of a second investigation and enforcement notice. If a data user has complied with an enforcement notice (thereby exhausting it) and subsequently intentionally does the same act or commits the same omission, as specified in the required steps in the enforcement notice, the data user is liable to a HK$50,000 fine (US$6440) or imprisonment for two years.[219]

The 2009 Consultation Document discussed empowering the Commissioner to require data users to pay a monetary penalty for serious contraventions of DPPs,[220] and the Commissioner argued in favour of this. Although this type of 'administrative penalty' is not uncommon in other jurisdictions, such as in Macao and in the 2012 revisions to the Australian law, this was not pursued in the 2012 Amendments.

(p.113) Offence of disclosure of personal data obtained from a data user without

consent

A new offence has been created where a third party has obtained personal data from a data user without that data user's consent, and then disclosed the data with the intent of obtaining gain for themselves or another, or causing loss in money or other property to the data subject.[221] Another offence is where a third party has obtained personal data from a data user without that data user's consent, and discloses it such that (with no requirement of intent) 'the disclosure causes psychological harm to the data subject'.[222] Conviction of either offence carries penalties of a maximum fine of HK$100,000 (US$13,000) or imprisonment for five years. There are a number of defences to protect disclosures for the prevention of crime, where necessary to prevent or detect crime, where authorized by law, where it was believed the data subject had consented, and for a 'news activity' in the public interest.[223]

8.5. Rights of appeal and review arising from complaints

A complainant may appeal to the AAB, a quasi-judicial statutory body,[224] against a decision of the Privacy Commissioner not to issue an enforcement notice as a result of an investigation into the complaint.[225] Similarly, a data user can appeal to the AAB against the Commissioner's decision to issue an enforcement notice.[226] There is no appeal from the decision of the AAB to a court, but aggrieved parties can seek judicial review of AAB decisions. Individuals have occasionally been prepared to bring AAB cases, and this does give them their 'day in court' with little risk of costs being awarded against them—but still no compensation or other remedies (for which they must bring separate proceedings under section 66—see section 8.7 of this chapter).

The data subject can also appeal to the AAB against the Commissioner's decision not to investigate the data subject's complaint or to discontinue an investigation that had commenced.[227] This right of appeal is very important in helping ensure that data protection authorities do not abuse their powers to prevent complaints being investigated, and is a strong point of the Ordinance. As a public authority the Privacy Commissioner is also subject to judicial review of his actions, as is the AAB of its decisions. Such judicial review concerning the Ordinance has occurred infrequently but includes the important *Eastweek* case.

8.6. Public reports of breaches by data users ('naming and shaming')

'Naming and shaming' data users for breaches of data privacy laws is increasingly being used in Hong Kong as a sanction. The Commissioner has powers to issue a public report under section 48(2), arising from any investigation (whether based on a complaint, or self-initiated), where he considers it is in the public interest to do so, and such reports may name the data user but not the complainant or other individuals.[228]

Until 2005, only one such 'section 48(2) report' had ever been issued. This concerned the covert video-taping of a female university student by a male co-student in the early days of the Ordinance. In 2005, a local newspaper first reported that Hongkong Post had installed **(p.114)** pinhole cameras in the working areas of a Post Office (see section 4.1 of this chapter). After the consequent 'own motion' investigation, the Commissioner issued a

section 48(2) report finding that Hongkong Post had breached the principles in numerous ways previously discussed. An enforcement notice directed Hongkong Post to immediately cease the practice, destroy the records, formulate a general privacy policy on video monitoring activities, and communicate it regularly to staff. Subsequent reports concerned a 'data spill' by the Independent Policy Complaints Council, Yahoo!'s disclosures on the Chinese mainland, and collection of personal data by a credit provider, but in these cases the data user's identity was already known to the public, due to press publicity.

From 1997–2010, successive Commissioners issued only 15 reports, and these had not identified the respondents, other than where previous press reports meant that the respondent's identity was already public knowledge, so section 48(2) was not in effect being used as a 'name and shame' sanction. In June 2011 Commissioner Chiang adopted an explicit policy of naming data users wherever he considered that a section 48(2) report was justified,[229] with a few specified exceptions.[230] He made eight such 'name and shame' reports in 2011, eight in 2012, and six in 2013, all naming the respondent data users. He correctly says 'the sanctioning of public scrutiny has been stepped up'. Since 2011, banks, insurance companies, retailers with loyalty card schemes, and news magazines, have figured prominently among the data users named in the reports. There have now been 37 section 48(2) investigation reports from 1997–2013, with 22 of them since 2011 naming the respondent data users.

As well as now functioning as a 'name and shame' sanction, these reports are the most detailed accounts available of how the Commissioner applies and interprets the Ordinance, so they perform that valuable transparency function as well. All section 48(2) reports are available from the Commissioner's website.[231]

8.7. Compensation actions

Apart from the right to make a complaint to the Commissioner (who, as discussed, has few remedial powers, and no powers to award compensation), the only remedy available to individuals is through an action in the courts under section 66 of the Ordinance. Complainants have a statutory right of compensation for damage, including injury to feelings, arising from a contravention of the Ordinance, including a breach of a DPP. The data user has a full defence if it can show it has taken reasonable care to avoid the contravention, or if the contravention was because of inaccurate data received from a third party.[232] Compensation therefore depends on the data user's culpability, not the harm caused to the complainant.

Therefore to obtain compensation, individuals are required to start a civil action for compensation in a Hong Kong court. Prior to the 2012 Amendments, this had the attendant risk of litigation costs of the defendant being awarded against them if their claim failed (following normal Hong Kong practice), and no guarantee of anonymity. The **(p.115)** Privacy Commissioner did not have any specific function of mediating between the parties to reach a mutually satisfactory outcome, and in his many reported complaint summaries there are no references to compensation or damages being paid. Prior to

2012, it does not seem that the Commissioner played any significant role in obtaining compensation payments in informal settlement of disputes. He could not assist complaints in any section 66 litigation (in contrast to the Hong Kong practice in discrimination cases), and any section 48(2) report by him concerning a breach would not be admissible as evidence of the breach or the damage. The claim had to be proven *de novo*.

It seems therefore that complainants were left to their own resources to pursue compensation under section 66, but for whatever reason[233] this system did not work. There is believed to be only one successful claim under section 66[234] in the first 15 years of operation of the Ordinance, and one misconceived attempt. This contrasts with South Korea, where small compensation for breaches is routine, and with the practices in Australia and New Zealand, where compensation payments are a feature of orders and settlements, although still exceptional.

Legal assistance and other reforms in compensation actions (2012 Amendments)

After the 2012 Amendments, the District Court has exclusive jurisdiction over claims for damages for contraventions of the Ordinance, with the same remedies as are available from the Court of First Instance,[235] bringing the Ordinance into line with Hong Kong's equal opportunities legislation. The usual costs order in such proceedings is 'no order as to costs'.[236] The Commissioner may prescribe forms to assist complainants in asking questions of respondents. If the respondent replies, the reply will be admissible in evidence, but if the respondent intentionally does not reply, or the reply is evasive or 'equivocal', then the court can draw adverse inferences if it is just and equitable to do so.[237]

Another notable and desirable feature of the 2012 reforms to the Ordinance is that the Commissioner now administers a legal assistance scheme to assist those wishing to institute compensation actions. He must consider applications for assistance, and grant them where he 'thinks fit to do so'.[238] Factors which may be considered by the Commissioner include:

> the merits of the case; whether the case raises a question of principle and would establish useful legal precedents; whether it is unreasonable to expect the applicant to deal with the case unaided having regard to the complexity of the case (e.g. the applicant is an individual whilst the prospective defendant is a large corporation), and the resources allocated by the Government for the Scheme.[239]

Once an application is approved, the Commissioner may assist complainants by giving advice, arranging for a solicitor's or counsel's advice, or arranging for representation 'by **(p.116)** any person', including for 'giving effect to a compromise', and 'any other form of assistance which the Commissioner may consider appropriate'.[240] There seems therefore to be ample scope for the Commissioner, or the law, to assist in the negotiation of settlements or compromises of compensation claims. The Commissioner's costs would be met from any costs or expenses payable to the claimant (or arising from a settlement) as a first charge.[241] In the first nine months, 16 applications for legal aid have been made to the Commissioner, with one granted, five rejected, two withdrawn, and the rest still

under consideration.[242]

9. Systemic enforcement measures in Hong Kong

An assessment of the effectiveness of data protection legislation must take into account not only a Commissioner's reactive powers of complaint investigation, but also those powers which enable him to proactively influence the level of compliance so as to reduce complaints received. The Hong Kong Commissioner has an abundance of such functions and powers, and uses some of them effectively and others not at all.

9.1. Transparency—reporting complaint interpretations and outcomes

One of the most important systemic tools of a data protection agency (DPA) is simply to publish both the statistics of complaint investigation and (particularly) enforcement, and summaries of significant complaints that have interpreted and applied the legislation. By doing so, they provide the necessary 'feedback loop' to both potential complainants and data users (and their representatives), an essential component of responsive regulation. Hong Kong has some of the best practices in Asian jurisdictions. The publication of section 48(2) reports on complaints of particular significance, identifying the respondent as a 'name and shame' sanction (see section 8.6 of this chapter), and the publication of AAB decisions relevant to the Ordinance by the Commissioner (see section 2.4 of this chapter), are also important aspects of the transparency of the Hong Kong system.

Complaint statistics, including outcomes

Section 48(2) reports, while exceptionally valuable, account for only a tiny percentage of the complaints which are formally investigated by the Commissioner. The significant aspects of this 'silent majority' of cases can only be made known by publication of good statistics and selected complaints summaries. Complaint statistics in the Commissioner's Annual Reports are valuable but could be improved. Many complaints are resolved by mediation[243] rather than resulting in formal findings of contravention of the Ordinance. The statistics provided state the formal steps taken by the Commissioner,[244] but do not at present indicate what remedial outcomes for complainants[245] resulted from the complaints **(p.117)** resolved by mediation, or even from all of the complaints resulting in formal contravention findings.[246] Unless some indication of outcomes is given, an observer could incorrectly conclude that the Ordinance and its complaint procedures achieved very little indeed beyond a tiny number of prosecutions with insignificant fines, a few warning letters, and a small number of 'name and shame' reports concerning serious breaches. This conclusion would be incorrect,[247] but the only way it can be countered is for the Commissioner to report the details of 'remedial outcomes', i.e. the benefits that complainants do actually receive from the Ordinance. The Commissioner has decided that future reports[248] will include details of remedies resulting from complaint outcomes.[249] Systematic provision of information on remedial outcomes is rarely provided by any DPA, so this innovation will place Hong Kong further ahead in the transparency of its privacy enforcement.

Summaries of significant complaints

Details of some of the complaints investigated by the Commissioner have, since the

inception of the Ordinance, been provided on the Commissioner's website under the heading 'Complaint & Enquiry Casenotes',[250] and republished on the HKLII website.[251] They provide valuable practical information about how the PCPD administers and interprets the Ordinance, and are numerically the broadest source of such information. On the Commissioner's website they are categorized both by subject matter and by legislative provision ('By Provision/ DPPs/ COPs/ Guidelines').[252] There are nearly 300 such case notes from 1997–2012,[253] an average of almost 20 per year until 2009 when reporting stopped for three years; however, since mid-2013 reporting has resumed and the previous years are being caught up.[254]

9.2. Systemic examination of types of processing

The Ordinance does not require permits (or other prior permission) to be obtained for particular categories of processing, except for data-matching exercises (see section 5.3 of this chapter), and does not require privacy impact assessments (PIAs). The Commissioner is empowered to require a form of registration of some classes of data users ('data user returns'), but does not do so. Although he is empowered to do formal inspections of classes of data systems, he has instead developed a system of informal 'compliance checks'.

(p.118) Privacy impact assessments—lack of use

There are no powers in the Ordinance for the Commissioner to require PIAs to be carried out on potentially privacy-invasive systems before they are built (or legislated for), and data user returns (discussed in the following section) would not cover prospective systems, but PCPD has issued guidance on PIAs.[255] Few 'voluntary' PIAs are known to have been carried out in Hong Kong,[256] other than three of limited scope at various stages of development of the 'smart' ID card.[257]

Notification of processing—data user returns scheme (DURS) and 'accountability'

Part IV of the Ordinance deals with a form of registration of classes of data users. It empowers the Commissioner to specify classes of data users required to submit 'data user returns',[258] and the information to be included.[259] He would then compile a public register of this information.[260] Since the 2012 amendments he has new powers to require verification of such returns.[261] Successive Commissioners have not utilized Part IV, but the current Commissioner announced proposals in 2011 to apply it to the public sector, banking, telecommunications, and insurance. He has since 'put the project on hold' until it becomes clear how the EU will reform its own requirements for registration systems (including proposals for 'accountability' requirements and mandatory data protection officers).[262] However, he has requested data users in those four sectors to develop 'privacy management programs', by which they could at least have a demonstrable capacity to comply with the Ordinance.[263] The Commissioner is therefore expecting these sectors to voluntarily adopt something like the 'accountability' approach under consideration in Europe, while he defers the use of his statutory powers. It is a subtle use of the Commissioner's limited powers, but its value depends on the extent of compliance in the four sectors and whether the Commissioner measures this by compliance checks. The Commissioner claims 'significant buy-in' from these sectors.[264]

Hong Kong, therefore, has no register either of all data users or of data users in classes considered to be particularly dangerous to privacy interests. This is consistent with the lack of such registers in other Asia-Pacific jurisdictions until now, in contrast with the earlier European laws, which placed much stress on registration systems. However, registration of certain classes of data users is now required in Malaysia, and can be required in Macau.

9.3. Auditing compliance—inspections and compliance checks

The Commissioner has powers to carry out formal inspections of personal data systems, so as to make recommendations arising from such inspections to the data user concerned, or to members of a class of data users,[265] and to publish them.[266] The Commissioner **(p.119)** developed an inspection methodology manual in 1999,[267] but has only exercised his inspection power and published a 'section 48(1) report', on four occasions (once each in 2008, 2011, 2012, and 2013).[268] The last 2013 report, inspecting the installation of CCTVs on MTR trains and stations, is a substantial report of over 50 pages[269] which examines every aspect of compliance with the Ordinance from the question of whether CCTV collection of data might be excessive, through to deletion policies, and makes eight recommendations for improved practices.

Instead of using the formal section 48(1) powers, successive Commissioners prior to the current Commissioner had informally carried out what they call 'compliance checks'. These involve requesting specific data users to improve or remedy practices that have come to his notice as potentially contrary to the Ordinance (but falling short of commencing an 'own motion' investigation). Early examples included checks involving compliance with the code of practice on the Hong Kong identity card number, and compliance by Hong Kong-based websites.[270] In 2004–05 the Privacy Commissioner's Office carried out 95 compliance checks, 87 involving private sector organizations. More than half (48) were directed against those placing blind recruitment advertisements. Significant examples were included in each Annual Report. In 2012–13 the Commissioner carried out 220 compliance checks, the majority (73 per cent) of which related to private sector organizations. The two checks detailed in the Report indicate how extensive such checks can be, and the important systemic improvements that can result.[271] Checks on the security practices of 12 unnamed schools revealed that nine of them had inadvertently exposed personal data affecting 2,115 students on their websites. The investigation involved 20 hours of computer searching, and resulted in recommendations to the Education Bureau and follow-up talks at schools. A report to the Commissioner by a government department of three missing computers containing personal data of 5,161 persons resulted in extensive reforms to Departmental procedures.

10. Self and co-regulation and Codes of Conduct in Hong Kong

Self-regulatory or co-regulatory codes have played relatively little role in Hong Kong. The Commissioner has the power to approve and issue Codes of Practice codifying how the Ordinance may be complied with by a particular sector or in relation to a particular activity.[272] Non-compliance with a requirement of such a code of practice does not itself amount to a contravention of the Ordinance, but in legal proceedings it is admissible in

evidence and raises a rebuttable legal presumption against the data user concerned.[273] It would also weigh unfavourably against the data user in any case before the Privacy Commissioner.[274] Part III is silent on whether compliance with a Code constitutes compliance with the Ordinance. It does not, but it would influence the Commissioner when considering enforcement, or a court that was considering whether a data user had acted reasonably, and any penalty in the event that a breach was found.

(p.120) In Hong Kong as in other jurisdictions, special industry codes have generally not proved popular. Three codes of practice have been issued, on the identity card number and other personal identifiers, on consumer credit data, and on human resources management. The first two Codes can be seen as legitimating and expanding surveillance practices as much as they can be seen as clarifying the Ordinance.[275]

11. Conclusions—Asia's leader in data privacy

Hong Kong has the longest-established comprehensive data privacy law in Asia. Until very recently it has lacked an adequate range of enforcement measures, but this was significantly improved by 2012 reforms. It is therefore possible to make an overall assessment of its privacy standards, enforcement structures and their use, and transparency. Hong Kong compares well with other jurisdictions (see Chapters 17 and 18).

11.1. Privacy standards in Hong Kong

The context of Hong Kong's privacy Ordinance is relatively supportive, with constitutional and treaty protections of privacy, though lacking a history of common law protections. The privacy standards in the Ordinance, while largely based on the minimum principles of the 1980s, go beyond them by including later European principles of minimum collection, direct marketing opt-out, deletion, prior checking (although not yet used), and destination-based data export restrictions (although not yet in force). Perhaps more significant is their overall very careful drafting and relative lack of exemptions, leading to generally sensible results when applied. Recent strong applications of the Ordinance (by the Commissioner and the AAB) in such areas as re-use of 'public domain' data, and intrusive photo-surveillance by the media, have shown that the principles can have considerable 'bite' when applied energetically.

11.2. Effectiveness of enforcement within Hong Kong

There are two separate questions: does the amended Ordinance yet provide a sufficient range and strength in its enforcement measures; and how vigorously and effectively do the Commissioner and the courts use the enforcement powers provided? Prior to the 2012 amendments, the enforcement powers were completely sub-standard. The new high penalties for commercial misuse of data (particularly in direct marketing), the higher penalties for repeated contraventions, the availability of enforcement notices for any type of contravention, and the improvements to the civil compensation measures, appear on paper to be a major improvement. However, the Commissioner still cannot grant compensation or issue fines, so effectiveness continues to depend on serious convictions and penalties, resulting from the work of prosecutors and courts. It remains to be seen

whether the new offences will remedy the previous low conviction rates and derisory fines.

While the Commissioner is still hampered by limited powers, he can issue enforcement notices far more readily, and the AAB has endorsed his giving specific directions in relation to future conduct. Within the previous constraints the current Commissioner was already making vigorous use of his powers, as indicated by the increasing use of all of the enforcement mechanisms of the Ordinance, and his use of section 48(2) 'name and **(p.121)** shame' reports. The effectiveness of enforcement should improve further with the new powers available following the 2012 reforms. The use of systemic measures to encourage compliance, such as education and training, and inspection powers, is probably as good as is found anywhere (assisted by Hong Kong's small size).

11.3. Transparency regarding data privacy in Hong Kong

There are more judicial, quasi-judicial (AAB) and DPA interpretations of the Ordinance, and published examples of its application, than is found in relation to data privacy laws in any other Asian country (or most countries, internationally). Transparency, in relation to both standards and enforcement, is probably the strongest aspect of Hong Kong's system, and the reporting practices will benefit further from the improvements proposed by the Ordinance.

Notes:

([1]) Benny Y.Y. Tai, ch. 2 'Hong Kong: Maintaining a Common Law Legal System in a Non-Western Culture' in E. Ann Black and Gary F. Bell, *Law and Legal Institutions of Asia: Traditions, Adaptations and Innovations* (Cambridge University Press, 2011), p. 62.

([2]) Yash Ghai, *Hong Kong's New Constitutional Order, The Resumption of Chinese Sovereignty and the Basic Law* (Hong Kong University Press, 2nd Edn., 1999), p. 56.

([3]) Constitution of the People's Republic of China, art. 31.

([4]) Basic Law of the Hong Kong Special Administrative Region of the People's Republic of China <http://www.basiclaw.gov.hk/en/basiclawtext/cover.html>.

([5]) Basic Law (HK), art. 2.

([6]) For an introduction, see Tai, ch. 2 in Black and Bell, *Law and Legal Institutions of Asia*, pp. 66–75.

([7]) 'The ultimate aim is the selection of the Chief Executive by universal suffrage upon nomination by a broadly representative nominating committee in accordance with democratic procedures': Basic Law (HK), art. 45.

([8]) Basic Law (HK), art. 68.

([9]) Basic Law (HK), art. 8. There is an exception for those previous Hong Kong laws found to be inconsistent with the Basic Law, of which there were few examples, not relevant

here.

([10]) Decisions of the Privy Council pre-1997 remain binding on Hong Kong courts, but those post-1997 only have persuasive effect: Tai, ch. 2 in Black and Bell, *Law and Legal Institutions of Asia*, p. 69.

([11]) Tai, ch. 2 in Black and Bell, *Law and Legal Institutions of Asia*, pp. 75–8.

([12]) For a succinct discussion, see Tai, ch. 2 in Black and Bell, *Law and Legal Institutions of Asia*, pp. 78–9.

([13]) J. Chan and C.L. Lim (Eds.), *Law of the Hong Kong Constitution* (Sweet & Maxwell, HK, 2011), pp. 60–5.

([14]) For further details of surveillance practices see Robin McLeish and Graham Greenleaf, ch. 8 'Hong Kong' in James B. Rule and Graham Greenleaf (Eds.), *Global Privacy Protection: The First Generation* (Edward Elgar, 2008). See also Graham Greenleaf, 'Country Studies: B3 Hong Kong' in D. Korff (Ed.), *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments* (European Commission, 2010), <http://ssrn.com/abstract=2025550> (hereinafter 'Korff, European Commission study').

([15]) Graham Greenleaf, 'Hong Kong's "Smart" ID Card: Designed to Be Out of Control' in Colin Bennett and David Lyon (Eds.), *Playing the Identity Card* (Routledge, 2008) <http://ssrn.com/abstract=2027862>.

([16]) For a more detailed discussion, and references, see McLeish and Greenleaf, ch. 8 in Rule and Greenleaf (Eds.) *Global Privacy Protection*, pp. 231–2, or Greenleaf, 'Hong Kong' in Korff (Ed.), *European Commission study*.

([17]) See the Hong Kong Law Reform Commission reports: *Report on Privacy: Regulating the Interception of Communications* (1996); *Report on Reform of the Law Relating to the Protection of Personal Data* (1994); *Privacy and Media Intrusion* (2004); *Civil Liability for Invasion of Privacy* (2004) and *Privacy: The Regulation of Covert Surveillance* (2006), all available at <http://www.hklii.org/hk/other/hklrc/reports/>.

([18]) For examples, see Anne Cheung, 'An Evaluation of Personal Data Protection in Hong Kong Special Administrative Region (1995–2012)' (2013) 3(1) *International Data Privacy Law*, pp. 29–41; Mark Berthold and Raymond Wacks, *Data Privacy Law in Hong Kong* (Pearson Professional (Hong Kong) Ltd, 1997); Mark Berthold and Raymond Wacks, *Hong Kong Data Privacy Law: Territorial Regulation in a Borderless World* (Thomson, Sweet & Maxwell Asia, 2002); Raymond Wacks, *Personal Information: Privacy and the Law* (Clarendon Press, 1989), and Doreen Wiesenhaus, *Hong Kong Media Law: A Guide for Journalists and Media Professionals* (2nd Edn., Hong Kong University Press, 2014).

([19]) The reports and the UNHRC responses are at Human Rights Report—ICCPR (Constitutional and Mainland Affairs Bureau, 2014)

<http://www.cmab.gov.hk/en/press/reports_human.htm>.

([20]) UNHRC, *Concluding observations on the third periodic report of Hong Kong, China, adopted by the Committee at its 107th session (11–28 March 2013)* (UNHRC CCPR/C/CHN- HKG/CO/3, 2013).

([21]) *HKSAR v Yeung Wai Birney* [2012] HKCA 109 [122]; CACC176/2010 (2 March 2012), <http://www.hklii.hk/eng/hk/cases/hkca/2012/109.html>.

([22]) For details, see McLeish and Greenleaf, 'Hong Kong, in Global Privacy Protection', section 'Constitutional protections of privacy and the crisis over surveillance laws', pp. 234–5.

([23]) *Wainwright v Home Office* [2003] UKHL 53; [2004] 2 AC 406.

([24]) See *Vidal-Hall v Google Inc* [2014] EWHC 13 (QB).

([25]) *Campbell v MGN Ltd* [2004] UKHL 22; [2004] 2 AC 457.

([26]) Wiesenhaus, *Hong Kong Media Law*, pp. 118–19; *Chor Ki Kwong David v Lorea Solabarrieta Cheung*, [2013] HKCFI 1625.

([27]) *Lau Tat Wai v Yip Kuen Joey* [2013] HKCFI 639. See also *Wong Yat Keung Billy v Kai Shun International Accounting Co Ltd* [2013] HKDC 1475.

([28]) See *Malcomson Bertram & Anr v Naresh Mehta* [2001] 4 SLR 454 at 470H to 474A. However, there are now contrary decisions in Singapore: see Chapter 10, section 1.4.

([29]) *Lau Tat Wai v Yip Kuen Joey* [2013] HKCFI 639, para. [64].

([30]) See the lengthy discussion in Rick Glofcheskli, *Tort Law in Hong Kong* (3rd Edn., Hong Kong: Sweet & Maxwell Asia, 2012), pp. 13–15.

([31]) HKLRC, *Civil Liability for Invasion of Privacy* (HKLRC, 2004).

([32]) Hong Kong Law Reform Commission, *Report on Stalking* (HKLRC, 2006).

([33]) McLeish and Greenleaf, 'Hong Kong, in Global Privacy Protection', pp. 238–9; Greenleaf, 'Hong Kong', in Korff, European Commission study', section titled 'Origins of and influences on the Ordinance'.

([34]) HKLRC, *Report on Reform of the Law Relating to the Protection of Personal Data* (1994).

([35]) Personal Data (Privacy) Ordinance of 1995 (PDPO (HK)), s. 5.

([36]) PDPO (HK), s. 8.

([37]) Based on comparison of figures in PCPD, *Annual Report 2012–13* and PCPD, *Annual*

Report 2005–06.

([38]) Constitutional and Mainland Affairs Bureau, *Consultation Document on Review of the Personal Data (Privacy) Ordinance* (Hong Kong government, 2009).

([39]) For this history, see Allan Chiang, ch. 11 'Reviewing the Personal Data (Privacy) Ordinance through Standstill and Crisis' in Michael Tilbury, Simon N.M. Young, and Ludwig Ng (Eds.), *Reforming Law Reform* (Hong Kong University Press, forthcoming 2014) <http://www.pcpd.org.hk/english/files/infocentre/speech_20110917.pdf>.

([40]) There are 293 on the Commissioner's website, and 278 casenotes republished (slightly in arrears) on *Office of the Privacy Commissioner for Personal Data Complaint Case Notes* (HKLII, 2014) <http://www.hklii.hk/eng/hk/other/pcpd/complaint/>. On the HKLII website the full texts of the decisions are searchable.

([41]) See 37 section 48(2) reports on *Investigation Report/Inspection Report* (PCPD, 2014) <http://www.pcpd.org.hk/english/publications/invest_report.html>.

([42]) PCPD, *Data Protection Principles in the Personal Data (Privacy) Ordinance—from the Privacy Commissioner's perspective* (2nd Edn., PCPD, 2010), 163 pages (hereinafter 'PCPD *Principles*'). The first edition was in 2006. Most aspects of the Ordinance have not been subject to AAB or judicial interpretation, and PCPD must act as if their interpretation of the Ordinance is correct. It constitutes the *de facto* law.

([43]) See 108 decisions reported at Office of the Privacy Commissioner for Personal Data Administrative Appeals Board Decisions (HKLII, 2014) <http://www.hklii.hk/eng/hk/other/pcpd/AAB/>. These may not be comprehensive, omitting some decisions in Chinese only.

([44]) A search on HKLII <http://www.hklii.hk> shows 13 decisions in English but there are some additional decisions only in Chinese. Both the Commissioner and the Ordinance are mentioned in other cases, but rarely in any significant context.

([45]) Cheung, 'An Evaluation of Personal Data Protection in Hong Kong Special Administrative Region (1995–2012)', pp. 29–41.

([46]) PDPO (HK), s. 3(1) confirms that the Government of the HKSAR is bound.

([47]) PDPO (HK), s. 2 definition 'personal data'.

([48]) PDPO (HK), s. 2.

([49]) *Eastweek v Privacy Commissioner* [2000] 1 HKC 692.

([50]) PCPD, 'Verbal disclosure of information about an individual', [1999] HKPCPD 2 (HKLII).

([51]) *Kenneth Poon Sai-Ho and PCPD* [2000] HKPCPDAAB 16; AAB No. 16/2000.

([52]) *Kenneth Poon Sai-Ho and PCPD*, p. 9.

([53]) *Wu Kit Ping v AAB* [2007] HKCFI 1104; [2007] 5 HKC 450.

([54]) Respectively, AAB No. 14/2007, and AAB No. 49/2001.

([55]) PDPO (HK), s. 39(2)(b); see PCPD *Principles*, p. 10.

([56]) *Shi Tao and PCPD* [2007] HKPCPDAAB 16; [2008] 3 HKLRD 332.

([57]) PDPO (HK), s. 2(1), definition of 'data user' says it 'means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data'.

([58]) *Shi Tao v Privacy Commissioner for Personal Data* [2008] 1 HKC 287.

([59]) PDPO (HK), s. 2(12).

([60]) PDPO (HK), s. 26(2)(a).

([61]) PDPO (HK), s. 52.

([62]) PDPO (HK), ss. 57, 58.

([63]) *Lily Tse Lai Yin & Others v The Incorporated Owners of Albert House & Others* [2001] HKCFI 976.

([64]) PDPO (HK), ss. 53, 56.

([65]) PDPO (HK), s. 60.

([66]) PDPO (HK), s. 59.

([67]) PDPO (HK), s. 62.

([68]) PDPO (HK), s. 51A.

([69]) PDPO (HK), s. 63B.

([70]) PDPO (HK), s. 63C.

([71]) PDPO (HK), s. 63D.

([72]) PDPO (HK), s. 61(1).

([73]) PDPO (HK), s. 61(2) referred to as a '"whistle-blower" provision' in Berthold and Wacks, *Hong Kong Data Privacy Law*, pp. 355–7.

([74]) For discussion of media-related cases, see Weisenhaus, *Hong Kong Media Law*, pp.

105–11.

([75]) PCPD, 'Display of Identity Card Number in a newspaper article' [2001] HKPCPD 4.

([76]) *Apple Daily Ltd and Privacy Commissioner for Personal Data* [1999] HKPCPDAAB 5 <http://www.hklii.hk/eng/hk/other/pcpd/AAB/1999/5.html>.

([77]) HKLRC, *Report on Reform of the Law Relating to the Protection of Personal Data*, para. 6.2.

([78]) M.M.Y. Suen (Sec. Home Affairs, HK) Second Reading Speech, Personal Data (Privacy) Bill (Hong Kong Legislative Council, 19 April 1995).

([79]) PDPO (HK), Sched. 1.

([80]) PDPO (HK), s. 2.

([81]) PDPO (HK), Sched. 1, DPP 4.

([82]) PDPO (HK), Sched. 1, DPP 1(1).

([83]) *Eastweek v Privacy Commissioner* [2000] 1 HKC 692.

([84]) *Eastweek*, per Ribeiro JA, at 90I, and similarly put by Godfrey VP, at 102D.

([85]) *Eastweek*, per Ribeiro JA, at 93C.

([86]) PCPD *Principles*, p. 18.

([87]) PCPD *Principles*, pp. 20–2.

([88]) See *Kirpalani and PCPD* [2006] HKPCPDAAB 55; AAB No. 55/2006; see also PCPD *Principles*, p. 20.

([89]) PCPD, 'University Refusing to Comply with Data Access Request in Relation to Examination Marking' (PCPD, s. 48(2) Report R08-10578, 19 January 2009).

([90]) PCPD, 'The practice of collection of employees' personal data by pinhole cameras without proper justification is excessive and unfair in the circumstances of the case' (PCPD, s. 48(2) Report R05-7230, 8 December 2005).

([91]) PCPD, 'Food Company Collecting Participants Personal Data in Lucky Draw Activity' (PCPD, s. 48(2) Report R09-3658, 7 August 2009).

([92]) PCPD, 'Employer Collecting Employees Fingerprint Data for Attendance Purposes' (PCPD, s. 48(2) Report R09-7884, 13 July 2009).

([93]) PDPO (HK), Sched. 1, DPP 1(2).

([94]) *Eastweek v PCPD* [1999] HKCFI 433, per Keith JA at para. 23 (at first instance).

([95]) PCPD *Principles*, pp. 37–9.

([96]) PCPD, s. 48(2) Report R97-1948, 13 October 1997.

([97]) *Hui Kee Chun and PCPD* [2006] HKPCPDAAB 46; AAB No. 46/2006.

([98]) *Cathay Pacific Airways Ltd v AAB and Anor* [2008] HKCFI 734; [2008] 5 HKC 229.

([99]) PCPD *Principles*, p. 38.

([100]) Weisenhaus, *Hong Kong Media Law*, p. 108.

([101]) PCPD, 'Unfair Collection of an Artiste's Personal Data by Face Magazine Ltd' (PCPD, s. 48(2) Report R12-9164, 28 March 2012); PCPD 'Unfair Collection of an Artiste's Personal Data by Sudden Weekly Limited' (PCPD, s. 48(2) Report R12-9159, 28 March 2012).

([102]) *Face Magazine Ltd and the PCPD* [2012] HKPCPDAAB 5; *Sudden Weekly Ltd and the PCPD* [2012] HKPCPDAAB 6. The decisions were handed down on 6 January 2014.

([103]) *Campbell v MGN Ltd* [2004] 2 AC 457.

([104]) PDPO (HK), Sched. 1, DPP 1(3).

([105]) PDPO (HK), s. 2(1) defines 'use' of personal data as including 'disclosure or transfer' of such data.

([106]) PDPO (HK), s. 2 definition of 'disclosing'.

([107]) PDPO (HK), s. 2(3).

([108]) PDPO (HK), s. 35H and definition in s. 35A(1).

([109]) Difficulties of interpretation are discussed in PCPD *Principles*, pp. 63–4.

([110]) PCPD, 'Tutorial Centre Using a Student's Results Notice for Promotion without the Student's Consent' (PCPD, s. 48(2) Report R09-2902, 3 August 2009).

([111]) PCPD *Principles*, pp. 60–3.

([112]) Examples and decisions by various Commissioners on this point are inconsistent: see PCPD *Principles*, pp. 56–8. The AAB decision in □□□ *and PCPD* [2006] HKPCPDAAB 41 is best understood as a situation where s. 58 makes DPP 3 inapplicable.

([113]) PCPD *Principles*, pp. 55–7.

([114]) PCPD, 'Use of Personal Data Obtained from a Public Register' [2002] HKPCPD 4

(HKLII). See also PCPD *Principles*, pp. 59–60.

([115]) PCPD, 'Glorious Destiny Investments Limited and Brilliant United Investments Limited Publicly Disclosed Litigation and Bankruptcy Information Collected from the Public Domain to Their Customers via Smartphone Application "Do No Evil"' (s. 48(2) Report R13-9744, 13 August 2013).

([116]) For an analysis see Graham Greenleaf, 'Private Sector Uses of "Public Domain" Personal Data in Asia: What's Public May Still Be Private' (2014) 127 *Privacy Laws & Business International Report*, pp. 13–15.

([117]) PDPO (HK), Sched. 1, DPP 2.

([118]) PDPO (HK), s. 2(1) definition of 'inaccurate'.

([119]) PDPO (HK), s. 22.

([120]) PDPO (HK), DPP 2(1) in Schedule 1.

([121]) PDPO (HK), s. 26(1).

([122]) PCPD *Principles*, pp. 50–2.

([123]) PCPD, 'Prolonged Retention of Customers' Bankruptcy Data by Hang Seng Bank Limited' (PCPD section 48(2) Report R11-6121, 15 December 2011).

([124]) PDPO (HK), Sched. 1, DPP 4.

([125]) For numerous examples of such considerations, see PCPD *Principles*, pp. 67–72.

([126]) PCPD, 'Randomly assigned instead of fixed reset password preferred when reactivating a lockout account', [2003] HKPCPD 5.

([127]) PCPD, 'Loss of documents when subscribing to a mobile phone service', [2001] HKPCPD 3.

([128]) PCPD, 'Data breach notification' (PCPD Annual Report 2012–13), p. 83.

([129]) PDPO (HK), Sched. 1, DPP 5.

([130]) *Priscilla Sit Ka-Yin and PCPD* [2000] HKPCPDAAB 15.

([131]) PCPD *Principles*, pp. 74–6.

([132]) Social Sciences Research Centre, University of Hong Kong, *2004 Data Users Opinion Survey* (PCPD, 2004) <http://www.pcpd.org.hk/english/publications/annualreport2005_20.html>.

([133]) Under the previous s. 34(1), the first time that a data user made a marketing

communication (e.g. in a 'cold-call' telemarketing approach or 'mail shot') it must inform the data subject that if he or she so requests, it will (at no charge) cease using their personal data for direct marketing. This information must be given to the data subject even if the data were collected directly from the subject and he or she gave consent at that time to their being used for direct marketing. If the data subject made such a request, the data user must comply with it.

([134]) In 2003–04, 71 complaints were the fourth-highest category: HKPCO *Annual Report 2003–04* (HKPCO, 2004).

([135]) Unsolicited Electronic Messages Ordinance (HK).

([136]) For details of the proposals in the Bill, see Robin McLeish and Graham Greenleaf, 'Reform of Hong Kong's Privacy Ordinance After 15 Years' (2011) 113 *Privacy Laws & Business International Report*, pp. 15–17, <http://ssrn.com/abstract=1972669>.

([137]) PDPO (HK), ss. 35C and 35E.

([138]) PDPO (HK), s. 35D.

([139]) PDPO (HK), s. 35C(7).

([140]) PDPO (HK), s. 35E.

([141]) PDPO (HK), ss. 35J, 35K.

([142]) PDPO (HK), s. 35K(1)(b).

([143]) PDPO (HK), s. 35F.

([144]) PDPO (HK), s. 35G.

([145]) PDPO (HK), s. 36G(1).

([146]) See McLeish and Greenleaf, 'Reform of Hong Kong's Privacy Ordinance After 15 Years'.

([147]) CLIC, 'The Rehabilitation of Offenders Ordinance' (Community Legal Information Centre, undated) <http://www.clic.org.hk/en/topics/policeAndCrime/>.

([148]) PDPO (HK), s. 2.

([149]) Although s. 30(1)(d) of the Ordinance exempts matching 'required or permitted under any provision of any ordinances specified in Schedule 4', there is none yet specified.

([150]) PDPO (HK), s. 30(1).

([151]) PDPO (HK), s. 32.

([152]) The six types of procedures given new approvals in the previous two years were: by the Housing Society to compare Housing Authority records to prevent 'double dipping' of housing benefits; by the Student Financial Assistance Authority to prevent 'double dipping' with another educational benefit; by the Social Welfare Department with Immigration Department travel movement records to identify those who fail to meet a residence requirement for a benefit; by the Housing Society against records of the Buildings Department and the Urban Renewal Authority to prevent duplicate loans being granted; and by each of these last two authorities against the records of the other two, for the same purpose.

([153]) Registration of Persons Ordinance (ROPO), s. 5(1)(b).

([154]) PCPD Code of Practice on the Identity Card Number and Other Personal Identifiers (PCPD, December 1997) <http://www.pcpd.org.hk/english/ordinance/code_id.html>.

([155]) PDPO (HK), s. 12(8).

([156]) Registration of Persons (Amendment) Ordinance 2003.

([157]) Greenleaf, *Global Privacy Protection*.

([158]) See Greenleaf, 'Hong Kong's "Smart" ID Card' in Bennett and Lyon (Eds.), *Playing the Identity Card*, pp. 75–92. The position has not changed.

([159]) PCPD, *ID Code* (PCPD, 1997), paras. 2.3.1 and 2.3, particularly para. 2.3.3.3.

([160]) PCPD, *ID Code* (PCPD, 1997), para. 2.6.3.

([161]) Greenleaf, 'Country Study: Hong Kong' in Karff (Ed.), *European Commission Study*, section titled 'ID card complaints illustrate "day to day" privacy protection'.

([162]) PDPO (HK), Sched. 1, DPP 4.

([163]) PDPO (HK), Sched. 1, DPP 1.

([164]) PCPD, *Annual Report 2012–13* (PCPD, 2013), p. 50.

([165]) PCPD, *Annual Report 2012–13* (PCPD, 2013), 'Excessive collection of personal data and ineffective communication in retailers' customer loyalty programmes', p. 78.

([166]) PDPO (HK), s. 52.

([167]) PDPO (HK), s. 65(2).

([168]) See Chan and Lim, *Law of the Hong Kong Constitution*, pp. 88–9, citing *R v Lau Tung Sing* [1989] 1 HLKR 490, 500; *Somchai Liangsiriprasert v Government of the USA*

[1990] HKLR 85, 105.

([169]) See *Akai v The People's Insurance Co* (1996) 188 CLR 418, pp. 442–3.

([170]) *Shi Tao v Privacy Commissioner for Personal Data* [2008] 1 HKC 287.

([171]) PDPO (HK), s. 33.

([172]) PDPO (HK), s. 1(2).

([173]) PDPO (HK), s. 33(3).

([174]) See answer 4 in HKPCO Fact Sheet 1.

([175]) Following a Law Reform Commission report, a consultation paper with a working draft of the Contracts (Rights of Third Parties) Bill was issued on 31 Oct 2012.

([176]) Such processing is extensive but the extent unknown. In 2004 the Commissioner announced a project to measure offshore processing, but no further results emerged.

([177]) PCPD, 'The Year 2013 saw a 48% increase in Privacy Complaints' (PCPD, Press Release, 23 January 2014) <https://www.pcpd.org.hk/english/infocentre/press_20140123a.htm>.

([178]) PCPD, 'The Year 2013 saw a 48% increase in Privacy Complaints'.

([179]) PDPO (HK), s. 25.

([180]) For a full account, see PCPD, *Principles*, pp. 77–96 concerning access rights, and pp. 97–105 concerning correction rights.

([181]) PDPO (HK), s. 18(1).

([182]) PCPD, 'Supply of Consolidated Document List' [2001] HKPCPD 8; confirmed in AAB No. 24/2001.

([183]) PCPD *Principles*, p. 79.

([184]) PCPD has, however, issued and gazetted a data access request form.

([185]) For details of methods of response to requests, see PCPD *Principles*, p. 83.

([186]) □□□□□□□□□□□□, [2007] HKCA 635; □□□□□□□□□□□□, [2006] HKCA 659; see PCPD *Principles*, p. 85.

([187]) See PCPD *Principles*, p. 95 and *Wu Kit Ping v AAB* [2007] HKCFI 1104; [2007] 5 HKC 450.

([188]) PDPO (HK), s. 22(1).

([189]) PDPO (HK), s. 23(1) and s. 25(1)(a).

([190]) PDPO (HK), s. 27.

([191]) PDPO (HK), s. 25(2) and (3).

([192]) PCPD, 'Data correction request cannot be made verbally', [2008] HKPCPD 11.

([193]) PDPO (HK), s. 23.

([194]) PDPO (HK), s. 28.

([195]) See PCPD *Principles*, pp. 87–8 for detailed considerations.

([196]) PCPD, 'Bank Imposing Fee at a Flat Rate for Complying with a Data Access Request' (PCPD s. 48(2) Report R10-5528, 24 February 2010).

([197]) PCPD, *Guidance Note on Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users* (PCPD, June 2012). See also Commissioner of Correctional Services and PCPD [2009] HKPCPDAAB 37.

([198]) Based on a comparison of PCPD *Annual Report 2004–05* (PCPD, 2005) and PCPD *Annual Report 2012–13* (PCPD, 2013).

([199]) PDPO (HK), ss. 38 to 50.

([200]) PDPO (HK), s. 38.

([201]) PDPO (HK), s. 37(2).

([202]) PDPO (HK), s. 42(1).

([203]) PDPO (HK), s. 44.

([204]) PDPO (HK), s. 50.

([205]) PDPO (HK), ss. 46(2)(a) and (7).

([206]) PCPD *Annual Report 2011–12*.

([207]) PDPO (HK), s. 50.

([208]) PDPO (HK), s. 50(1)(b)(iii).

([209]) PDPO (HK), ss. 62(10), 64(7).

([210]) PDPO (HK), s. 50.

([211]) PDPO (HK), s. 50(1)(b).

([212]) Graham Greenleaf, 'Octopus Scandal Exposes Hong Kong Privacy Deficiencies' (2010) 108 *Privacy Laws & Business International Newsletter*.

([213]) In the *Face Magazine* decision, the AAB decided that the Commissioner was justified in concluding that the appellants' conduct was likely to be continued or be repeated (despite their removal of the photos in question from their websites) because of their stance that they had done nothing wrong; their lack of effort to provide guidance on the Ordinance's requirements to their staff; and their financial incentive to contravene again.

([214]) Cheung, 'An Evaluation of Personal Data Protection in Hong Kong Special Administrative Region (1995–2012)', pp. 29–41.

([215]) The second case was not a conviction but a ONE (Offer No Evidence) Bind Over.

([216]) PDPO (HK), s. 64(10) (pre-amended Ordinance).

([217]) PDPO (HK), s. 50A(1).

([218]) PDPO (HK), s. 50A(2).

([219]) PDPO (HK), s. 50A(3).

([220]) 2009 Consultation Document Proposal No. 10: Monetary Penalty for Serious Contravention.

([221]) PDPO (HK), s. 64(1).

([222]) PDPO (HK), s. 64(2).

([223]) PDPO (HK), s. (4).

([224]) Administrative Appeals Board Ordinance; Chief Secretary for Administration's Office 'Administrative Appeals Board—General Information' (AAB, 16 December 2013) <http://www.admwing.gov.hk/eng/links/aab.htm>.

([225]) PDPO (HK), s. 47(4).

([226]) PDPO (HK), s. 50(7).

([227]) PDPO (HK), s. 39(4).

([228]) PDPO (HK), s. 48(4).

([229]) PCPD, 'Privacy Commissioner Publishes Five Investigation Reports' (PCPD, 20 June 2011), <http://www.pcpd.org.hk/english/infocentre/press_20110620.html>.

([230]) Namely: '(i) it is against Hong Kong's public interests such as security, defence or

international relations; (ii) it will prejudice the investigation or detection of crime; or (iii) there are other legislative requirements prohibiting publication and identification of the relevant data users in particular cases.'

([231]) PCPD, 'Investigation Report / Inspection Report' (PCPD, to December 2013) <http://www.pcpd.org.hk/english/publications/invest_report.html>. These reports are not yet available on HKLII.

([232]) PDPO (HK), s. 66(3).

([233]) Although s. 66 is inhospitable to privacy claims by anyone other than the very wealthy, the paucity of cases is somewhat puzzling. Hong Kong is a relatively litigious society by Asian standards and there are frequent defamation actions to uphold one's reputation if a 'false accusation' has been made. It may be that the connection has not been made in the minds of litigants and their lawyers that privacy laws can also be used to vindicate reputation.

([234]) The PCPD advises that there was one newspaper report around 2012 that a claimant was awarded HK$5,000 for breach of the Ordinance, but there was no written decision.

([235]) PDPO (HK), s. 65(5).

([236]) This is also the case in the equal opportunities legislation, although some in-roads have made into this 'default' position in cases on that Ordinance.

([237]) PDPO (HK), s. 66A.

([238]) PDPO (HK), s. 66B.

([239]) PCPD, *Legal Assistance for Civil Claims under the Personal Data (Privacy) Ordinance* (leaflet) <http://www.pcpd.org.hk/english/publications/files/legal_assistance_e.pdf>. See PDPO (HK), s. 66B.

([240]) PDPO (HK), s. 66B(3).

([241]) PDPO (HK), s. 66B(5).

([242]) PCPD, 'The Year 2013 saw a 48% increase in Privacy Complaints', para. 21.

([243]) These 'mediated' matters are resolved after preliminary enquiries with the data user but without necessarily proceeding to formal investigations, because the problems raised by the complainant have been remedied by the data user.

([244]) Which were 'Advice/recommendations made' (141), 'Undertakings/warning notifications' (21) and 'Enforcement notices issued' (3): PCPD *Annual Report 2011–12*, p. 74.

([245]) It is possible that these remedial actions could sometimes include outcomes such as an apology, voluntary compensation, correction of a record, or change of respondent's practices, only some of which would be matters within the PCPD's formal jurisdiction, but all of which might occur nevertheless, and would be important outcomes resulting from the Ordinance's complaint procedures.

([246]) For example, of the 1,502 complaints completed in 2011–12, 169 (11%) were resolved through mediation. We do know that of the 87 (6%) of such complaints resolved after formal investigation, 24 (2%) involved breaches of the Ordinance. Other than the 12 which resulted in s. 48(2) reports (and thus the naming of the respondent), no details of outcomes are given of the 12 other contravention cases. The Report includes case notes on five of the 169 mediated cases (entitled 'Improvements in data handling'). Otherwise, the Annual Report 2011–12 provides no statistics of the outcomes of these 169 mediations, in terms of remedies resulting.

([247]) The Commissioner's office states that over 90% of the cases resulted in change of respondent's policies and practices, whereas in the others the remedies were specific to the complaints.

([248]) This refers to Annual Reports from 2013–14, as remedial outcome are not included in the 2012–13 Report.

([249]) Reporting of remedial outcomes is desirable both as statistics extracted from all mediated cases, and by case notes of selected complaint investigations that are particularly illustrative of problems resolved.

([250]) PCPD, 'Complaint/Enquiry Case Notes' (PCPD, undated) <https://www.pcpd.org.hk/english/casenotes/case_complaint.php>.

([251]) Hong Kong Legal Information Institute (HKLII) database, 'Office of the Privacy Commissioner for Personal Data Complaint Case Notes' (1997–2009) <http://www.hklii.hk/eng/hk/other/pcpd/complaint/2009/9.html>.

([252]) PCPD, 'Complaint/Enquiry Case notes' <http://www.pcpd.org.hk/english/casenotes/case_complaint.php>.

([253]) 293 on the Commissioner's website, 278 on the HKLII website published slightly in arrears.

([254]) According to the Commissioner, there is no change in policy, only a change of work priorities since 2010 (including the increased focus on section 48(2) reports), but normal case note reporting practices were to resume: Email from the Privacy Commissioner to the author, July 2013.

([255]) PCPD, *Privacy Impact Assessment (PIA)* (PCPD, Information Leaflet, July 2010) <http://www.pcpd.org.hk/english/publications/files/PIAleaflet_e.pdf>.

([256]) Former Commissioner Woo announced in 2005 that encouraging data users to voluntarily undertake PIAs of proposed systems would be a priority of his office, but this did not occur.

([257]) Greenleaf, 'Hong Kong's "Smart" ID Card' in Bennett and Lyon (Eds.), *Playing the Identity Card*, pp. 78–80.

([258]) PDPO (HK), s. 14.

([259]) PDPO (HK), Sched. 3, ss. 14 and 67(1).

([260]) PDPO (HK), s. 15.

([261]) PDPO (HK), s. 14A.

([262]) PCPD, *Annual Report 2012–13* (PCPD, 2013), p. 84.

([263]) PCPD, *Annual Report 2012–13* (PCPD, 2013), p. 85.

([264]) PCPD, 'The Year 2013 saw a 48% increase in Privacy Complaints', para. 26.

([265]) PDPO (HK), s. 36.

([266]) PDPO (HK), s. 48(1).

([267]) PCPD *Annual Report 1998–99* (PCPD, 1999), p. 38.

([268]) On the personal data systems of the Hospital Authority, Transunion Ltd, a trial of a school drug system, and the MTC's CCTV system: see 'Inspection Report' (CPDP, December 2013) <http://www.pcpd.org.hk/english/publications/invest_report.html>.

([269]) PCPD, 'Report on the Inspection of the Personal Data System of the MTR's CCTV System' (PCPD, s. 48(2) Report R13-2768, 9 April 2013).

([270]) PCPD, *Annual Report 1998–99*, pp. 36–7.

([271]) PCPD, *Annual Report 2012–13* (PCPD, 2013), pp. 74–5.

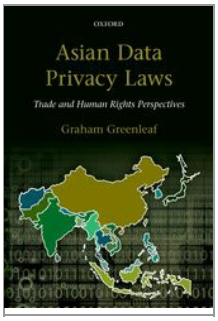
([272]) PDPO (HK), pt. III and s. 12.

([273]) PDPO (HK), s. 13.

([274]) PCPD, *Code of Practice on the Identity Card Number and other Personal Identifiers*, 1997.

([275]) McLeish and Greenleaf, 'Hong Kong' in Rule and Greenleaf (Eds.), *Global Privacy Protection*, pp. 236–8 and 247–8.

University Press Scholarship Online
Oxford Scholarship Online



Asian Data Privacy Laws: Trade & Human Rights Perspectives
Graham Greenleaf

Print publication date: 2014
Print ISBN-13: 9780199679669
Published to Oxford Scholarship Online: December 2014
DOI: 10.1093/acprof:oso/9780199679669.001.0001

South Korea—The Most Innovative Law

Graham Greenleaf

DOI:10.1093/acprof:oso/9780199679669.003.0005

[–] Abstract and Keywords

South Korea's new Personal Information Protection Act (PIPA) of 2011 has comprehensive private and public sector scope, and includes strong and innovative privacy principles, and much stronger enforcement measures. This chapter first sets out South Korea's successful transitions from dictatorship to democracy, and the strong context of constitutional protection for privacy resulting. PIPA is analysed in detail, particularly the many unusual and innovative principles and requirements it contains. The enforcement of South Korea's privacy laws have involved, for over a decade, an innovative means of resolving privacy disputes by a mediation body, the payment of modest amounts of compensation, and a high degree of transparency. South Korea is moving away from the 'ministry enforcement' model, because PIPA now includes a data protection authority, the Personal Information Protection Commission (PIPC). The PIPC's role is as yet less clear and its enforcement activities yet to be demonstrated. North Korea's surveillance state is also briefly considered.

Keywords: data protection, privacy, Asia, South Korea, data protection authority

(p.124)

1. Introduction

South Korea (the Republic of Korea, hereinafter 'South Korea') has made one of the world's most successful transitions from dictatorship to democracy. Since the gradual overturn of authoritarian military rule, accelerating from 1980, South Korea has in the last 30 years established a very energetic multiparty democracy. It is now a country in which the rule of law is well established. South Korea's achievements in the protection of privacy are therefore relatively recent, but more notable for that, because (as in Eastern Europe at the same time) they represent a significant element of the post-authoritarian construction of a liberal-democratic state.

South Korea's Personal Information Protection Act (PIPA) of 2011 is the first such act with comprehensive scope, includes strong and innovative privacy principles, and much stronger enforcement measures. It includes an independent 15-member Personal Information Protection Commission, which is a departure from the primarily ministry-based enforcement of the previous Korean law, and of its civil law neighbours Japan and Taiwan. Commentators have described this Act as the 'strictest in the world',[1] but whether its formal strength on paper will be translated into reality through enforcement requires further time to assess.

An important contextual factor in Korean data privacy law is the country's high Internet saturation. From a population of just on 50 million, South Korea has over 40 million (80 per cent usage) Internet users, with 81 per cent of households having personal computers, almost all of which have broadband connections. South Korea has the second-highest high-speed fibre broadband connectivity of OECD countries. Use of mobile broadband in mobile telephones is close to universal.[2] This Internet saturation has led to early adoption of some forms of Internet services and regulation in South Korea, some of which have privacy implications and make South Korea an important jurisdiction to watch for new privacy dangers and responses.

The position in North Korea (the Democratic People's Republic of Korea or 'DPRK'), a state whose survival is based upon continuing state surveillance of its population, and where no aspect of privacy is respected, is discussed briefly in section 9 of this chapter.

1.1. History and politics of Korea

Modern Korea bears the scars of its past more than most countries.[3] Korean kingdoms and dynasties played major roles in East Asia from more than 2,000 years ago, and maintained their political and territorial integrity against their gigantic Chinese neighbour for almost all of that time,[4] as well as surviving repeated destructive attempts at subjugation by Japan. However, the long-lived Joseon Dynasty (1392–1910) entered the twentieth century in an economically and militarily weak position compared with Japan. A series of treaties gradually put Japan into a position to fully annex Korea in 1910. Thirty-five years of brutal **(p.125)** colonial occupation and attempted destruction of Korean culture followed, coupled with the development of some 'colonial modernity'.[5] The end of World War II and Japanese colonialism unfortunately did not leave a unified country, due to the hostility of the occupying USA and USSR governments, and the deep divisions that had emerged between Korea's contending political elites. The Korean War, including Chinese military intervention, then froze the division of the peninsula at the 38th parallel Demilitarized Zone (DMZ), where it remains, separating North Korea and South Korea.

The half-century history of South Korea (the Republic of Korea) since these two wars has combined almost constant economic growth and improvement (interrupted by the 'IMF financial crisis' of the late 1990s) and a gradual development of democratic institutions. The current vitality and stability of Korea's democracy makes it easy to overlook how recent it is, and how hard-won it was. By the end of the nearly 20-year dictatorship of President Park Chung Hee with his assassination in 1979, there may well have already been a broad-based desire in South Korea 'to create an open democracy and to curb the excessive powers of the executive'.[6] Another dictatorship under General Chun Doo Hwan coupled with a massacre of civilians in the city of Kwangju delayed those aspirations for the best part of another decade. Although that dictatorship finally ended after massive protests in 1987, Chun's anointed successor Roh Tae Woo was elected President after the opposition split. Former opposition politician Kim Young Sam became President in 1992 after forming a coalition with the ruling party, and liberalization of Korean politics commenced with amnesties for former dissidents, restructuring of the Korean Central Intelligence Agency (KCIA) to reduce domestic surveillance, and a 'real name' law which made it illegal to hold bank accounts or property in a fictitious name, a strong blow against corruption. National reconciliation was advanced through the convictions of former Presidents Chun and Roh for bribery, then sedition and mutiny. However, it was not until the election of Kim Dae Jung as President in 1997 that there was 'the first peaceful transition of power between government and opposition parties'.[7] The

development of data privacy laws in South Korea therefore takes place in the context of a post-authoritarian phase in the democratizing and restructuring of South Korean society and law that is less than 20 years old.

1.2. Legal system of South Korea

Korean legal institutions have a long history,[8] most significantly from the Joseon Dynasty, the Codes of which included elements of the rule of law. From the mid-19th century, some Western legal concepts became influential. Following full annexation by Japan in 1910 this process was accelerated as Japanese legal Codes replaced those of the Joseon era and became the primary source of law in Korea. Because the Japanese legal system had by then been very substantially influenced by Germany (with some Anglo-American and French influences), 'Korea indirectly accepted Western legal tradition'.[9] The post-war **(p.126)** period of recovery from colonialism and the Korean War meant that Japanese influences in the legal system continued for many years. However, there were also direct Western influences such as US and European influences on the Constitutions of 1948 and subsequently, particularly in relation to separation of powers. Strong civil law (particularly German) influences remain in the post-war Codes enacted by South Korea; however, American influence has been strong in some areas of law. As a primarily civil law system, statutes are the dominant source of law, supplemented by Presidential or Ministerial decrees, within the limits set by the statute. The Constitutional Court, established as recently as 1988 as a result of the 9th amendment to the Constitution, is independent of the Supreme Court and has as one of its functions to decide the constitutionality of legislation,[10] and so far has found the laws considered in 303 of 774 cases heard to be either wholly or partly unconstitutional.[11]

The Supreme Court is the apex of a court hierarchy with five High (appellate) Courts, 18 District Courts, and various specialized courts. Although court decisions are not formally regarded as sources of law, 'Supreme Court decisions function as a de facto source of law'.[12] The courts also perform an important 'gap filling' function, interpreting broadly worded statutes to make them more precise, with the interpretations of higher courts in effect binding lower courts. The divide between civil law and common law approaches is diminishing with the growth in importance of court decisions.

1.3. State surveillance in South Korea

Until the 1990s South Korea's military-dominated regimes had a very strong state surveillance apparatus, particularly the feared KCIA. It was not until the presidency of Kim Young Sam from 1992 that the KCIA was restructured in order to reduce its surveillance activities.[13] In 2005 the former heads of the National Intelligence Service (NIS, a successor to the KCIA) were arrested and sentenced for illegal wiretapping in 1998–2003.[14] A major factor in surveillance in South Korea, in both public and private sectors, has been the pervasive use of the resident registration (RR) number.[15] A succession of laws has progressively 'rolled back' the use of the RR number (with new restrictions proposed), in what is one of the world's more noteable curtailments of an existing surveillance mechanism, though many allowed uses remain (see section 4.5 of this chapter).

A study of systemic government access to private sector personal data in South Korea[16] has highlighted that the legislation concerning search warrants may not apply to stored electronic data, but this remains untested. In relation to access without a warrant, the Seoul High Court held that Internet Service Providers (ISPs) had no obligation to disclose personal data merely because of requests by police authorities, and to do so breached **(p.127)** their customers' constitutional privacy rights of self-determination and anonymous speech (see section 2.1 of this chapter), and accordingly ordered payment of compensation.[17] Jong concludes that ISPs will be extremely reluctant to disclose any personal information in the absence of a warrant.[18] Although there are many statutes authorizing disclosure without warrant in particular circumstances, in light of this decision any private sector body will have to be very clearly satisfied that they apply, and the courts may also be called on to examine the legality of any such disclosure after it has occurred.[19]

2. Constitutional and general law protections of privacy in South Korea

Specialized data privacy legislation is not the only legal means of protecting privacy in South Korea, but it has become the most important.

2.1. Constitutional and treaty protections

The Korean Constitution provides for the general protection of privacy,[20] and specifically for the protection of privacy of the home[21] and in communications.[22] The Constitution also affirms that freedoms and rights of citizens must not be neglected on the grounds that they are not enumerated in the Constitution.[23] These protections can be restricted by law only when necessary for national security, law and order, or public welfare—but even then, essential aspects of these rights must not be violated.[24] Therefore, any legal measures imposed to attain public interests should be the less restrictive alternative with regard to freedom of speech.[25] There is no exception for the need to enhance administrative efficiency.

In 2003, the Constitutional Court interpreted these provisions to protect people from inappropriate access to, and abuse or misuse of, their personal information, in the *Seatbelt Case*:[26]

> The right to privacy is a fundamental right which prevents the state from looking into the private life of citizens, and provides for the protection from the state's intervention or prohibition of free conduct of private living. Concretely, the privacy protection is defined as protecting and maintaining the confidential secrecy of an individual; ensuring the inviolability of one's own private life; keeping from other's intervention of such sensitive areas as one's conscience or sexual life; holding in esteem one's own personality and emotional life; and preserving one's mental inner world.

In 2005 the Court made a further ruling, using terminology close to the idea of 'informational self-determination' developed by the German Constitutional Court, when it said in the *Fingerprint Case*:[27]

> **(p.128)** The right to control one's own personal information is a right of the subject of the information to personally decide when, to whom or by whom, and to what extent his or her information will be disclosed or used. It is a basic right, although not specified in the Constitution, existing to protect the personal freedom of decision from the risk caused by the enlargement of state functions and info-communication technology.

In that case, a majority of the Court found that the governmental power to collect (as part of the issuing of a resident registration card) and keep prints of all 10 fingers of all citizens 17 years of age or above, and to use them for investigation purposes, does not excessively violate the right to control personal information. A very strong opinion by the dissenting minority focused on the use of fingerprints of persons who had never been convicted, with no restrictions on the investigative uses that could be made, and considered that this was not consistent with the concept of minimum justifiable restrictions.

In the *Real Name Cases* in 2012 the Court held that South Korea's online 'real name' statute (also called 'limited identity verification system' statute) was[28] unconstitutional because the public gains achieved had not been substantial enough to justify restrictions on individuals' rights to free speech and privacy.[29] Two cases were brought by individuals required to provide their real names in order to make online postings. They were joined by an online Internet publisher required by the law to verify the names of those posting. The Court considered that the purpose of the legislation was legitimate insofar as it aimed to contribute to a sound Internet culture by preventing users from posting illegal or defamatory messages on Internet bulletin boards, and collecting data to identify who did so. However, the system requiring the operator of the Internet bulletin board to verify the real name of its users and block their posting if their names failed to be verified was over-restrictive, beyond the extent necessary to attain that purpose. The Court concluded that the statute at issue was in violation of the principle of less restrictive alternatives, in violation of freedom of speech of both users and information and communications service providers, and also in violation of the self-determination of personal information of the users.[30]

In numerous other cases the Constitutional Court has ruled on specific issues involving personal information, in areas such as disclosure of diseases by public servants,[31] numbers of cases handled by lawyers,[32] and designation of no-smoking zones.[33] The complex balance between constitutional privacy protections and freedom of speech is explored in the *Information Publication Prohibition Case*.[34] The constitutional protection of privacy is therefore a very important part of South Korea's overall protection of privacy.

(p.129) 2.2. South Korea's Human Rights Commission

South Korea's National Human Rights Commission (NHRC) is able to investigate complaints of interference with a person's constitutional privacy rights. Although it can only make recommendations, occasionally its interventions are very significant.[35] One of the most significant privacy struggles between the government and the public concerned the National Education Information System (NEIS) scheme proposed in 2003. NEIS sought to centralize personal data of about 8 million students from 12,000 primary and secondary schools across the country in a national computerized network, including students' academic records, medical history, counselling notes, and family background, and even including data on teachers' trade union activities. The National Teachers' Union (NTU) and other civic organizations conducted protest rallies and threatened a general strike. They brought an action before the NHRC, which recommended that three of 27 categories of personal data be excluded from the NEIS databases, and the Education Ministry complied. Although there were numerous further stages in this dispute,[36] resulting in the modified NEIS databases being determined by the Constitutional Court to comply with the Constitution and the relevant laws on data protection, the NHRC's early intervention helped ensure that NEIS was modified to be less privacy-intrusive.[37]

Privacy-related issues are not a major part of the work of the NHRC, but it has made other notable interventions. For example, in 2009 the NHRC made a suggestion in terms of privacy protection that CCTV for anti-crime purposes should not be installed at public rest rooms, sauna and bath rooms, etc., that only CCTVs without in-built audio function should be allowed, and that CCTV monitoring should not be entrusted to private companies. The NHRC recommended that the Minister of Labor should improve relevant laws and regulations so as to protect the human rights of employees from improper electronic monitoring at workplaces.[38]

2.3. Civil law protections

The 'horizontal' application of the constitutional protection of privacy in Korea to relationships between private parties, and its implementation via the Civil Act, was set out in 2011 in the *Information Publication Prohibition Case*:[39]

> The fundamental constitutional right, in basic, is a defensive right to protect an individual's free scope from the infringement of public power, but on the other hand, it specifies the constitutional order of values in all legal areas including private law. Thus, legal relation among private persons should also be regulated according to constitutional provisions providing fundamental rights. However, except those directly applicable to private law relations, fundamental right provisions are generally incorporated into Articles 2, 103, 750, and 751, etc. of the Civil Act as a general principle of private laws and as an interpretational criteria indirectly affecting private law relations (*see* Supreme Court en banc Decision 2008Da38288, April 22, 2010). As seen in the above, the general personality right or the constitutional provision of the rights of privacy and freedom will be specified in the general provisions of the Civil Acts in the form of guaranteeing **(p.130)** legal interest in personalities to private persons. Thus, if disclosure of personal information without consent can be viewed as infringing the legal interest of the person whose information is disclosed in personality, its unlawfulness should be acknowledged.

The interpretation of the Civil Act provisions are therefore guided by the constitutional rights concerning privacy. The Civil Act provides possible actions for torts to protect privacy, authorizing damages awards for negligent or intentional causation of damages to another, principally under article 750,[40] and article

751 concerning mental distress.[41] The Supreme Court has made few decisions on Civil Code issues concerning privacy. A case in 2013 demonstrated that tortious damages can be available where media intrusions, including in public places, result in publication of private facts.[42] In this case the defendant corporation was held to have infringed A and B's privacy by vividly describing the meeting between the families of the soon-to-be-married A and B as well as scenes of the two dating, and published a report with A's photograph taken without permission. The court held that that the company infringed A and B's privacy and portrait rights, and was obliged to pay damages for the emotional distress caused.

A significant issue in Korea is the circumstances under which mental distress arising from data leaks can be compensated even though no pecuniary damage can be shown. The leading Supreme Court decision is known as the *GS Caltex Data Breach Case*.[43] The Court stated the relevant principles in such cases as:

> In a case where personal information collected by a person who handles the information was leaked out by the person's employee against the intentions of the subject of the personal data (hereinafter 'data subject'); when determining whether the leak caused the data subject to suffer emotional distress which qualifies as compensable damages, the determination should be made after considering the following circumstances, and judged accordingly and specifically to each individual case. Firstly, the type and characteristic of the leaked personal information; whether the data subject is identifiable through the leaked information; whether a third party accessed the leaked information, and if it did not occur, whether there is probability that a third party had such access or will have access in the future; to what extent the leaked information was spread; whether the leak possibly caused any additional infringement of rights; the actual reality of how the personal information was managed by the person who handled the information, and the specific circumstances in which the information was leaked; and what measures were taken to prevent injury caused by the leak, and to prevent the spread of leaked information.

Here, defendant GS Caltex Co had built a database based on the personal information of members of its gas credit card service. It commissioned GS Nextation Co, which managed its customer service centre, to manage the database. An employee of GS Nextation used his account to download without authority the personal details of nearly 12 million members, then conspired with others to sell the information to a law firm preparing a class action. **(p.131)** To avoid suspicion falling on the law firm, they had pretended to find the data on CD and DVDs in a garbage collection, and provided copies to media organizations. The police were able to arrest the conspirators immediately, and believed that they had retrieved all copies of the data from the conspirators and the media organizations. The lower court found, and the Supreme Court considered, that there was no basis for overturning this finding of fact, that '[t]here is no evidence that the personal information of this case was leaked through any other channels'. The Supreme Court found that, given that there was no evidence that either the conspirators or the media organizations looked at, or were interested in, the individual personal details among the 12 million files:

> [t]here were no circumstances to perceive that additional injury caused by the information leak was inflicted upon the plaintiffs, such as identity confirmation or illegal use of another person's name. Upon examining these surrounding circumstances in light of the aforementioned legal principles, it is difficult to perceive that the plaintiffs suffered emotional distress which qualifies as compensable damages. Thus, the court below's determination that it is difficult to perceive that the plaintiffs suffered emotional distress is just; and contrary to the alleged ground of appeal, there were no errors in the misapprehension of related legal principle.

It seems, therefore, that emotional distress cannot be assumed merely due to the existence of a large data spill. Either actual damage, or emotional distress, will have to be proven to exist, and to have been caused by the data spill.

From analysis of a history of large-scale data breach incidents and resulting litigation in South Korea,[44] Whon-il Park distinguishes between data breach cases, where employees negligently leak or intentionally

steal personal information, and those where it is leaked by outsiders. In either of these situations, where there are inadequate technical safeguards and lack of caution when dealing with customers' data, both the likelihood of liability and the probable level of damages are increased. In the *Kookmin Bank Case* in 2006, the bank accidentally sent a promotional email to its customers which contained details of other customers. Over 1,000 customers sued, and were awarded 3 billion won (US$3 million) damages at first instance. The *GS Caltex Case* is another important example of a case falling into the first category.

In the *SK Communications Case #1* (2011),[45] unidentified hackers stole personal data relating to two very popular social networks (Nate and Cyworld). Nearly 3,000 plaintiffs sued, but failed because Seoul Central District Court found that the defendants had employed appropriate technical and managerial safety measures, and its software was not responsible for the attack, which seemed to have used methods undetectable at the time. However, on the same facts in *SK Communications Case #2* (2013), Seoul Western District Court ordered SK Communications to pay a total of 576.4 million won (US$534,200), or 200,000 won each (US$200), to 2,882 petitioners. The court held that the defendant company 'neglected its duty to protect customers' information, which resulted in inviting a hacking incident'. This is said to be 'the first ruling that holds the corporate manager accountable for leaking customers' information regardless of intentionality'.[46]

(p.132) In another example falling in the second category, the *Auction case* (2008),[47] an overseas hacker took personal details relating to 18 million customers of Auction, of whom 145,000 (organized in ten groups) commenced 'collective' individual actions.[48] In 2010 the Seoul Central District Court held in favour of Auction (upheld on appeal by the Seoul High Court in 2013), finding that its security was not at fault (it said it was not mandatory to install firewalls at that time, because they had low credibility), and apparently taking into account the swift response by Auction management. A successful example of where inadequate technical safeguards were involved is the *Lineage Case* where a court held that game site operators obtaining commercial profits from users have a duty of special care to protect the personal information (personal ID and password) of customers by encryption, resulting in payment of 500 thousand won (around US$500) to each plaintiff.[49] The considerable divergence in the decisions of Korean courts will need to be resolved by higher levels of decisions. It is expected that a number of collective individual actions will be filed with the courts in the aftermath of the unprecedented card data leakage of three credit card companies in 2014[50] (see section 8.2 of this chapter).

2.4. Criminal law protections

In addition to the complex offences in PIPA, some of which can apply to third parties as well as data controllers (see section 5.6 of this chapter), there are numerous offences under the Criminal Act which can apply to misuse of personal information,[51] or various other Acts.

3. Data privacy legislation and enforcement authorities in South Korea

South Korea has a long history of data privacy protection legislation, which has been established and extended sector by sub-sector since the mid-1990s. The result was different privacy principles in the key laws in the public and private sectors, different enforcement bodies and approaches in each sector, and incomplete and inconsistent private sector coverage. The previous legislation had considerable strengths, but until its 2011 law, South Korea had neither unified data protection principles for both public and private sectors, nor an independent data protection authority covering both, or even the whole of the private sector. The new legislation is, however, one of the most comprehensive in Asia.

(p.133) ### 3.1. Previous legislation

South Korea became an OECD member in 1996. Like some other OECD members such as Australia, Canada, and Japan, it initially only legislated in relation to the public sector, in 1995. Private sector legislation was subsequently implemented incrementally from 2001.

Public sector legislation 1995 onwards

The Public Agency Data Protection Act of 1995 previously governed the government's collection of

personal information, based on the OECD Guidelines on privacy protection. This Act applied to all public institutions, government departments and offices in the administration, the legislature and the judiciary as well as local governments, various schools, government-owned companies, and public sector institutions. Under this Act, government agencies were required to limit data collection, ensure the accuracy of data, keep public registers of data files, ensure the security of the information, and limit use of personal data to the purposes for which they are collected. The Act included most basic OECD principles, but with few limits on excessive data collection by governments. Only computerized data fell within the scope of this Act, but manually collected information could sometimes be protected by confidentiality requirements in administrative work found in the Criminal Code and other laws.[52] The Act was enforced by the ministry responsible for government administration and police affairs, now the Ministry of Security and Public Administration (MOSPA).[53] There was no guarantee of the independence of the oversight body established in the ministry nor of the Personal Information Protection Deliberation Committee established under the Prime Minister's Department. There was no publication of case details, and there seems to have been minimal enforcement.

Private sector legislation 2001–2011

The key private sector legislation was the 2001 Act on Promotion of Information and Communications Network Utilization and Information Protection, etc (ICN Act), which was frequently amended. Chapter 4 of the Act, 'Protection of Personal Information' was generally known as the Data Protection Act and will be referred to in this chapter as 'the previous Act'. Its scope was limited to businesses utilizing telecommunications services, although it was actively enforced by the Korea Internet & Security Agency (KISA) and a mediation body (PIDMC), which published case details, although the overall administration of the ICN Act was and is by the Korea Communications Commission (KCC). It was extended to apply to most businesses in relation to personal information on users of their services and their customers, and it was strengthened very considerably in 2007, particularly in relation to consent. Its stronger features, including the PIDMC, are continued in the new legislation.

3.2. Personal Information Protection Act 2011—a near-comprehensive Act

South Korea's new Personal Information Protection Act (PIPA)[54] was promulgated on 29 March 2011, and came into force six months later, although there was a further six-month **(p.134)** grace period, until 31 March 2012, during which the Act was not strictly enforced. The new Act replaced the previous Public Agency Data Protection Act in whole, and in relation to the private sector it replaced in part the ICN Act, but only in relation to those non-ICSPs to whom the previous Act had been extended.

The ICN Act continues to impose additional privacy and other obligations on information and communications service providers (ICSPs), and the Korea Communications Commission (KCC) therefore continues to play a significant role in privacy protection because ICSPs have such a significant social role in relation to personal information, and also because they have been responsible for major data breaches in Korea. There is thus a considerable potential overlap of responsibilities between the KCC and the new PIPC in relation to ICSPs such as Google. In 2014 the KCC was continuing to investigate Google's Street View and reported to be considering fines.[55] The KCC is a general media regulatory agency which is modelled in part on the USA's Federal Communications Commission (FCC), but without the same degree of independence. Korea also has a number of Acts with specific requirements, which will still take precedence over the new PIPA,[56] in relation to both the public sector[57] and private sector.[58] Other than the ICN Act, the Use and Protection of Credit Information Act is probably the most important. This chapter focuses on PIPA rather than the ICN, credit information, and other sectoral laws, despite their continuing significance. In relation to ICSPs, the ICN Act must always be considered.

PIPA is therefore a near-comprehensive Act for the first time in Korea, because it covers both public and private sectors, and the whole of the private sector (even though other Acts add stronger provisions). More than 3.5 million public entities and private businesses are now regulated by common criteria and principles, and common enforcement mechanisms. The new Act has added many new features to existing strong foundations (at least in relation to the private sector). Statutory references in this chapter are to

PIPA unless otherwise stated.

3.3. South Korea's data protection authorities

PIPA, with its expanded scope applying to both the public sector and the whole private sector, establishes a complex administrative and enforcement structure which involves at least six parties: (i) the Personal Information Protection Commission (PIPC); (ii) the Ministry of Security and Public Administration (MOSPA);[59] (iii) the Korea Communications Commission (KCC) (iv) the Personal Information Dispute Mediation Committees ('PIDMC' or 'Pico'); (v) the Korea Internet & Security Agency (KISA) and its KISA Privacy Center; and (vi) other ministries and agencies.

Korea has developed a unique system for data protection involving both a significant amount of ministerial enforcement, plus two independent data protection authorities (DPAs): one for individual complaint resolution (PIDMC), serviced by a government **(p.135)** agency (KISA/Privacy Center) and the other for 'policy matters' (PIPC), serviced by a secretariat within MOSPA. The real location of regulatory power within this complex structure will take some time to be established as a matter of practice. Self-regulation and co-regulation is not a major part of the system, but is covered in section 8 of this chapter.

The Personal Information Protection Commission (PIPC)

PIPA provides for establishment of a Personal Information Protection Commission (PIPC) under the Presidential Office 'to deliberate and resolve the matters regarding data protection', and that it 'shall independently conduct the functions belonging to its authority'.[60] It has a wide range of powers concerning determining policy matters, the giving of opinions, issuing reports, the 'coordination of positions taken by public institutions', and the interpretation of laws and regulations,[61] but not the resolution of individual complaints. The PIPC website is primarily in Korean but contains some information in English.[62]

The PIPC consists of not more than 15 Commissioners, including a Chairperson (appointed by the President from among the Commissioners who are not public officials[63]) and one full-time Standing Commissioner in charge of administrative affairs of the PIPC. While the President appoints the rest of the Commissioners, this is within constraints of the separation of powers and multiparty system. Appointments are for a fixed term of three years. The Commission commenced operation in January 2012. A secretariat is 'established within the Commission' (and would therefore in principle be independent of MOSPA)[64] to support its administration, and is headed by a Director.

The Ministry of Security and Public Administration (MOSPA)

MOSPA has many responsibilities under PIPA, and is central to the Act's operation.[65] The secretariat for the new PIPC is located physically within MOSPA, although part of the PIPC. MOSPA appoints members of the Dispute Mediation Committee.[66] It is influential in the development of the Enforcement Decree which provides operational detail for the enforcement of the Act. It is responsible for preparing a Data Protection Basic Plan every three years, but submits it to the PIPC and then carries it out 'subject to the deliberation and resolution' of the PIPC.[67] The Basic Plan is required to include such matters as goals, intended improvements and development of counter-measures, facilitating self-regulation, education and training. Departments and agencies are then required to carry this out, once again 'subject to the deliberation and resolution' of the PIPC. MOSPA is responsible for establishing 'Standard Guidelines' concerning data privacy, which departments and agencies can then modify for particular sectors.[68] It can also investigate the 'actual state of **(p.136)** regulatory compliance' in all sectors.[69] Other aspects of the Act's operation are left to MOSPA by various sections to 'work out'.

The Privacy Center within KISA

KISA[70] will continue to exercise various data privacy functions, as it did under the previous Act, and other privacy-related functions delegated by MOSPA and KCC.[71] KISA will issue necessary guidance and guidelines for the private sector. The KISA Privacy Center[72] receives and investigates complaints,

and mediates minor complaints, as the '118' centre required by the Act.[73] It helps complainants to prepare complaints to go to the PIDMC. In more serious cases of data breach, upon receiving notice of such incidents under article 40 of the Act and article 34(3) of the Enforcement Decree, it notifies MOSPA, the police, and the prosecutors' office of violations or incidents.

The Personal Information Dispute Mediation Committee (PIDMC)

The PIDMC is comprised of up to 20 members (increased from 15 under the previous Act), appointed by MOSPA from among qualified lawyers, academics, senior government officials, and representatives of consumer organizations and IT businesses, and with a non-government chair.[74] Members have a term of two years, can be re-appointed once, and cannot be removed from office except for loss of qualification, serious offence, or incapacity. Since 2001, PIDMC subcommittees have had the role of mediating in disputes between individual data subjects and processors, and under PIPA they will also be able to mediate collective complaints (as discussed below) and complaints against public sector bodies (not previously possible). KISA continues to provide Secretariat services to the PIDMC,[75] including receiving petitions for dispute mediation, conducting the factual investigations, and preparing the agendas for the PIDMC subcommittee meetings and keeping their minutes. The PIDMC website provides considerable information in Korean.[76]

The Korea Communications Commission (KCC) and other ministries and agencies

The KCC, which took over a part of the former Ministry of Information and Communication, is responsible for policy-making on broadcasting and communications, and enforcement of the ICN Act. The KCC still regulates ICSPs with respect to data protection as well as communication affairs subject to the ICN Act. Heads of central administrative departments or agencies can also establish guidelines in fields under their jurisdiction,[77] in addition to the 'Standard Guidelines' issued by MOSPA. It remains to be seen whether the **(p.137)** possibility of ministry-issued guidelines will lead to their fragmented development with little central coordination.

3.4. Sources and transparency

Each of the above authorities has a separate website detailing its privacy activities, noted where they are discussed. Most information is only available in Korean. The available of decisions by the various authorities is essential to an assessment of the effectiveness of the Korean law. The first decision as yet made by the PIPC (concerning Google's terms of service) is available in English, but there is another decision available only in Korean, so the PIPC's practice is as yet uncertain. The PIDMC publishes summaries of many of its mediation decisions, including in an annual book,[78] but only in Korean. Summaries of 61 PIDMC mediation decisions, prepared by the PIDMC from its Annual Reports 2002–07, are available online in English.[79] No official summaries in English are available of decisions since 2007, but Whon-il Park has selected from the official PIDMC summaries (in Korean) a set of noteworthy PIDMC mediations from 2007–11 and summarized a selection of them in English.[80] These mediations are prior to the coming into force of PIPA. These summaries are used to provide examples of the operation of PIPA (and its preceding legislation) in the sections that follow. Whon-il Park's 'KoreanLII' website[81] is a valuable English language resource on many aspects of South Korean data privacy law,[82] including his translations of the Act (and amendments) and the Enforcement Decree.

4. PIPA's innovative privacy principles

PIPA first makes a general statement of data protection principles,[83] and rights of the data subject[84] and then provides detailed obligations in relation to all principles.[85] Many articles have further operative details provided by the Enforcement Decree.[86] In addition, there are MOSPA 'Standard Guidelines',[87] and additional guidelines from other central administrative departments or agencies.

4.1. Scope of PIPA

PIPA covers both public and private sectors, and the whole of the private sector, with relatively few exemptions, and with a broad definition of 'personal information' and other key terms.

(p.138) Definitions

Key terms are defined in article 2 of PIPA. The Act applies to 'personal information', which is given a conventional definition,[88] essentially meaning any information capable of identifying a living person, including when 'combined with other information'. A natural person so identifiable is a 'data subject'. A 'personal information file' is a set of personal information systematically organized to enable easy access. As with all data protection laws influenced by the European Union (EU) Data Protection Directive, the term 'processing' refers generally to all types of actions that can be taken in relation to personal information.[89] A 'personal information processor' is any person or organization that processes (directly or indirectly) personal information 'to operate personal information files for official or business purposes'.

Exemptions

Various categories of personal information are exempt from the principles concerning processing and the enforcement measures in Chapters 3–7 of PIPA, namely, personal information collected under the Statistics Act, for national security analysis, to be processed temporarily in cases where it is 'urgently necessary for public safety and welfare, public health etc', or used for reporting by the press, or for missionary activities of religious organizations, or for nomination of candidates by political parties.[90] Where these exemptions apply, the processor must process the information as little as possible to achieve its purposes, and must make arrangements for security and for handling grievances.[91] However, the normal enforcement provisions will not apply to these obligations. The requirements of consent to collection, a privacy policy and a privacy officer are also waived for clubs and associations such as alumni associations or hobby clubs.[92] These exemptions are not extensive compared with other jurisdictions in the Asia-Pacific, so it is reasonable to describe the South Korean legislation as largely comprehensive.

4.2. Proving breaches—openness, accountability, and onus of proof

PIPA is unusual in how easy it is for individuals to prove breaches of the Act. This can be seen in three requirements, concerning privacy policies, the onus of proof, and privacy officers.

A *privacy policy* must be issued, covering required matters including the purpose of processing, retention period, and any policy concerning disclosure to third parties or consignment for processing.[93] In the event of any discrepancy between the policy and an agreement with a data subject, 'what is beneficial to the data subject prevail'.[94] Processors **(p.139)** therefore cannot obtain consents from individuals which are contrary to what their privacy policy promises.[95]

The *onus of proof* of many requirements under the Act is on the processor, not on the individual who is claiming a breach.[96] Although an individual would still have to prove a breach of the Act on the balance or probabilities, once this is done the processor must 'prove non-existence of its wrongful intent or negligence' to avoid payment of damages,[97] and where the damage results from 'loss, theft, leak, alteration or damage of personal information' damages can only be reduced on proof by the processor of 'compliance with this Act and non-negligence of due care and supervision'.[98]

A *privacy officer* must be appointed, with detailed duties to implement a data protection plan, survey and improve its actual operation, set up internal control systems, investigate complaints, and provide 'remedial compensation'.[99] The MOSPA Standard Guidelines suggest this officer must be appointed regardless of the size or nature of the entity, and whether a public or private sector body (except fraternal associations). This is similar to the EU's proposed version of an 'accountability principle', and makes it easier for individuals to show that a processor has failed in its duties to properly safeguard personal information.

4.3. Purpose specification and collection limitations for personal data

The South Korean legislation has provisions to minimize collection of personal data, and collection is also limited by the provisions requiring notice, on sensitive information and ID numbers, and on restrictions on visual surveillance.

Purpose specification, consent, and notice

The requirements of purpose specification, consent, and notice are first stated generally (articles 3 and 4), and then more specifically in Chapter 3 of PIPA. Data controllers ('personal information processors') must make their purposes of processing explicit and specific,[100] and data subjects have the right to be informed of those purposes and to consent to them.[101] Processing requires consent,[102] or it must come within a small number of common exceptions (legal requirements, contract, interests of the data subject), or an exception where the data controller's interests are clearly superior to those of the data subject.[103] The data subject must be informed of the purpose of collection and other matters when consent is obtained.[104] How consent is obtained, both at the point of collection, and later for changes of purpose or disclosures, is strictly regulated (see section 4.4 of this chapter). 'Processor', as used here, is roughly similar to 'controller' in the EU.

(p.140) Minimal collection

PIPA has a number of principles which put it in the 'most restrictive' category in relation to collection of personal information. At least four provisions contribute to this: minimum collection; anonymity; 'no denial of services'; and unfair collection.

Only the minimum collection of personal data necessary for the purpose of collection is allowed, and the processor has the burden of proof to show that it is the minimum.[105] The PIDMC reported an example where a company selling financial products of more than a specified value required more personal information than the 'authentication certificate' that it normally accepted, which was held not to be excessive collection because this justified a more strict policy.

Processors are also required to 'make efforts to process personal information in anonymity, if possible',[106] as a requirement additional to the principle of minimal collection. The only other data protection Acts to include a specific requirement that anonymity should be offered where possible are those of Germany and Australia.

A distinctive Korean principle is that there must be no denial of services because of a person's refusal to provide legally unnecessary information.[107] Organizations therefore cannot decline to provide services because a person refuses to provide more than the minimum data allowed to be collected. Such action would be a separate breach of the Act. This principle is reiterated in relation to data subjects who refuse to consent to matters where consent is optional under the Act,[108] discussed later in relation to consent. These protections for data subjects are more explicit than in legislation found in other countries. They are reinforced by 2013 amendments providing that the data subjects must be explicitly informed of their right to refuse to provide information more than the minimum necessary.[109]

PIPA imposes individual obligations on anyone processing personal information, prohibiting obtaining it, or consent relating to it, 'in a fraudulent, improper or unfair manner',[110] which includes what is often called 'unfair collection'.

Taken together, the South Korean requirements equate to the European standard (minimality), not the weaker OECD/APEC standards that there be some limits on collection. The other provisions support the minimality requirement, and in the case of the 'anonymity' provision, go beyond it.

Limits on visual surveillance

In content unusual for a data protection law, there are strict limits on operation of 'visual data processing devices', such as CCTV, both in public ('open') places,[111] and for some sensitive uses within enclosed spaces. The meaning of 'visual data processing device' is limited to 'devices installed continuously at a certain place' to take (and store or transmit) pictures of persons or things.[112] So a human photographer is not included, nor a device which does not take a representation of a person/thing but only some abstract information such as height or speed. Where these provisions apply the data collected is not considered **(p.141)** to be 'personal information',[113] and the normal PIPA provisions do not apply; however, analogous protections apply, including prohibition of use of the information for purposes other

than the initial one; prohibition of directing cameras to new locations; prohibition of collection of audio data in addition;[114] and strict security measures.[115] The details of article 25 and related provisions are not covered here.

Purpose limitation and consent—Google's combined terms of service

The first decision made by the PIPC[116] was that Google's January 2012 changes to the terms of service (TOS) of over 60 of its services, unifying them in a single TOS, may be in breach of various provisions of PIPA. Google's TOS changes, which became effective on 1 March 2012, were considered by the PIPC to be likely to breach PIPA in three ways: (i) they did not specify the purpose of collection clearly enough, and could not comply with the requirement that personal information may only be collected and used to the minimum extent necessary for the purpose for which it is collected; (ii) they did not comply with the requirement that where personal information is to be used for purposes other than the purpose for which it was collected, it is necessary to obtain additional consents for such uses; and (iii) they did not specify that that personal information would be erased immediately upon the expiration of its retention period or on request from a data subject.[117] The PIPC decision has not subsequently been confirmed (although the PIPC stated it was waiting for Google's response), nor revoked, and no further decision on this was made by the PIPC in 2013–14. Although the PIPC is reported as stating that 'possible further steps could include administrative and criminal sanctions but the most likely outcome in the long term if Google continues its stance will be a fine up to one percent of its annual revenue', it is not clear what role the PIPC would play. It may have been referring to the penalty that the KCC could impose in an enforcement action against an ICSP.

4.4. Disclosure and use limitations—strict consent rules

Articles 17 and 18, setting out the basic principles, are somewhat overlapping and confusing, but are in fact consistent. Other principles elaborate the meaning of consent, and impose special rules for data exports, processing, and sale of businesses.

Consent-based limits

Consent for disclosure by a processor to third parties is required, except where such disclosure is 'within the scope' of the purpose of collection.[118] Individuals must be informed of the identity of the party to whom the personal information is to be disclosed, the proposed uses, retention, the fact that consent may be denied, and the consequences of refusal of consent.[119] This is the basis of informed consent. In effect, consent is also **(p.142)** required for any change of use by the controller,[120] and the individual must be informed of the same matters before there is informed consent.[121]

In relation to both disclosure to third parties and change of use by the controller, there are limited exceptions to the need for consent: where special provisions exist in other laws; where the data subject (or legal representative) is not in a position to give consent, or their address is unknown, and it is necessary to protect the interests of the data subject or a third party (but not the interests of the processor); or whether the use or disclosure is for 'statistics or academic research' and individuals are 'kept unidentifiable'.[122] Furthermore, the use or disclosure must not be likely to infringe unfairly on the interests of the data subject or a third party. There are further limited exceptions applicable only to public authorities,[123] and where they are relied upon this must be gazetted or notified on the agency's website.[124] The consent requirements of the Korean Act are one of its strictest requirements, and an aspect that will be considered onerous by some businesses.

PIPA also imposes individual obligations on anyone processing personal information prohibiting them from disclosing personal information obtained in the course of business or providing it to another without authority.[125]

Examples of disclosure and use complaints

The majority of the reported PIDMC mediation cases from 2002–2007[126] concerned breaches of the previous (similar) disclosure principles. In the reported case resulting in the highest damages to date, a

woman specifically requested her mobile phone company not to disclose details of her telephone calls to anyone else. Then she found that a branch of the telephone company had nevertheless disclosed them to her ex-husband, who had produced a copy of her ID card when applying for the details. The mobile phone company was held responsible for professional negligence, and she was awarded 10 million won (equivalent to US$10,000) in compensation for the economic and mental damages. Other reported cases have resulted in damages, more typically of a few hundred dollars. These have involved matters such as (damages amounts are stated in approximate US$): a plastic surgeon displayed a movie of a patient's operation on his clinic's website (US$4,000), and the award would have been increased if she had objected during the filming; a translation service company posted a woman's résumé on its website without her consent, as if she was an interpreter employed by them (US$200); an insurance company provided a person's personal information to another company so that it could solicit business from that person (US$200); a telecommunications company failed to stop telemarketing after a person unsubscribed (US$300); and disclosure to a family member was a breach (US$100).

Since 2007 there have been similar reported cases concerning the previous Act.[127] A company printing wedding invitations used surplus invitations to show to prospective customers, disclosing photos of previous couples (US$200). 'Before and after' photos of a complainant's plastic surgery, placed on a clinic's website, were blurred but still recognizable and were a very serious breach (US$3,000). Disclosure of a complainant's phone call history to his wife, by a telco, which did not sufficiently check the documents presented by **(p.143)** his wife, was in breach and found to be a contributing factor in a successful divorce action against him (US$5,000).

Consent—a strong interpretation

The Korean Act is unusual in both the range of circumstances where consent of the data subject is required (most disclosures and change of use, and data exports) and in what is required for consent to be legitimate. Notifications that must be given before consent is obtained (e.g. under article 15(2) or 18(3)) must explicitly separate three types of matters requiring consent, so as to assist data subjects to recognize what requires consent and what does not:

> (i) each matter requiring consent must be stated separately, and each consent obtained separately, so that it is possible to consent to one but to refuse consent to another (i.e. no 'bundling' of different consents);[128]
> (ii) where information is collected which requires consent, it shall be segregated from information which does not require consent (i.e. there should be no misleading bundling of information), and the burden of proof that no consent is required is borne by the processor;[129]
> (iii) if consent is being obtained so as to use information 'to promote goods or services or solicit purchase therefor' then the data subject must be told this, and their consent to this obtained (i.e. data subjects must opt-in to marketing uses of their information, a stronger requirement than in Europe or other laws in the region).[130]

A processor must not deny the provision of goods or services to a data subject who refuses to provide consent under article 22(2) or (3), or 'additional consent' under article 18(2) to allow additional uses or disclosures of personal information beyond what was consented to at the time of collection.[131] This does not cover article 22(1), only because article 16(2) already provides that there can be 'no denial' of services because of refusal to provide more than the minimum information a processor is entitled to require.

Additional requirements for the method by which consent must be obtained under article 22(6) are provided by the Enforcement Decree.[132] Though there is no explicit requirement that consent must be express, the better interpretation of the above provision, and of article 17(2) of the Enforcement Decree, is that it must be express. For example, it is difficult to see how the right 'to elect the scope of consent'[133] could be implemented as implied (opt-out) consent. This is different from some legislation in the region (e.g. Australia) which allows consent to be implied. Knowingly providing or receiving personal

information without the required consent is an offence.[134]

Examples of consent complaints

Since 2007 there have been reported cases concerning consent under the previous Act.[135] A complainant who stopped halfway through completing an online 'Marriage Club' **(p.144)** enrolment form was entitled to object when the defendant company used the information she had provided to contact her ($US300).

Control of processing by data controllers

When a data controller consigns processing of personal information to another party, it must document or get an agreement concerning (i) prevention of use other than consigned purpose; (ii) technical and managerial safeguards; and (iii) other matters required by the Enforcement Decree.[136] The data controller must inspect these matters, as required by the Enforcement Decree.[137]

Notice of the fact of processing to the data subject is also required,[138] and the processor must be identified. Alternatively, a notice of processing must be posted on its website or at a publicly visible place for more than 30 days. This applies even if the 'processing' is marketing ('public relations') on behalf of the data controller.[139] It will also apply to any overseas processing.

Processors are deemed to be employees of the data controller,[140] who therefore has vicarious liability for their actions. However, the processor also has separate liability for any use of the personal information beyond the purpose of consignment or disclosure of the information.[141] Almost all other obligations of data controller[142] also apply to the processor.

Sale of businesses

The Act is very strict in relation to business transfers, and may be a disincentive to the sale of some information-based businesses if it is likely that existing customers would object to the transfer of their personal information to a new owner. Data subjects must be informed of the transfer of their personal information as the result of sale of a business in whole or part, and that they have a right to opt-out (withdraw consent) from their personal information being transferred,[143] at which point it is (presumably) destroyed. This notice must be given by the previous owner prior to transfer,[144] but if it has not been given, it must be given by the new owner upon receipt of the personal information.[145] In any event, the purchaser can only use the personal information for the purpose for which it was held by the seller.[146]

4.5. Sensitive data and IDs

Sensitive data cannot be processed without consent. In South Korea 'sensitive data' includes 'ideology, belief, admission/exit to and from trade unions or political parties, political mindset, health, sexual life',[147] 'DNA information obtained from genetic examination', and certain criminal history data under the extinction of punishment legislation.[148] Laws and regulations may make exceptions.[149] The consent required is a specific (non-bundled) **(p.145)** consent obtained where the individual is informed of the content required by articles 15(2) or 17(2).

Special restrictions on unique identifiers including Resident Registration (RR) numbers

The most controversial personal information in South Korea is the resident registration (RR) number which was previously compulsory in almost all dealings with government and many organizations in the private sector.[150] 'Unique identifiers', namely RR number, passport number, driver's licence number, and alien registration numbers[151] may not be processed unless (i) the same consent is obtained as for sensitive data processing or (ii) there is explicit legislative approval.[152] The public sector is exempted.

Alternative means of identification other than the RR number must now be provided by processors where individuals are subscribing to web-based services, by specified means.[153] Additional 2012 legislation imposed even tighter requirements on ICSPs, who are prohibited from collecting RR numbers

except in very narrow circumstances.[154] Further 2013 legislation, effective August 2014, prohibits any organization from processing RR numbers, except where laws or regulations explicitly require or allow this, or it is explicitly necessary for the protection of life, body, or property of the data subject or a third party.[155] MOSPA is also to take into account the role of RR numbers in any data breaches, in deciding whether to apply very high 'surcharges' on companies responsible.[156] It is therefore, increasingly difficult for private sector organizations to make use of the RR number except where legislation requires this. Further restrictions may follow the 2014 data breach catastrophe (see section 8.2 of this chapter). However, there is still considerable concern among Korean commentators that there are too many laws allowing or requiring use of RR numbers, and thereby exempt from PIPA, article 24, and so RR numbers are still very widely used and collected. Continuing heavy reliance for identity verification is seen to be an unnecessarily high risk of privacy invasion and identity theft. Particular problem areas are seen as the ICN Act, which allows the KCC to authorize by regulation any ICSP to collect RR numbers (and that the KCC has authorized all telcos to collect RR numbers),[157] and that the Real Name Financial Transactions Act requires use of RR numbers, requiring all banks and credit card companies to collect them.[158] The evolving history of the use of RR numbers in Korea is on the one hand one of the most significant attempts in any country to 'roll back' **(p.146)** a surveillance mechanism, but on the other hand is a project that is arguably far from complete.

4.6. Security safeguards

Security and data quality

Detailed security measures ('technical, managerial and physical measures') are required, both locally and for data exports, with six types of measures prescribed,[159] including management plans, access controls, encryption, log-in records, upgrading of security measures, and storage protections. The obligations are not in the form used in the OECD Guidelines (i.e. 'take reasonable steps') but the stronger requirement of taking whatever steps are 'necessary to ensure' security.[160] There are also likely to be considerable obligations in relation to data transferred abroad: 'The government shall work out relevant policy measures so that the rights of data subjects may not be infringed upon owing to cross border transfer of personal information.'[161]

Under the previous Act, South Korea was particularly proactive in trying to get businesses to improve their data security, rather than sitting back and waiting for complaints. Security measures have been reinforced by the new Enforcement Decree in which six types of required security measures are spelled out.[162] These also apply to unique identifiers.[163] Further details of security measures will be established and notified by MOSPA. PIPA also imposes individual obligations on anyone processing personal information, prohibiting actions which 'damage, destroy, alter, forge or leak another's personal information'.[164]

Mediation cases reported by the PIDMC from 2002–07 under the previous Act include breaches of the requirements to take security measures, usually with compensation required for 'emotional damage': a social networking site allowed disclosure of a member's personal information due to errors in its search software (US$500); even the unexpected disclosure of a third party's personal data due to an error in website software was regarded as a breach deserving compensation to the person to whom the data was exposed (US$60). Since 2007, PIDMC-mediated security complaints included a number of compensation payments because of inadequate security measures, including exposure on the Internet of a patient's extensive medical records, kept for research purposes by a medical institution (US$2,000); and exposure of intimate communications on a social network site (US$500).

Data breach notification

Large-scale data breaches have been a very significant issue in South Korea for many years, with a catastrophic breach experienced at the start of 2014 (see section 8.2 of this chapter). Data breach notification to data subjects is mandatory,[165] including what was leaked, when and how, steps to take in mitigation, countermeasures being taken, and where to report damage. There must also be notification to MOSPA and to either KISA or the National Information Society Agency (NIA) if the breach is 'large scale'

(affecting over 10,000 data subjects).[166] Details must be posted on websites for seven days.[167] Additional 'surcharges' **(p.147)** of up to 500 million won (US$500,000) may be imposed by the MOSPA where RR numbers have been lost, stolen, leaked, altered, or damaged by a processor who has failed to take necessary security measures.[168] ICSPs have additional obligations to notify the Korean Communications Commission (KCC) or the KISA of any 'data leak or breach'.[169]

An increasing number of victims go to court to claim for damages, but usually fail to get compensation owing to the difficulty to prove the causal relation between the data leakage and loss of property or mental distress.[170] 'Voice phishing' (i.e. using the telephone to obtain personal information by deception) has posed particular problems in Korea, and victims experienced great difficulty in recovering their funds, so a special law has been enacted to facilitate recovery.[171]

4.7. International data flows—export restrictions and extraterritoriality

The data export restrictions in PIPA are not 'border based', in that they do not depend on what data privacy laws exist in the jurisdiction in which the data is received. Data exports (disclosures to 'a third party overseas') are subject to prior consent of data subjects, after disclosure of all matters required by article 17(1), and processors must not make contracts to export data in violation of the Act.[172] In other words, consent first needs to be obtained. There is, however, no requirement to inform data subjects about the country of destination, and the state of its laws. This is a weakness in the Korean law, because it is difficult to see how data subjects can give informed consent if they have no idea to where their personal data is destined to be sent, nor what privacy protections are provided there. Where consent is obtained (by using standard contractual clauses adopted in South Korea), and overseas disclosure made, the original data controller is not liable for any breaches of the Act by the recipient, even if no effective remedies are available in the overseas destination. There still may be liability under the Civil Act tort provisions (see section 2.3 this chapter).

Overseas processors other than acting for the benefit of the original collector (i.e. data controller) will be considered to be a ?third party? for purposes of A 17(3), and so consent to overseas processing in such case is required, not only notice (as required for a Korean processor). The Korean data controller will also remain vicariously liable for any breaches by the overseas processor for the benefit of the Korean data controller. In case of transfer of a database of clients or business itself to a third party overseas, a relevant notice and corresponding consent are required as if it is a Korean party.[173] There are no explicit provisions dealing with extraterritorial application of the Korean law.[174]

(p.148) 4.8. Rights of the data subject

The rights of data subjects in relation to their personal information are first stated very generally: to be informed of processing; to consent to processing, including to 'elect the scope of consent' (i.e. unbundle consents); to confirm processing; to demand access (including 'issuance of certificate'); to suspend processing; and 'to make correction, deletion and destruction'.[175] These rights are then expanded by specific provisions, discussed at various points in this section.

Access and correction rights

The procedures for access include justifiable grounds to suspend or deny access to part or all of a record.[176] The content which can be accessed includes not only the content held, but the purpose of collection and use, the retention period, details of disclosures to third parties, and details of consents by the data subject.[177] Access must be provided within 10 days.[178] Access to public sector files can be via either the agency concerned or MOSPA.[179] Correction (and deletion) requests must also be decided within 10 days, and if denied the reasons (including information about how to appeal) must be provided in a standard outcome notice.[180]

Notification of data collection from third parties

On request from the data subject, notification is required of the details of data collection from third parties.[181] In practice, it is most likely to occur after the data subject has obtained access to his or her

file. This notification must include an explanation that the data subject is entitled to demand suspension of the processing of that personal information. Identification of the source is also required except where (subject to the data subject's interests not being higher), there is a danger to the 'life or body' of another, or the 'property or interests' of another, or to a list of prescribed public interests.

Deletion rights and suspension of processing

A data subject may request deletion of any personal information except that collected under other laws and regulations.[182] South Korea does have something close to the 'right to be forgotten'. In addition, automatic destruction of personal data is required after the purpose of processing is complete, or any other retention period completed.[183] Retention periods must be specified at the time of collection, so this is another period that must be complied with. Suspension of processing can also be required by the data subject,[184] subject to limited exceptions.[185] Outcome notices must be given for refusals of deletion or suspension.

(p.149) The deletion and suspension provisions indicate very clearly the extent of control over their personal information that individuals are given by the South Korean law, not only in relation to content provided by the data subject, but also in relation to data provided by third parties. A very informative PIDMC decision is one where the plaintiff had consented, when joining the defendant's online service, to his name, place of work, school he had graduated from, and address being displayed on the defendant's website. He later decided that he wanted this information to be deleted, and the defendant denied this, saying the consent was irrevocable. The PIDMC upheld his request for deletion, referring not only to the equivalent to article 37 under the previous law, but also to the plaintiff's constitutional right to self-determination of his personal information (*Fingerprint Case*).[186]

Other complaints mediated by the PIDMC involving deletion rights or suspension of processing (with compensation noted) have included the following: failure to delete data, and to continue to use it for telemarketing after requests to cease (US$200); continued receipt of marketing messages after ceasing to use a service (US$200); and continued sending of spam despite claimant's express rejection of such messages (US$200 and education of staff required).

5. Reactive enforcement in South Korea

Compared with any other data privacy legislation in Asia, South Korea's PIPA has two strong advantages. It gives regulators a wide range of sanctions of differing degrees of seriousness, which can be applied to a situation, both in terms of measures which are reactive to an individual problem, and measures which are systemic. This flexibility is one of the key elements of theories of 'responsive regulation' (see Chapter 3, section 4.2). Secondly, it does not leave enforcement to the discretion of regulators, but gives people who have been affected by privacy breaches both individual and collective remedies that they can initiate themselves. The broader scope of the new Act, and its stronger principles, also apply these remedies to more situations.

The foundation of enforcement under PIPA is that any data subject who suffers damage may sue for damages for breach of any provision of PIPA.[187] Such actions take place in the civil courts, not before a specialist tribunal. However, most breaches are dealt with by the KISA Privacy Center (informal mediation) or the PIDMC (formal mediation) before civil actions are necessary.

5.1. Individual dispute informal mediation by the KISA Privacy Center

Individuals with complaints about breaches of the Act can apply for mediation directly to the PIDMC.[188] In practice, however, they will first report a dispute to the KISA Privacy Center or '118 Call Center' established by the MOSPA in the KISA,[189] which has the functions of receiving, investigating, and 'counselling' such complaints.[190] If such informal advice or mediation does not resolve the matter, the complainant will be advised to apply to the PIDMC for formal mediation.

(p.150) Statistics from 2007–2011 reported by the KISA Privacy Center[191] concerning breaches of data privacy legislation show the total number of complaints received. The sixfold increase over six years

is startling: 25,965 (2007), 39,811 (2008), 35,167 (2009), 54,832 (2010), 122,215 (2011), and 166,801 (2012). Almost all of the huge increases in 2011 and 2012 came from the category of complaint 'damage, infringement or theft of other person's data', with a lesser contribution from 'data leakage out of failure of technical and managerial measures of the data processor' (such as in large-scale data breaches). Park suggests that popular demand for 'withdrawal of consent from, or membership in the portal sites' was a major factor. He also considers that a series of large-scale data breach incidents in 2011 meant that many users 'found fault with insufficient technical and managerial measures taken by portal site operators'. It may be that the 2012 legislative changes to the use of RR numbers will cause changes to this behaviour, and to complaints numbers in future years.

5.2. Individual dispute formal mediation by the PIDMC

Personal Information Dispute Mediation Committees (PIDMC) (see section 3.3 this chapter) mediations usually involve individual disputes with businesses, whereas disputes between individuals usually go to the court. Until PIPA, the PIDMC could only mediate in disputes with private sector processors, but it now covers public sector processors as well.[192] The considerable advantage of PIDMC mediation to data subjects is there is no cost involved in commencing a mediation request, and data subjects may be self-represented.

PIDMC sub-committees propose informal settlement of complaints, after considering documents from the parties and, if necessary, evidence from the parties or witnesses.[193] The PIDMC proposes a draft settlement for agreement by the parties[194] within 60 days from the filing of the petition.[195] If it is accepted, the mediation record is executed[196] and becomes legally enforceable like an out-of-court settlement.[197] The parties are required to notify acceptance or rejection within 15 days.[198] The PIDMC may also suspend mediation proceedings which it thinks are inappropriate, and must do so if a party commences litigation.[199] The data subject may take the matter to court at any time, and the PIDMC is required to suspend the dispute mediation and notify the other party of filing of a lawsuit. The Civil Mediation Act applies in relation to any procedures not covered by PIPA.[200] The remedies which can be proposed in a PIDMC draft mediation are very broad, and include suspension of infringing activity, damages, restitution and 'other necessary remedies', and preventive measures to prevent future occurrences.[201]

Throughout this chapter, examples have been given of the types of breaches which have resulted in compensation payments following PIDMC mediation. The statistics of cases referred to the PIDMC from 2007–12, and the outcomes of those mediations 2009–12, have been translated by Whon-il Park[202] from official sources (see Table 5.1).[203] The average number of **(p.151)**

Table 5.1 Outcomes of PIDMC mediations, 2009–2012 (Park)

Classification	2009	2010	2011	2012
Both parties' agreement prior to mediation	50	53	21	32
Institutional improvement after mediation	41	12	11	12
Institutional improvement and damages after mediation	31	32	31	26
Damages after mediation	20	87	7	6
Rejection of application of mediation	3	6	55*	20
Dismissal of application due to deficient legal requirements	–	1	1	47
Total	145	191	126	143

(*) Fifty-two simultaneous petitions by the same plaintiffs against five ISPs were rejected on account of insufficient proof: see Tables 2–4, Pico and KISA, *Personal Information Dispute Mediation Cases in 2012* (in Korean), May 2013, p. 24.

mediations over the four years was 151 per year, with the number per year not increasing over that

time. Bearing in mind that these are formal mediations, and that they usually result in a finding by the mediation panel both in relation to whether there has been a breach of the Act, and what are the appropriate remedies, this is a substantial number. It should also be remembered that company privacy officers should provide 'remedial compensation' before matters ever get to the PIDMC.

The most common subject matter classifications of these mediations were 'out-of-purpose use or onward transfer of data' and 'data leakage out of failure of technical and managerial measures of the data processor', which together accounted for about 60 per cent of all mediations.

Of the cases where mediation resulted in a finding in favour of the complainant, 76 per cent (242) resulted in payment of damages as part or all of the remedy, whereas only 24 per cent (76) resulted in institutional improvement but no payment of damages. The 156 cases settled prior to mediation but after referral to the PIDMC may well have also involved a substantial number of agreements to pay damages, but this is not known.

These statistics are consistent with analysis of 22 reported cases in 2003–04 where English language summaries are available. The PIDMC awarded compensation (from US$100–10,000) in 17 cases. Damages ranged from US$100 to US$10,000.[204] In only a few published cases of breach did the PIDMC recommend corrections or other remedies without any payment of compensation. The KISA Privacy Center/PIDMC combination has been claimed to be very effective[205] and has resulted in numerous accepted mediations, usually involving modest payments of compensation.

5.3. Civil damages actions

Any data subject who suffers damage may sue for damages in the courts (not before a specialist tribunal) for breach of any provision of PIPA.[206] However, as discussed in the previous two sections, most breaches are dealt with by the PIDMC before civil actions are necessary. As mentioned in section 4.2, while the plaintiff will have the civil onus of proof of the existence of a breach, if processors wish to avoid liability, they have the onus of proof of lack of 'wrongful intent or negligence'.[207] If the processors wish to reduce the damages payable, they have the onus of showing 'compliance with the Act' and 'non-negligence of **(p.152)** due care and supervision'.[208] However, most of the victims of massive scale data breach incidents have difficulty in proving the causal relation between the data leak and their pecuniary damage. Even victims of voice phishing could not prove that the personal information used in the voice phishing came from the data breach incident about which they were complaining. Generally speaking, appropriate remedies cannot be found for large-scale data breach incidents because the damage that can be proven to be causally related is limited to mental distress, and there is the associated risk to the losing party of being required to pay the proceedings expenses and legal cost of the winning side ('costs follow the event').

5.4. Collective mediation and class actions

Collective dispute mediation by the PIDMC is now possible.[209] Where multiple data subjects are affected, any parties can request the PIDMC to undertake collective dispute mediation. Procedural details are set out in the Enforcement Decree.[210] Contrary to the normal rule, mediation continues even if some of the complainants go to the court.[211] Additional data subjects, or additional processors, can make a request to be joined in the mediation.[212]

Proceedings are also now like class actions provided by the new Act for the prevention or suspension of violations of data protection under the name 'Data Protection Collective Suit' (Chapter 7 of the Act). This collective suit is only applicable if and when a processor rejects collective mediation under article 49, or does not accept the mediation award. Various types of consumer organizations or non-profit civic groups, defined in the Act,[213] are then entitled to file a collective suit. Suit can only be filed in the District Court of the defendant's place of business, or of the main office of a foreign business's representative.[214] Collective suit proceedings are subject to the Civil Procedure Act and the Civil Execution Act, if applicable, in addition to this Act, and the Supreme Court Rules as well.[215]

5.5. Compliance orders (MOSPA and PIPC)

MOSPA (acting through KISA) has considerable powers to give orders and advice concerning remedial measures when breaches of the Act have been found. It can order any private sector processors to suspend violating actions, or temporarily suspend processing, or take other remedial measures, and other relevant ministries and agencies are given similar powers in relation to bodies under their jurisdiction.[216] MOSPA can advise government bodies to do likewise.[217] It can also advise that disciplinary action should be taken against individuals.[218] In 2013 MOSPA took 468 enforcement actions under PIPA, including 113 administrative fines. Two-thirds were in the private sector. The Financial Supervisory Service also made orders under the Credit Information Act.

(p.153) 5.6. Offences and administrative penalties

It is not an offence simply to breach a provision of PIPA, but Chapter 9 of the Act sets out very complex lists of offences and administrative fines (with graduated penalties) which occur when particular sections are breached.[219] Breaches of specified provisions of articles may result in offences punishable by imprisonment from up to between two and five years, and fines of up to between 2 million and 5 million won (US$2,000–$5,000).[220] Major disruptions to public sector institutions are offences punishable by up to 10 years' imprisonment and fines of up to 100 million won (US$100,000).[221] The first criminal prosecutions for breaches of the previous Act took place in 2010,[222] but prosecutions under the new Act are reported to be increasing.

A lengthy list of lesser breaches, are subject to administrative fines for negligence, of up to 50 million won (US$50,000).[223] These will now include processing a RR number without authority.[224]

5.7. Publication of investigation results—'name and shame'

MOSPA or the relevant central agency may, subject to the 'deliberation and resolution' of the PIPC, make the following information publicly available: identity of violators; substance of violations; and actions taken, including punishments and advice given.[225] The information must be published on the government body's website and in a general daily newspaper.[226] Before the PIPC considers whether such publication should be made, MOSPA or the agency concerned must take into account such matters as the seriousness, repetition, and damage resulting from the violation, and give the respondent an opportunity to put their case against disclosure.[227]

5.8. Joint penalties for breaches

If a data controller's employee, agent or representative (including a processor) breaches any of the penal provisions in articles 71–73 then the data controller will be subject to the same fine, unless the data controller can prove it was not negligent in its supervisory duties.[228]

6. Systemic enforcement measures in South Korea

In any data privacy system, the proactive steps that regulators can take to increase the level of compliance with legislation can be just as important as the 'reactive' effect of actions to enforce the legislation. Under the previous Act, KISA undertook a wide variety of proactive measures, not just complaint investigation, and this will continue under PIPA. The systemic measures are decentralized under PIPA, and MOSPA has a variety of functions relevant to systemic enforcement, particularly concerning various forms of education and **(p.154)** support for compliance.[229] The functions of education and public relations concerning data protection, and of fostering specialists and developing criteria for privacy impact assessments have been delegated by MOSPA to its National Information Society Agency (NIA).[230] MOSPA has the function of running education programmes for privacy officers.[231]

6.1. Accountability—privacy officer and supervision of 'data handlers'

Almost all organizations are required to provide a privacy officer with specific duties including developing a data protection plan and 'internal control system', surveying the actual practices of the organization,

dealing with grievances and providing 'remedial compensation', developing education within the organization, and destroying 'personal information whose purpose of processing is attained or retention period expired'.[232] These are significant and comprehensive obligations. The privacy officer must have rights of inspection, is required to 'take immediate corrective measures' where necessary, and must not be disadvantaged for carrying out his or her obligations. The required level of position for privacy officers is prescribed for all types of organizations, to ensure that these positions are sufficiently senior.[233]

Data controllers also have a specific obligation to properly supervise, and to educate, everyone who handles personal information on their behalf.[234]

6.2. Compliance checking

Under the previous Act, KISA conducted surveys of compliance with privacy protection provisions[235] in such areas as mobile communications, online shopping malls, banking and financing, department stores, accommodation and travel. It also monitored whether websites provided information required in a privacy policy such as purpose of collection and use of personal information, and whether they properly implemented permissions for access to the collected data, the period of retention, etc.

Under PIPA, similar practices will continue. For example, following the large-scale data breaches in February 2014 (see section 8.2 of this chapter), systemic campaigns to prevent ID abuse and misuse are planned. The first step will be the mandatory encryption of the RR numbers on any banking form (currently optionally adopted), following a unanimous National Assembly amendment to PIPA.[236] This will be extended to all RR uses by 2016.

(p.155) ### 6.3. Mandatory PIAs in the public sector

Where, according to criteria set out in PIPA Enforcement Decree,[237] 'probable' violation of privacy will result from operation of personal information files by a public sector body, the head of that body must conduct 'the assessment for the analysis and improvement of such risk factors' (a privacy impact assessment or 'PIA'), covering specified matters, to be carried out by a 'PIA Institution'.[238] Factors to be considered include the amount of personal information being processed; whether it is provided to third parties; probable risks; whether sensitive data or unique identifiers will be processed; and the retention period,[239] and there are detailed specifications of what is required by a PIA.[240] PIA Institutions may be designated by MOSPA, according to specified criteria.[241] MOSPA may provide its opinion, subject to the deliberation of the PIPC, upon receiving the PIA results.[242] MOSPA is to facilitate carrying out of PIAs.[243] The PIA results must be registered with the files concerned,[244] so it appears that details of the results of the PIA will be available to any person. The Korean provisions are the only mandatory PIAs in Asia.

Private sector processors are only required to make 'positive efforts' to conduct a PIA if privacy violations are 'highly probable' in operation of particular system of files.[245] It remains to be seen what pressure MOSPA or the PIPC will bring to bear on private bodies to conduct PIAs.

7. Co-regulation and self-regulation measures in South Korea

In contrast with Korea's structure for both complaint-driven enforcement, and for proactive enforcement, self-regulation and co-regulation has not been regarded as a central element of privacy regulation. PIPA requires the MOSPA to 'promote and support' self-regulatory measures, including a 'privacy mark system'.[246] It is authorized to provide them with assistance to promote such activities.[247] There are no provisions in PIPA allowing co-regulatory schemes (such as approved codes) to supplant or supplement the legal regime. As self-regulation is not common in regulatory schemes in South Korea, the position of privacy regulation is not exceptional. There was no significant self-regulation in South Korea under the previous Act.[248]

A new Personal Information Protection Level Certification Management System (PIPL) has been

implemented by MOSPA by regulations under PIPA, article 13.[249] Companies and government agencies are now eligible to apply for certification. Certification will provide benefits for companies including reduced supervision and potentially reduced penalties. Alternative certification systems operated by another ministry already operate in South Korea, so the significance of this system will need to be seen in practice. Under the **(p.156)** previous Act, a semi-official 'Privacy Mark' scheme for websites was also established by the Korea Association of Information and Telecommunication (KAIT), a private entity supported and supervised by the government.[250]

8. Conclusions—South Korea, leader in data privacy innovation

South Korea's democracy is still less than a quarter-century old and with continuing post-authoritarian desire to protect liberties. When coupled with the ubiquity of computing, the Internet, and mobile telecommunications in Korean life, liberties are underpinned by a constitution and a Constitutional Court responsive to privacy issues. The PIPA is consistent with this environment and is the most innovative data privacy law in Asia, although its enforcement has not yet fully proven itself.

8.1. Innovations in PIPA

Among the significant innovations in PIPA's privacy principles are the requirements for most businesses and agencies to have privacy officers; strong data minimization through anonymous transactions requirements; the prohibition on 'denial of service' and various requirements to 'unbundle' consents; opt-in required for marketing using a company's own databases; mandatory data breach notification to both affected individuals and to authorities; deletion of data on request; various forms of joint liabilities; and a 'rolling back' of uses of the RR number. Some of these are innovations from a global perspective, not only in Asia.

Innovations in the enforcement aspects of PIPA include South Korea's long-standing innovation in mediation through the PIDMC, now enhanced by collective mediation for disputes with widespread small damage; clear provisions for 'name and shame' publication; mandatory privacy impact assessments (PIAs) for potentially dangerous public sector systems; and extremely high financial penalties for misuse of RR numbers. PIPA includes almost every type of enforcement mechanism, with a wide range of degrees of application, so there is no impediment in theory to the law being well enforced. After two years of operation, there is evidence of active enforcement but it is by a variety of bodies. The new PIPC, despite its innovative status as the first DPA in a civil law country in Asia, has done little that is visible to establish its credentials as an enforcement body. Despite decentralization and limited translation from Korean, the transparency of the Korean system, through various types of publications, is also one of its stronger points, despite the fact that the overall distribution of enforcement powers and responsibilities in Korea is not yet clear. This uncertainty over enforcement calls into question what would otherwise be a clear leading role for Korea in privacy protection in Asia.

8.2. 2014 privacy catastrophe points to further reforms

At the start of 2014 a massive data breach in South Korea involved 104 million data items being stolen from three credit card companies, including RR numbers and sufficient information for current credit cards to be used.[251] At the time of writing, collective court **(p.157)** actions against the companies are threatened, top company officials have announced their intention to resign, and the seller and buyers of the data have been indicted. On March 10, 2014, the government announced proposed further law reforms in the finance sector, including: punitive surcharges of up to 5 billion won (US$4.6 million) on companies causing or exploiting leakage of personal data, plus a one per cent surcharge on resulting transactions; a prohibition on sharing of personal information between affiliated companies without consent; and prohibition of SMS dissemination without consent. All telemarketing was also suspended for two months to reduce fraud possibilities, causing lay-offs of thousands of telemarketers, and US insurers arguing that this was in breach of the US–Korea Free Trade Agreement. Parliamentary hearings on strengthening data protection laws will also be held in a pre-election climate. South Korea's highly interconnected and technological society is likely to continue to indicate the direction that Asian data protection laws will take. It is the 'canary in the coalmine' where problems, and solutions, happen first.

9. Appendix—North Korea, a surveillance state

9.1. Overview

This book is about data privacy, not surveillance, so there is little to say about North Korea (the Democratic People's Republic of Korea or 'DPRK') that deserves more than a brief end-note to the chapter on what is at present another country, South Korea. It is easy to forget that 'from 1953 to the early 1970s, the DPRK was at least economically the equal, if not more, of a struggling South Korea',[252] but its economy collapsed from the mid-1980s, hastened by the end of the Soviet bloc (and its trading advantages) from 1989. With a third generation of leader from the same family installed in 2012, the DPRK is at present a hereditary dictatorship.[253] It stands out from the other communist one party regimes in Asia (China and Laos)[254] not only in this stunted aspect of its political structure, but also in its shrunken state-dominated economy and the brutality of its regime, including the pervasiveness and intensity of its surveillance of the North Korean people. The report of a UN Commission of Inquiry on human rights in the DPRK[255] (the 'Kirby Commission') has found that:

> systematic, widespread and gross human rights violations have been and are being committed by the [DPRK]. In many instances, the violations found entailed crimes against humanity based on State policies.

Speculation about the likely future of North Korea ranges from whether that might involve an evolution toward a more modern state based on something more like the Chinese model, to more extreme predictions of collapse followed by reunification with the South.[256] **(p.158)** Of course, it may continue to defy expectations that it must change in some dramatic fashion, and continue as an isolated, intermittently belligerent regime in an impoverished country.

However, some attention to North Korea is justified in this study, if only because, if reunification of Korea occurs, the unified polity will face similar issues to those faced by Germany following reunification of East and West. There will be difficult questions to be resolved concerning the extent to which secret police files should be open to the victims of state surveillance, and the identities of informants revealed to their victims, equivalent to those concerning the Stasi files in Germany. Something similar may occur if the North Korean state otherwise evolves toward becoming a state not involved in crimes against humanity against its own people. It is, therefore, worth mentioning some aspects of what is known of the surveillance system in North Korea.

9.2. State surveillance in North Korea

The DPRK is a state whose existence is based upon continuing surveillance of its population by the state apparatus, and no privacy rights are respected. The Kirby Commission found that:[257]

> State surveillance permeates the private lives of all citizens to ensure that virtually no expression critical of the political system or of its leadership goes undetected. Citizens are punished for any 'anti-State' activities or expressions of dissent. They are rewarded for reporting on fellow citizens suspected of committing such 'crimes'.

Whether 'North Korea collapses, evolves, or continues to muddle through, will depend a great deal on the viability of this all-pervasive [surveillance] apparatus', argue some authors.[258] There is no reason to expect any reform of this aspect of the regime, because that would rapidly undermine its continued existence in anything like its current form. As the Kirby Commission found, the 'key to the political system is the vast political and security apparatus that strategically uses surveillance, coercion, fear and punishment to preclude the expression of any dissent'.[259] Among its recommendations, but scarcely likely to be voluntarily adopted, are that the DPRK should:[260]

> dismantle the neighbourhood watch (*inminban*), the secret resident registration file system, and all surveillance of persons and their communications that serve purposes of political oppression and/or are not subject to effective judicial and democratic control; and publicly acknowledge the

> extent of surveillance practices carried out in the past and provide citizens with access to their resident registration file

These recommendations indicate the types of preconditions for protection of human rights that will be necessary when the existing regime is replaced and North Korea develops in the direction of a normal state.

(p.159) 9.3. State, law, and theoretical privacy rights

North Korea's legal system has taken an essentially Stalinist interpretation of law as a weapon to implement state policy, with no role for concepts such as the rule of law. The concept of Juche ('often translated simply as self-reliance or self-determination, but…essentially a nationalist ideology of "North Korea first"') was introduced into the North Korean Constitution in 1972.[261] The Korean Workers' Party (KWP) prevails over all state organs including the legislature and the court. The judiciary was found by the Kirby Commission to be one of the 'main perpetrators' of systematic human rights violations including crimes against humanity. In contrast, the Constitution of North Korea provides:[262]

> Citizens are guaranteed inviolability of the person and the home and privacy of correspondence. No citizens can be placed under control or be arrested nor can their homes be searched without a legal warrant.

This provision has been comprehensively breached, as is clear from the Kirby Commission report.

Notes:

([1]) Quotations from a business conference in Washington, cited in BNA staff, 'Strict New Privacy Law's Grace Period For Enforcement Ends March 31, 2012' (2012) 12 WDPR 25, *BNA World Data Protection Report*. See also Graham Greenleaf, 'Korea's New Act: Asia's Toughest Data Privacy Law' (2012) 117 *Privacy Laws & Business International Report*, pp. 1–6.

([2]) Government of Korea (in Korean) <http://www.index.go.kr/potal/main/EachDtlPageDetail.do?idx_cd=1345>.

([3]) For accessible histories of modern Korea, see Michael Robinson, *Korea's Twentieth-Century Odyssey: A Short History* (University of Hawaii Press, 2007); Francis Pike, *Empires at War: A Short History of Modern Asia Since World War II* (I B Tauris, 2011), chs. 14, 25, 44, and 57. For more detail on international relations see Don Oberdorfer, *The Two Koreas: A Contemporary History* (Basic Books, 2001).

([4]) Robinson, *Korea's Twentieth-Century Odyssey*, pp. 1–2.

([5]) Robinson, *Korea's Twentieth-Century Odyssey*, ch. 4.

([6]) Robinson, *Korea's Twentieth-Century Odyssey*, p. 139.

([7]) Robinson, *Korea's Twentieth-Century Odyssey*, p. 174 (and see ch. 8 for details of the events outlined in the previous paragraph).

([8]) This section is derived primarily from Youngjoon Kwon, ch. 5 'Korea: Bridging the Gap between Korean Substance and Western Form' in E. Ann Black and Gary F. Bell (Eds.), *Law and Legal Institutions of Asia* (Cambridge University Press, 2011). Another valuable source, though now dated, is Dae-Kyu Yoon, ch. 5 'Korea' in Poh-Ling Tan (Ed.) *Asian Legal Systems: Law, Society and Pluralism in East Asia* (Butterworths, 1997). See also Jootaek Lee, 'A Research Guide and a Bibliography for Korean Legal Resources in English' (GlobaLex, Nov./Dec. 2012) <http://www.nyulawglobal.org/globalex/South_Korean_Legal_Resources1.htm>.

([9]) Kwon, ch. 5 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, p. 154.

([10]) Kwon, ch. 5 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, p. 166.

([11]) Constitutional Court, 'Case Statistics of the Constitutional Court of Korea' <http://english.ccourt.go.kr/home/english/decisions/stat_pop01.jsp>.

([12]) Kwon, ch. 5 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, p. 163; Yoon, ch. 5 in Tan (Ed.) *Asian Legal Systems*, p. 179.

([13]) Robinson, *Korea's Twentieth Century Odyssey*, p. 171.

([14]) They were found to have secretly and illegally intercepted the conversations of 1,800 politicians, journalists, government officials, and businessmen: Whon-il Park, ch. 7 'Republic of Korea' in James Rule and Graham Greenleaf (Eds.), *Global Privacy Protection: The First Generation* (Edward Elgar, 2008); 'Ex-KCIA Heads Arrested for Eavesdropping 1800 VIPs' (*JoongAng Daily*, 17 November 2005).

([15]) For a summary see Whon-il Park, ch. 7 in Rule and Greenleaf (Eds.), *Global Privacy Protection*, pp. 214–15 and 227.

([16]) Sang Jo Jong, 'Systemic Government Access to Private Sector Personal Data in the Republic of Korea' (2014) 4(1) *International Data Privacy Law*, pp. 21–9.

([17]) Seoul High Court Decision 2011NA19012, 18 October 2012, cited by Jong, 'Systemic Government Access to Private Sector Personal Data in the Republic of Korea', p. 25.

([18]) Jong, 'Systemic Government Access to Private Sector Personal Data in the Republic of Korea', p. 25.

([19]) Jong, 'Systemic Government Access to Private Sector Personal Data in the Republic of Korea', p. 27.

([20]) Constitution (South Korea), art. 17.

([21]) Constitution (South Korea), art. 16.

([22]) Constitution (South Korea), art. 18.

([23]) Constitution (South Korea), art. 37(1).

([24]) Constitution (South Korea), art. 37(2).

([25]) Constitution (South Korea), arts. 21(1) and 21(2).

([26]) *Mandatory Seatbelt*, 2002Hun-Ma518 [2003] 15-2(B) KCCR 185 (30 October 2003), English summary at <http://english.ccourt.go.kr/home/english/decisions/mgr_decision_list.jsp>. See also Supreme Court Decision 96Da42789, 24 July 1998.

([27]) *Collecting and Computerizing Fingerprints and Using them for Investigation Purposes case* (2005) 17-1 KCCR 668, 99Hun-Ma513 and 2004Hun-Ma190 (consolidated) (26 May 2005). English summary <http://english.ccourt.go.kr/>.

([28]) Article 44–5 of the Act on Promotion of Information and Communications Network Utilization and Data Protection, etc. ('ICN Act') required large-scale portal sites (more than 100,000 visitors on average a day) to record the real name identities of visitors posting comments. The poster's resident registration number was usually used to verify whether the name given by an Internet poster was his/her real name. One justification for the law was that the poster's details could be disclosed if a victim then wanted to take legal action for defamation or privacy breaches.

([29]) Constitutional Court Decision, 2010Hun-Ma47, 23 August 2012. An English summary by Whon-il Park is available on KoreanLII <http://koreanlii.or.kr/w/index.php/2010Hun-Ma47>.

([30]) For details see Whon-il Park and Graham Greenleaf, 'Korea Rolls Back "Real Name" and ID Number Surveillance' (2012) 119 *Privacy Laws & Business International Report*, pp. 20–1 <http://ssrn.com/abstract=2187232>.

([31]) *Disclosure of Military Health Records of Public Officials Case*, 2005 Hun-Ma 1139 [2007] KRCC 4 (31 May 2007), English summary at <http://www.asianlii.org/kr/cases/KRCC/2007/4.html>.

([32]) *Report of the Number of Cases Accepted and the Amount of Case Acceptance by Attorneys Case*, 2007Hun-Ma667 [2009] KRCC 26 (29 October 2009). English summary at <www.asianlii.org/kr/cases/KRCC/2009/26.html>.

([33]) *No-smoking Zone and Right to Smoke Cigarette Case*, 2003Hun-Ma457 [2004] KRCC 10 (26 August 2004). English summary at <http://www.asianlii.org/kr/cases/KRCC/2004/10.html>.

([34]) *Information Publication Prohibition Case* 2008Da42430, decided 2 September 2011.

([35]) National Human Rights Commission Act (South Korea), art. 25.

([36]) Whon-il Park, ch. 7 'Republic of Korea' in Rule and Greenleaf (Eds.), *Global Privacy Protection: The First Generation*, pp. 212–13.

([37]) *Retention of Graduates' Information Case*, 2003 Hun-Ma 282, 425 (consolidated); [2005] 17-2 KCCR 81 (21 July 2005). English summary at <http://english.ccourt.go.kr/home/english/decisions/mgr_decision_list.jsp>.

([38]) National Human Rights Commission Decision, 12 November 2007.

([39]) *Information Publication Prohibition Case* 2008 Da42430, decided 2 September 2011.

([40]) Civil Act (South Korea), art. 750 (Definition of Torts): 'Any person who causes losses to or inflicts injuries on another person by an unlawful act, wilfully or negligently, shall be bound to make compensation for damages arising therefrom.'

([41]) Civil Act (South Korea), art. 751(1) (Compensation for Non-Economic Damages) provides that: 'A person who has injured the person, liberty or fame of another or has inflicted any mental anguish to another person shall be liable to make compensation for damages arising therefrom.'

([42]) *Violation of Privacy*, Supreme Court Decision 2012Da31628 27 June 2013. The facts are from the court summary. The court also considered when otherwise tortious acts 'can be justified because they occurred at a public place, or were performed in order to collect evidence for a civil suit', and the burden of proof of such a defence.

([43]) *Case of Damages Claim Regarding Leak of Customer Information*, Supreme Court Decision 2011Da59834,59858,59841 26 December 2012 <http://library.scourt.go.kr/jsp/html/decision/9-69%202012.12.26.2011Da59834.htm>. The facts are from the court summary.

([44]) Whon-il Park, 'Data Breach Incidents' (KoreanLII, 2014) <http://koreanlii.or.kr/w/index.php/Data_breach_incidents>. The following discussion is substantially based on, and in places paraphrases, his analysis.

([45]) Whon-il Park, 'Koreans' ID Numbers Fall Prey to Hacking Business' (2011) 112 *Privacy Laws and Business International Newsletter*.

([46]) *SK Communications Case #2* was decided on 15 February 2013; 'No More Information Leaks' (*Korea JoongAng Daily*, 18 February 2013) <http://koreajoongangdaily.joins.com/news/article/Article.aspx?aid=2967249>.

([47]) Whon-il Park, 'Auction Case' (KoreanLII, 2014) <http://koreanlii.or.kr/w/index.php/Auction_case>.

([48]) 'In Korea, the collective suits are quite different from the class action in the United States. In Korea, all defendants should file a suit individually with a court to claim damages against the plaintiff. Also it is different from the collective action led by an eligible civic organization under the Framework Act on Consumers': Whon-il Park, 'Data Breach Incidents'.

([49]) 'Seoul Central District Court Found NC Soft Guilty for Lineage II Data Leak' (*Chosun Ilbo*, 29 April 2006).

([50]) 'Collective Action Suits Over Data Leak May Cost 3 Card Firms 170 bln won' (Yonhap News, February 2014) <http://english.yonhapnews.co.kr/search1/2603000000.html?cid=AEN20140203002700320>.

([51]) Criminal Act (South Korea). See for example art. 316 (Violation of Secrecy); art. 317 (Occupational Disclosure of Other's Secret); art. 347-2 (Fraud by Use of Computer etc.); art. 355 (Embezzlement and Breach of Trust); art. 356 (Occupational Embezzlement, Occupational Breach of Trust); and art. 366 (Destruction and Damage, etc. of Property).

([52]) Whon-il Park, ch. 7 in Rule and Greenleaf (Eds.), *Global Privacy Protection*, pp. 210–11.

([53]) Previously called the Ministry of Government Administration and Home Affairs.

([54]) PIPA (South Korea). This Act is usually referred to as 'PIPA' rather than 'the PIPA'.

([55]) Shin Ji-hy, 'Google May Face Penalty Over Privacy' (*Korea Herald*, 24 January 2014) <http://www.koreaherald.com/view.php?ud=20140121000864>.

([56]) PIPA (South Korea), art. 6.

([57]) In relation to the public sector, privacy protection provisions are found in the Act on the Communication Secrets, the Telecommunications Business Act, and the Medical Services Act.

([58]) Other private sector legislation containing data protection provisions includes the Use and Protection of Credit Information Act, the Act on Real Name Financial Transactions and Confidentiality, the Framework Act on Electronic Documents and Electronic Commerce and the Electronic Signature Act, the Act on the Protection and Use of Location Information, and the Act on the Creation and Facilitation of Use of Smart Grids.

([59]) During the previous Lee Myung-bak government, it was the Ministry of Public Administration and Security (MOPAS).

([60]) PIPA (South Korea), art. 7.

([61]) PIPA (South Korea), art. 8.

([62]) Personal Information Protection Commission (PIPC) website <http://www.pipc.go.kr/cmt/main/english.do>.

([63]) As is typical in South Korea, the provisions here include that five 'shall be appointed or commissioned from among the candidates elected by the National Assembly', and another five 'from among the candidates designated by the Chief Justice of the Supreme Court'. Other appointees are to be persons

recommended by 'privacy-related civic organizations or consumer groups' or 'by the trade associations composed of personal information processors' and others 'who have ample academic knowledge and experiences related with personal information'.

([64]) However, some South Korean civil society observers consider that the PIPC's independence remains to be demonstrated because it is ministry-based, in that the PIPC does not yet have administrative staff whose principal loyalties are to it and its decisions (personal communications with the author).

([65]) MOSPA guidelines and other related laws, regulations, guidelines, and informative materials (in Korean) are available online at the Personal Information Protection Portal <http://www.privacy.go.kr/index.jsp>.

([66]) PIPA (South Korea), art. 40.

([67]) PIPA (South Korea), art. 9.

([68]) PIPA (South Korea), art. 12(2).

([69]) PIPA (South Korea), art. 11.

([70]) For KISA's activities regarding Internet security see <http://www.kisa.or.kr/eng/activities/mainActivites.jsp>.

([71]) KISA is delegated by the KCC to take necessary measures upon the occurrence of such Internet incidents such as hacking, computer virus, denial of service, etc. under art. 48(2) of the ICN Act. It is designated by MOSPA as the '118' call centre which will deal with any violation of the rights or interest related to personal information under art. 62(2) of PIPA and art. 56 of the Enforcement Decree.

([72]) KISA 'Privacy' (website, in Korean) <http://privacy.kisa.or.kr/kor/main.jsp>.

([73]) PIPA Enforcement Decree, art. 62(3). It can be contacted by dialling '118' like an emergency call.

([74]) PIPA (South Korea), art. 40.

([75]) PIPA (South Korea), art. 40(3) and PIPA Enforcement Decree, art. 50(2).

([76]) Personal Information Dispute Mediation Committee (PIDMC/Pico) <http://kopico.or.kr/>.

([77]) PIPA (South Korea), art. 12(2).

([78]) PIDMC, *Personal Information Dispute Mediation Cases* (PIDMC, 2012) <http://kopico.or.kr/data/after/read.jsp?reqPageNo=1&rowNum=0&rowCount=14&searchHospitalFK=0&stype=&sval=>.

([79]) Korean Personal Information Dispute Mediation Committee Cases (2002–07) (WorldLII) <http://www.worldlii.org/kr/cases/KRPIDMC>. English translations are by the PIDMC. Unfortunately, the PIDMC's reporting in English was declining in quantity from 2004–07 and in the seriousness of the matters reported. For example, its 2007 Annual Report only includes six examples of minor disputes, with the highest amount of compensation being US$500.

([80]) Whon-il Park, 'PIDMC Cases: Noteworthy Cases' (KoreanLII, undated) <http://koreanlii.or.kr/w/index.php/PIDMC_cases#Noteworthy_Cases>.

([81]) KoreanLII: Korean Law via the Internet <http://koreanlii.or.kr>.

([82]) 'Data protection' (KoreanLII) <http://koreanlii.or.kr/w/index.php/Data_protection>.

([83]) PIPA (South Korea), art. 3.

([84]) PIPA (South Korea), art. 4.

([85]) PIPA (South Korea), arts. 15–39.

([86]) PIPA Enforcement Decree (KoreanLII, transl. Whon-il Park) <http://koreanlii.or.kr/w/images/d/d7/DPAct_EnforceDecree.pdf>. The Decree was issued 29 September 2011, came into force from 30 March 2012, and as at December 2013 was the only one issued.

([87]) MOSPA, 'Standard Guidelines' issued September 2011.

([88]) '"Personal information" shall mean the information pertaining to any living person that makes it possible to identify such individual by his/her name and resident registration number, image, etc. (including the information which, if not by itself, makes it possible to identify any specific individual if combined with other information)' (art. 2).

([89]) '"Processing" shall mean the collection, generation, recording, storage, retention, value-added processing, editing, retrieval, correction, recovery, use, provision, disclosure and destruction of personal information and other similar activities' (art. 2).

([90]) PIPA (South Korea), art. 58(1).

([91]) PIPA (South Korea), art. 58(4).

([92]) PIPA (South Korea), art. 58(3).

([93]) PIPA (South Korea), art. 30.

([94]) PIPA (South Korea), art. 30(3).

([95]) In addition there is a requirement in the public sector that all personal information filing systems, with some specified exceptions, must be registered with MOSPA, with the registry being open to 'any person', whether or not they are a data subject of one of the files registered (PIPA (South Korea), art. 32). This is an implementation of the OECD Guidelines 'Openness principle'.

([96]) PIPA (South Korea), arts. 16, 22(2), 39.

([97]) PIPA (South Korea), art. 39(1).

([98]) PIPA (South Korea), art. 39(2).

([99]) PIPA (South Korea), art. 31.

([100]) PIPA (South Korea), art. 3.

([101]) PIPA (South Korea), art. 4.

([102]) PIPA (South Korea), art. 15(1).

([103]) Similar to EU Directive, art. 7(f); see European Union Agency for Fundamental Rights (FRA), *Handbook on European Data Protection Law* (FRA, 2013), pp. 84–90.

([104]) PIPA (South Korea), art. 15(2).

([105]) PIPA (South Korea), art. 16(1).

([106]) PIPA (South Korea), art. 3(7).

([107]) PIPA (South Korea), art. 16(2).

([108]) PIPA (South Korea), art. 24(4).

([109]) PIPA (South Korea), art. 16(2), amended 23 March 2013 and effective 7 August 2014.

([110]) PIPA (South Korea), art. 59(1).

([111]) The CCTV provisions previously in the Public Agency Data Protection Act have been incorporated into PIPA (South Korea), art. 25.

([112]) PIPA (South Korea), art. 2.

([113]) PIPA (South Korea), art. 58(2).

([114]) PIPA (South Korea), art. 25(6).

([115]) See PIPA, arts. 25(6) and (7) and PIPA Enforcement Decree, arts. 22–27.

([116]) Personal Information Protection Commission (South Korea) Decision, 'Comments on Improvements of Privacy Policy of Google Inc.', 11 June 2012, <http://www.pipc.go.kr/pds/news/120612.html>.

([117]) Graham Greenleaf and Whon-il Park, 'Korean DPA Faults Google's TOS Changes: Global Privacy Implications?' (2012) 119 *Privacy Laws & Business International Report*, pp. 22–5 <http://ssrn.com/abstract=2186874>.

([118]) PIPA (South Korea), art. 17(1).

([119]) PIPA (South Korea), art. 17(2).

([120]) PIPA (South Korea), art. 18(2).

([121]) PIPA (South Korea), art. 18(3).

([122]) PIPA (South Korea), arts. 18(2)1-4.

([123]) PIPA (South Korea), arts. 18(2)5-9.

([124]) PIPA (South Korea), art. 18(2).

([125]) PIPA (South Korea), art. 59(2).

([126]) English summaries of all of these cases are in the Korean Personal Information Dispute Mediation Committee Cases at the AsianLII website <http://www.asianlii.org/kr/cases/KRPIDMC>.

([127]) These examples are all from 'PIDMC cases: Noteworthy cases' (KoreanLII, transl. Whon-il Park, 2007–11) <http://koreanlii.or.kr/w/index.php/PIDMC_cases#Noteworthy_Cases>.

([128]) PIPA (South Korea), art. 22(1).

([129]) PIPA (South Korea), art. 22(2).

([130]) PIPA (South Korea), art. 22(3).

([131]) PIPA (South Korea), art. 22(4).

([132]) They are: (i) in writing, mail, facsimile with data subject's seal or signature, (ii) telephone recording, (iii) telephone notice and web-based consent confirmed by telephone, (iv) web-based consent, (v) e-mail confirmed by corresponding reply, and (vi) any other method similar to above methods.

([133]) PIPA (South Korea), art. 4(2).

([134]) PIPA (South Korea), art. 71(1).

([135]) These examples are all from 'PIDMC Cases: Noteworthy Cases' (KoreanLII, trans. Whon-il Park, 2007–11) <http://koreanlii.or.kr/w/index.php/PIDMC_cases#Noteworthy_Cases>.

([136]) PIPA (South Korea), art. 26(1).

([137]) PIPA (South Korea), art. 26(4).

([138]) PIPA (South Korea), art. 26(2).

([139]) PIPA (South Korea), art. 26(3).

([140]) PIPA (South Korea), art. 26(6).

([141]) PIPA (South Korea), art. 26(5).

([142]) PIPA (South Korea), arts. 15–25, 27–31, 33–58, and 59.

([143]) PIPA (South Korea), art. 27(1).

([144]) PIPA (South Korea), art. 27(1).

([145]) PIPA (South Korea), art. 27(2).

([146]) PIPA (South Korea), art. 27(3).

([147]) PIPA (South Korea), art. 23.

([148]) PIPA Enforcement Decree, art. 18.

([149]) PIPA (South Korea), art. 23(2).

([150]) For example, in 2007, abuse of the RR number, even after some initial limitations on its use, still accounted for over 20% of all complaints received by KISA (over 7,000 complaints per year), with abuse of all other identification information only about one third of that. (KISA/DMC, *2007 Annual Report*: 22.)

([151]) PIPA Enforcement Decree, art. 19.

([152]) PIPA (South Korea), art. 24(1).

([153]) PIPA (South Korea), art. 24(2) and PIPA Enforcement Decree, art. 19.

([154]) ICN Act, art. 23-2(1). The amended ICN Act, effective 18 August 2012, allows only (i) the authentication agencies, designated by the government for the purpose of provision of alternative ID numbers, (ii) qualified ICSPs permitted by the relevant laws, or (iii) the KCC-notified ICSPs which rely on the collection and use of RR numbers on business. This amendment was caused by a series of massive scale data breach incidents in which RR numbers became a prey to hackers and phishing scammers. For details see Whon-il Park, 'Data Breach Incidents' (KoreanLII, in English, undated)

<http://koreanlii.or.kr/w/index.php/Data_breach_incidents>.

([155]) PIPA (South Korea), art. 24-2 (Limitation to processing resident registration number), effective 7 August 2014.

([156]) PIPA (South Korea), art. 34, as amended 2013, effective 7 August 2014.

([157]) Kyung-Sin Park, 'It is Illegal for Telcos to Provide Identification Services' (in Korean) (*Kyunghyuang Sinmun*, 14 March 2013), <http://m.blog.daum.net/ruru63/15972810>.

([158]) Kyung-Sin Park, 'Must Ban Collection of RRNs by Financial Institutions in Wake of 100 Million-people Data Breach' (in Korean) (*Kyung-hyuang Sinmun*, 12 February 2014) <http://news.khan.co.kr/kh_news/khan_art_view.html?artid=201402112046175&code=990303>.

([159]) PIPA (South Korea), arts. 29, 14(2), and PIPA Enforcement Decree, art. 30.

([160]) PIPA (South Korea), art. 29.

([161]) PIPA (South Korea), art. 14(2).

([162]) PIPA Enforcement Decree, art. 30.

([163]) PIPA Enforcement Decree, art. 21.

([164]) PIPA (South Korea), art. 59(3).

([165]) PIPA (South Korea), art. 34.

([166]) PIPA (South Korea), art. 34(3) and PIPA Enforcement Decree, art. 39.

([167]) PIPA Enforcement Decree, art. 40(3).

([168]) PIPA (South Korea), art. 34-2, amended 6 August 2013 and effective 7 August 2014.

([169]) K.B. Park, 'New South Korean Amendments Include New Data Breach Notification Requirements, Expanded Data Protections' (2012) *BNA World Data Protection Report*, referring to 2012 changes to the ICN Act (arts. 27-3, 48-3).

([170]) See the Korean Supreme Court decision discussed in Whon-il Park, 'GS Caltex case' (KoreanLII, 2014) <http://koreanlii.or.kr/w/index.php/GS_Caltex_case> and Whon-il Park, 'Compensation for data breach' (KoreanLII, 2014) <http://koreanlii.or.kr/w/index.php/Compensation_for_data_breach>.

([171]) To facilitate the recovery of damages incurred by the victims of phishing scams the Special Act on the Recovery of Financial Scam Damages via Electric Communications (Act No. 10477, effective 30 September 2011) provides for mandatory extinction of scam-related deposit claims and accelerated recovery of damages. Victims have only to report to the competent police station such phone phishing to stop the payment of scam-related bank deposits: See Whon-il Park, 'Phishing' (KoreanLII, 2014) <http://koreanlii.or.kr/w/index.php/Phishing>.

([172]) PIPA (South Korea), art. 17(3).

([173]) Sung-Hey Park, 'South Korea's New Data Protection Act: Cross-Border Transfer Issues Examined In Relation To The Outsourcing Clause And The Relevant Regulatory Framework' (2011) 11 WDPR 6.

([174]) South Korean authorities have acted as if the Act had some extraterritorial effect. When investigating whether Google's Street View cars collected and stored personal data on unspecified Internet users from Wi-Fi networks in South Korea, the Korean investigators summoned Google

headquarters personnel to Seoul, without the basis of this action being clear.

([175]) PIPA (South Korea), art. 4.

([176]) PIPA (South Korea), art. 35 and PIPA Enforcement Decree, art. 42.

([177]) PIPA Enforcement Decree, art. 41(1).

([178]) PIPA Enforcement Decree, art. 41(3).

([179]) PIPA (South Korea), art. 35(2).

([180]) PIPA (South Korea), art. 36 and PIPA Enforcement Decree, art. 43.

([181]) PIPA (South Korea), art. 20.

([182]) PIPA (South Korea), art. 36(1).

([183]) PIPA (South Korea), art. 21 and PIPA Enforcement Decree, art. 16. For electronic files, this requires 'permanent erasure not to restore data'.

([184]) PIPA (South Korea), art. 37 and PIPA Enforcement Decree, art. 44.

([185]) There are four exceptions: (i) to comply with other laws; (ii) where suspension is likely to cause damage to the life or body or benefits of others; (iii) where necessary for a public institution to carry out its legally required work; and (iv) where necessary to carry out a contract which the data subject has not explicitly terminated.

([186]) PIDMC, 'Online Service Provider's Failure of Deletion of User's Personal Data on the Internet' (KoreanLII, trans. Whon-il Park) <http://koreanlii.or.kr/w/index.php/PIDMC_cases_in_2010>.

([187]) PIPA (South Korea), art. 39.

([188]) PIPA (South Korea), art. 43(1).

([189]) PIPA (South Korea), art. 62(2) and PIPA Enforcement Decree, art. 59.

([190]) PIPA (South Korea), art. 62(3).

([191]) Whon-il Park, 'Data Breach Claims Via KISA Privacy Center' (KoreanLII, undated) <http://koreanlii.or.kr/w/index.php/PIDMC_cases#Data_Breach_Claims_via_KISA_Privacy_Center>. English translation of KISA Privacy Center text by Whon-il Park.

([192]) PIPA (South Korea), art. 43(3).

([193]) PIPA (South Korea), art. 45.

([194]) PIPA (South Korea), art. 46.

([195]) PIPA (South Korea), art. 44.

([196]) PIPA (South Korea), art. 47(4).

([197]) PIPA (South Korea), art. 47(5).

([198]) PIPA (South Korea), art. 47(3).

([199]) PIPA (South Korea), art. 48.

([200]) PIPA (South Korea), art. 50(2).

([201]) PIPA (South Korea), art. 47.

([202]) Whon-il Park, 'Statistics of PIDMC' (KoreanLII, undated) <http://koreanlii.or.kr/w/index.php/PIDMC_cases#Statistics_of_PIDMC>. English translation of PIDMC text by Whon-il Park.

([203]) Pico and KISA, *Personal Information Dispute Mediation Cases in 2010, 2011 & 2012*, March 2011, March 2012, and May 2013.

([204]) See PIDMC 2005.

([205]) Whon-il Park, 'Republic of Korea' in Rule and Greenleaf (Eds.), *Global Privacy Protection*, pp. 217–18.

([206]) PIPA (South Korea), art. 39.

([207]) PIPA (South Korea), art. 39(1).

([208]) PIPA (South Korea), art. 39(2).

([209]) PIPA (South Korea), art. 49.

([210]) PIPA Enforcement Decree, arts. 52–54.

([211]) PIPA (South Korea), art. 49(6).

([212]) PIPA (South Korea), art. 49(3).

([213]) PIPA (South Korea), art. 51.

([214]) PIPA (South Korea), art. 52.

([215]) PIPA (South Korea), art. 57.

([216]) PIPA (South Korea), art. 64.

([217]) PIPA (South Korea), art. 64(4).

([218]) PIPA (South Korea), art. 65.

([219]) PIPA (South Korea), arts. 70–75.

([220]) PIPA (South Korea), art. 72.

([221]) PIPA (South Korea), art. 70.

([222]) In March 2010, the National Police Agency (NPA) filed criminal complaints against two companies that sold used cars and car navigation devices online for allegedly failing to properly protect customer data from unauthorized disclosure.

([223]) PIPA (South Korea), art. 75.

([224]) PIPA (South Korea), arts. 75(2)4-2, amended on 6 August 2013, effective 7 August 2014.

([225]) PIPA (South Korea), art. 66 and PIPA Enforcement Decree, art. 61.

([226]) PIPA Enforcement Decree, art. 61(1).

([227]) PIPA Enforcement Decree, arts. 61(2) and (3).

([228]) PIPA (South Korea), art. 74(2).

([229]) PIPA (South Korea), art. 13.

([230]) PIPA Enforcement Decree, art. 62(1); National Information Society Agency website <http://eng.nia.or.kr/english/eng_nia.asp>.

([231]) PIPA Enforcement Decree, art. 32(3).

([232]) PIPA, art. 31 and PIPA Enforcement Decree, art. 32(2).

([233]) PIPA Enforcement Decree, art. 32(2).

([234]) PIPA (South Korea), art. 28.

([235]) For example, during 2005, KISA documented 3,982 violations of privacy rules in a survey of 27 thousand businesses. Among these were unauthorized use of personal data and collection of children's data without parents' consent. Though the overall compliance ratio in 2005 was slightly over 80 per cent, KISA encouraged the information and communication businesses to implement technological and managerial safeguards, including the adoption of privacy enhancing technologies (PETs).

([236]) PIPA (South Korea), arts. 24-2(2) (2013 amendment in force 7 August 2014) requires that the RR numbers collected and maintained by banks and financial companies must be encrypted by set dates. The 2013 Amendment to PIPA (transl. Whon-il Park) are on KoreanLII <http://koreanlii.or.kr/w/index.php/Data_protection>.

([237]) Mandatory PIAs are applicable to the following personal information files in the public sector: (i) sensitive data or unique identifier-based data of more than 50 thousand people, (ii) personal data of 500 thousand people after consolidating inside and outside personal information files, (iii) personal data of over one million people, or (iv) personal information files where operational systems are modified after the initial PIA (PIPA Enforcement Decree, art. 35).

([238]) PIPA (South Korea), art. 33(1).

([239]) PIPA (South Korea), art. 33(2) and PIPA Enforcement Decree, art. 36.

([240]) PIPA Enforcement Decree, art. 38.

([241]) PIPA Enforcement Decree, art. 37.

([242]) PIPA (South Korea), art. 33(3).

([243]) PIPA (South Korea), art. 35(5).

([244]) PIPA (South Korea), art. 33(4).

([245]) PIPA (South Korea), art. 33(8).

([246]) PIPA (South Korea), art. 13.

([247]) PIPA Enforcement Decree, art. 14.

([248]) Whon-il Park, 'Republic of Korea' in Rule and Greenleaf (Eds.), *Global Privacy Protection*, p. 218.

([249]) *Regulations on the Operation of the Personal Information Protection Level Certification System* (MOSPA Official Notice No. 2013-45), effective 28 November 2013.

([250]) It now operates under art. 15 of the Act on Broadcasting and Communication Development, enacted in 2010.

([251]) For details on all of this section, see Whon-il Park, 'South Korea's Major Financial Institutions Suffer Data Breach' (2014) 127 *Privacy Laws & Business International Report*, p. 6.

([252]) Robinson, *Korea's Twentieth-Century Odyssey*, p. 148.

([253]) For brief histories, see Robinson, ch. 7 'Going it Alone: The DPRK 1953–Present' in *Korea's Twentieth-Century Odyssey*; Pike, *Empires at War*, chs. 26 and 47; Archie Brown, *The Rise and Fall of Communism* (Vintage, 2010), pp. 334–7 and 607–13; Victor Cha, *The Impossible State: North Korea, Past and Future* (Bodley Head, 2012). See also Oberdorfer, *The Two Koreas*. For an account of everyday life in North Korea, state control, and the famine of the 1990s, see Barbara Demick, *Nothing to Envy: Love, Life and Death in North Korea* (Fourth Estate, 2010).

([254]) Brunei is the other absolute monarchy remaining in Asia: see Chapter 14, section 2.

([255]) United Nations General Assembly, *Report of the commission of inquiry on human rights in the Democratic People's Republic of Korea* (UN General Assembly, A/HRC/25/63, January 2014) <http://www.ohchr.org/EN/HRBodies/HRC/CoIDPRK/Pages/ReportoftheCommissionofInquiryDPRK.aspx>. The Commission was chaired by former Australian High Court Justice, Michael Kirby.

([256]) Some think this option is a 'dead letter' because of the enormous costs and problems reunification would bring: Robinson, *Korea's Twentieth-Century Odyssey*, p. 147.

([257]) *Report of the commission of inquiry on human rights in the DPRK*, p. 7.

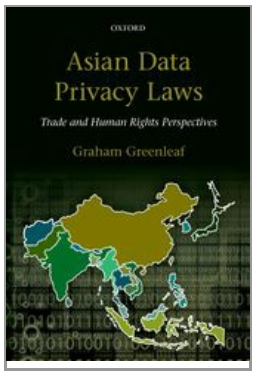
([258]) Ken Gause, *Coercion, Control, Surveillance, and Punishment: An Examination of the North Korean Police State* (Committee for Human Rights in North Korea, 2012), p. 162.

([259]) *Report of the commission of inquiry on human rights in the DPRK*, p. 15.

([260]) *Report of the commission of inquiry on human rights in the DPRK*, p. 17.

([261]) Patricia Goedde, 'Overview of the North Korean Legal System and Legal Research' (GlobaLex, 2008 updated March 2011) <http://www.nyulawglobal.org/globalex/North_Korea1.htm>; Dae-Kyu Yoon, 'The Law and Legal System of North Korea' in Tan (Ed.) *Asian Legal Systems*, pp. 188–93.

([262]) Article 79, Socialist Constitution of the Democratic People's Republic of Korea, 1972 <http://web.archive.org/web/20100703103008/http://www.kcckp.net/en/great/constitution.php>; original source is no longer accessible.



Asian Data Privacy Laws: Trade & Human Rights Perspectives
Graham Greenleaf

Print publication date: 2014
Print ISBN-13: 9780199679669
Published to Oxford Scholarship Online: December 2014
DOI: 10.1093/acprof:oso/9780199679669.001.0001

Taiwan—A Stronger Law, on a Constitutional Base

Graham Greenleaf

DOI:10.1093/acprof:oso/9780199679669.003.0006

[–] Abstract and Keywords

Taiwan's Personal Data Protection Act 2010 (PIPA) strengthens a previous very weak law, but its enforcement is not yet demonstrated. Taiwan has been a post-authoritarian society for 30 years, and is now the only fully democratic polity in the Chinese-speaking world. It has fashioned increasingly strong protections for civil liberties, based on forceful court interpretations of its constitutional protections, and tort protections under its civil code. Consistent with those developments, a previously weak and non-comprehensive data privacy law has been replaced with one that appears to be much stronger, though still missing a separate data protection authority. The PIPA and its Enforcement Rules are analysed in detail. Details of the as yet limited enforcement actions are included, and the limited transparency of the Act is criticized.

Keywords: data protection, privacy, Asia, Taiwan, constitution, China, post-authoritarian

(p.162)

1. Contexts of data privacy in Taiwan

Taiwan has been a post-authoritarian society for 30 years, and is now the only fully democratic polity in the Chinese-speaking world. During that period it has fashioned increasingly strong protections for civil liberties, based on forceful court interpretations of its constitutional protections, and tort protections under its civil code. Consistent with those developments, a previously weak and non-comprehensive data privacy law has now been replaced with one that appears to be much stronger, though still missing a separate data protection authority, but is too new to have yet been enforced. The Republic of China (ROC) is commonly known as 'Taiwan',[1] the name used in this chapter. It has a population of 23 million, comparable to that of many middle-sized countries in Asia.

1.1. Taiwan—political and economic context

Taiwan, as an island south of the Chinese mainland, has had a long and complex relationship with China, first recorded from 230 AD.[2] This history involved long periods as a 'pirate kingdom', complex relations with its other powerful neighbour, Japan, and a 40-year occupation by the Dutch East India Company to 1661. The Dutch were driven out by Cheng Cheng-kung (known as Koxinga), as part of the final resistance by the Ming dynasty, but Koxinga's establishment of a local principality lasted little more than 20 years against the Manchu forces establishing the Qing dynasty.

Taiwan then became a prefecture of the Qing dynasty China's Fukien province from 1683, and became a separate province in 1887 (Taiwan Province). However, it was ceded to Japan by China under the Treaty of Shimoneski (1895) following China's defeat in the Sino-Japanese War.[3] Fifty years of Japanese rule followed. In the aftermath of the Chinese war of liberation from Japanese occupation during World War II and the split between the Communist forces of Mao Tse Tung and the Nationalist (Kuomintang) forces of Chiang Kai Shek, Kuomintang forces eventually retreated to Taiwan. They took control of Taiwan from October 1945 when they entered Taipei following the surrender of the Japanese.[4] Their government continued to use the pre-World War II name of the government on the mainland, 'Republic of China'.

Kuomintang rule in Taiwan was initially authoritarian, effectively denying participation by the local Taiwanese population. Martial law operated until 1987. From the late 1980s, a series of political reforms rapidly transformed Taiwan into a multiparty democracy, with increasingly fair elections and transformation from a 'mainland' regime into a local one.[5] The old 'mainland' deputies elected in China in the 1940s and frozen in office were forced into retirement from 1990 onward and were replaced by ones elected locally.[6] Taiwan's democratization culminated with the election of Lee Teng-hui as the first freely elected president of Taiwan. Given the limitations of democratic developments in the Hong Kong SAR and Macau SAR, Taiwan is now the only fully democratic polity in the Chinese-speaking world.

(p.163) Despite this largely peaceful transformation from authoritarian rule within Taiwan, its international position is still uncertain. The People's Republic of China (the 'PRC' or 'mainland China') continues to claim that Taiwan is part of 'one China', and there is division within Taiwan as to whether it should claim to be a separate country, or should accept eventual peaceful unification with mainland China. As a result, Taiwan's participation in many international organizations is a matter of considerable contention between it and the PRC. The stated intention of the PRC to take military action against Taiwan in the event of a declaration that it is an independent state, coupled with the ongoing military support provided to Taiwan by the United States, has resulted in a continuing heightened level of security concerns within Taiwan.

Since the mid-1950s, the economy of Taiwan has been transformed from a state-dominated agrarian economy to an extremely successful capitalist economy. In 1953, 80 per cent of industrial capacity was state-owned,[7] but by 1983 it had more private companies per capita than any other country and was a major exporter.[8] It is an economy largely based on manufacturing in which the importing of personal data for outsourced processing, or for the provision of services, does not play a major role.

All of these factors have implications for the development of data privacy laws in Taiwan. Like South Korea, Taiwan emerged a little over 20 years ago from a long period of authoritarian rule following Japanese occupation. To some extent, the development of data privacy laws have been part of the development of more liberal political institutions in both countries, but (as we will see), to a lesser extent in Taiwan than in South Korea. Taiwan shares with both South Korea an uncertain security situation and the justifications this provides for increased levels of surveillance. Both have high levels of economic performance and international trade, and consequent pressures to attend to the trade implications of data privacy laws.

1.2. Taiwan's legal and administrative system

The Kuomintang government proclaimed in 1945 that the legal system of the mainland prior to World War II (i.e. that of the then Republic of China) was to be the law applying in Taiwan, with few exceptions.[9] As Wang points out, these pre-1945 mainland laws, drafted mainly in the 1920s and 1930s, were based on European civil law models, particularly those of Germany and Switzerland. For the 50 years prior to 1945, Taiwan's legal system had to a large extent been that of Japan, which had similar European civil law influences, and so pre-1945 mainland law 'was not much different from the Japanese law which had been implemented in [colonial] Taiwan prior to 1945'.[10] It has also been described as 'a primitive form of the Western legal system'.[11] Since 1945 the many major reforms to Taiwan's legal system have not changed the fundamental influence of a civil law approach, however, the introduction of many concepts from US law is creating an increasingly hybrid system. As in other civil law systems, legislation is the most important source of law in Taiwan, with the decisions of courts playing a subsidiary role, primarily that of interpretation and application of statutes.[12] Legislation is based around a number of key Codes (Civil; Criminal; Civil **(p.164)** Procedure; and Criminal Procedure), supplemented by specific laws outside the Codes in some cases. There is no central Code

for substantive administrative law although there is a Code of Administrative Procedure.

Taiwan's parliamentary and administrative system has a number of unique and complex features influenced by the theories of the founder of republican China, Sun Yat-sen, as implemented in the pre-World War II Republic of China.[13] In effect, Taiwan has a unicameral legislature (the Legislative Yuan), which has sole power to enact legislation.[14] Executive power rests jointly with the President, who is directly elected, and with the Premier, the head of the Executive Yuan (Cabinet). The Premier is nominated by the President, with the consent of the Executive Yuan. The Control Yuan exercises powers of audit and censure over government agencies, and is regarded as an independent, quasi-judicial body.

Taiwan's judicial system is unusual. It is headed by the Judicial Yuan, which is essentially an administrative body that does not decide cases. The Supreme Court, High Court, and District Courts apply civil and criminal laws, and there are separate Supreme and High Administrative Courts. Taiwan's courts do not follow a system of precedent where decisions of higher courts bind lower courts, but the Supreme Court does specify that certain decisions are to be regarded as precedents, and if they are not followed this is a ground of appeal.[15]

The Council of Grand Justices comprises 15 Grand Justices, appointed by the President with the consent of the Legislature to serve nine-year terms. The Council deliberates on the interpretation of the constitution and consistency of laws.[16] The Council is unusual in that it is empowered and required to give interpretations of constitutional questions, not only when they are based on a particular set of facts or dispute, but also on 'hypothetical' issues brought to it by various government agencies or individuals and to then give advisory opinions.[17] Its decisions invalidating laws on privacy grounds under the constitution are discussed in the next section and in section 2.2.

1.3. State surveillance and constitutional limits in Taiwan

Illegal wiretapping by the government was seen as a widespread problem in Taiwan. Under legislation from the martial law period 'judicial and security authorities simply had to file a written request with a prosecutor's office to wiretap a suspect's telephone calls'.[18] The Communication Protection and Surveillance Act 1999 imposed stricter controls on when and how wiretaps can be used, including the need for a warrant. Wiretaps can be approved for a list of enumerated crimes, based on sufficient facts, and the absence of any other method of surveillance for domestic wiretaps. There must be court approval for national security wiretaps against foreign governments. The Act also requires telecommunications **(p.165)** providers to assist law enforcement and sets technical requirements for interception, as is common in legislation in other countries.

National identification schemes are well advanced in Taiwan. One report described the compulsory national ID system, but was wrong in assuming the fingerprinting requirement would proceed:

> The government still retains the traditional paper national ID card. However, the

> Household Registration Law requires citizens over age 14 to submit all 10 fingerprints upon receipt of their renewed national ID cards which the Cabinet will use to establish a national fingerprint bank. The government also introduced the Citizen Digital Certificate system, a voluntary electronic card that allows citizens to engage in online activities such as tax filing, labor insurance issues, seniority and personal retirement program inquiry, personal travel restriction inquiry, health insurance personal data and fine inquiry, electronic motor vehicle & driver information needs, digital household registration copies, ID loss report and household registration office e-net services. As of July 2007, 1.2 million cards have been issued.[19]

The Council of Grand Justices was asked to examine the constitutionality of the proposed fingerprinting requirement,[20] and stated 'there are tons of existing laws and regulations requiring that an ROC identity card or a copy thereof shall be presented at the time of exercising one's rights or going through various administrative procedures', which it proceeded to detail, concluding that 'an ROC identity card has become an important document…to identify a person's identity in carrying on their personal and social life'.[21] It considered that the 'issuance or non-issuance of an ROC identity card will have a direct impact on the exercise of the people's fundamental rights' and eventually concluded that to require fingerprinting as a pre-condition for obtaining such a card was unconstitutional.

A health insurance 'smart card' also has near universal coverage:

> Another heavily criticized scheme is a national health insurance integrated circuit (IC) card system using the national ID number, also compulsory, that stores sensitive personal information (such as ICD-9 code for illness classification) on the patient's health insurance IC card. Introduced in 2001, IC cards were issued to 99 percent of citizens by 2004. The card was initially intended to store only enough information to make patient registration easier, but it now includes 'a record of every major illness, injury, organ donation and prescription.' Results of diagnostic tests are also stored on the IC card. Use of the national health insurance IC card at all hospitals and clinics became compulsory in 2004.[22]

The Taiwanese Interior Ministry has also introduced a 'Citizen's Digital Certificate' (using public key 'digital signature' technology), which it describes as 'your internet ID for bilateral identification while you are exchanging information on the Internet'. By 2013 **(p.166)** over 3 million cards had been issued,[23] a high level of take up. It was governed by a regulation under the previous data privacy law.

In the private sector, the most significant information surveillance system is the Joint Credit Information Center (JCIC), the predecessor of which was set up by the Bankers' Association of Taipei in 1975 to exchange credit data among member banks. In 1992–93, the JCIC was first transformed into a non-profit foundation. Later the Ministry of Finance assigned it the task of setting up a nationwide credit database, and it began to put on file the credit data of customers of other financial institutions.[24] There is now concern from non-governmental organizations (NGOs) that, when major Chinese mainland banks are

allowed to establish operations in Taiwan under the Cross-Strait Economic Cooperation Framework Agreement, those banks will become members of JCIC and have access to the financial information of most people in Taiwan.[25]

Taiwan is clearly a society where its high levels of technical sophistication and economic strength have also resulted in large-scale personal information systems. Its data privacy laws are only now starting to come to terms with these developments, but (as we will see), court decisions on its constitution have restrained their development.

1.4. Social attitudes to law, and to privacy, in Taiwan

Wang considers that 'Confucianism still has an impact on the Taiwanese legal system, but its influence is decreasing. Legal culture in present-day Taiwan is a combination of traditional Chinese and modern Western legal concepts'.[26] Perhaps the former is found more in policy objectives than legal form today. Lo considers that the Chinese proverb that it is 'better not to engage in litigation in your daily life' because the results are almost always inauspicious, 'no longer represents a commonly held belief among the Taiwanese', and that the resort to litigation is now becoming much more acceptable as a Western-oriented legal system becomes more established.[27] The concept of data privacy is certainly a modern Western legal concept, irrespective of what roots can be found for a more general concern for privacy in aspects of Chinese culture.

Civil society organizations involved in privacy

The Taiwan Association for Human Rights (TAHR),[28] established in 1984, is the oldest human rights NGO in Taiwan. It has campaigned against ID card proposals in Taiwan, against 'Taiwan's new plan requiring migrant workers from four Southeast Asian countries to submit fingerprint records as part of their Taiwan visa applications',[29] and in favour of additional legislation to regulate credit reporting.[30] In July 2002, TAHR created and coordinated the Personal Information Protection Alliance, which consisted of more than 50 civil societies and NGOs, in order to protest several government schemes that require citizens to submit sensitive personal data.[31] The strong role of civil society **(p.167)** organizations in supporting the taking of privacy issues raising constitutional issues to the Council of Grand Justices is discussed in section 2.2 of this chapter.

2. Privacy protections other than the data protection law in Taiwan

Taiwan may well have stronger constitution-based privacy protection than any other jurisdiction in Asia, with a series of constitutional interpretations, which are suggestive of the European approach of 'informational self-determination'. Taiwan's Civil Code also provides explicit protections against interference with privacy. Treaties are not relevant to privacy protection in Taiwan.

2.1. International obligations and engagements

Because of its disputed position in international law, Taiwan only has limited participation in international privacy developments. Taiwan (as 'Chinese Taipei') is a member of the Asia-Pacific Economic Cooperation (APEC), and is an observer (only) at some OECD meetings, so it did not participate in the revision of (or other activities concerning) the OECD

Privacy Guidelines. Since 1971, Taiwan has not been recognized as a United Nations (UN) member State. Nevertheless it has ratified several international human rights treaties, including the International Covenant on Civil and Political Rights 1966 (ICCPR), Article 17 which requires protection of privacy. In 2012, the Taiwan government released its first state report on the ICCPR and the International Covenant on Economic, Social and Cultural Rights (ICESCR) compliance. It has no access to the UN human rights mechanisms such as treaty bodies; therefore civil society groups are calling on it to set up alternative reviewing mechanisms.[32]

The question of whether an international treaty automatically becomes part of Taiwan's domestic law (the monist approach) is not fully settled,[33] and 'it is dualism that is actually practised' requiring separate legislation to implement most treaties.[34] In any event, there are no treaties relevant to privacy to which Taiwan is a party.

2.2. Constitutional protections

Taiwan's Constitution includes various rights from which a right of privacy may be inferred, but not an explicit clause protecting privacy,[35] although article 12 does provide for 'freedom of privacy of correspondence'. A 1992 decision of the Council of Grand Justices on the obligations of banks to keep credit records confidential left the constitutional breadth of a right of privacy uncertain.[36] Subsequent decisions[37] suggested, but did not decide, that a 'right of privacy' is implied by the Constitution.

(p.168) However, in a 2004 decision,[38] the Council made it clear that privacy is an implied right under Taiwan's Constitution. By using the expression 'the freedom of self-control of personal information' to describe one of the aspects of privacy which is protected, it suggests adoption of the 'informational self-determination' approach that has been taken in European jurisprudence. The Court held that:

> The right of privacy, though not clearly enumerated under the Constitution, is an indispensable fundamental right protected under Article 22 of the Constitution because it is necessary to preserve human dignity, individuality, and the wholeness of personality development, as well as to safeguard the freedom of private living space from interference and the freedom of self-control of personal information (see J.Y. Interpretations Nos. 509 and 535). Where the investigation power exercised by the Legislative Yuan may involve any restrictions imposed on the fundamental rights of the people, not only should there be a basis of law whose contents should be clear and definite, but it should also follow the principles of proportionality and due process of law.

This case involved a petition by legislators to the Council to determine whether provisions of the Act of the Special Commission on the Investigation of the Truth in Respect of the 319 Shooting[39] were unconstitutional. The Council decided, inter alia, that two articles of the law 'have failed to satisfy the requirements for due process of law and the principle of clarity and definiteness of law', and that the provisions of the law were null and void to the extent of this inconsistency. It is difficult to imagine considerations of privacy protection affecting the highest matters of state more starkly than in this case.

A year later, the Council considered the constitutionality of compulsory fingerprinting for ID cards.[40] It reiterated the approach it had taken in the *319 Shooting* decision in different and even stronger terms, and then elaborated on the right of information privacy in language which seem to set the 'goalposts' for what a Taiwanese data privacy law must include if it is to remain constitutional:

> To preserve human dignity and to respect free development of personality is the core value of the constitutional structure of free democracy. Although the right of privacy is not among those rights specifically enumerated in the Constitution, it should nonetheless be considered as an indispensable fundamental right and thus protected under Article 22 of the Constitution for purposes of preserving human dignity, individuality and moral integrity, as well as preventing invasions of personal privacy and maintaining self-control of personal information. (See J. Y. Interpretation No. 585.) As far as the right of information privacy is concerned, which regards the self-control of personal information, it is intended to guarantee that the people have the right to decide whether or not to disclose their personal information, and, if so, to what extent, at what time, in what manner and to what people such information will be disclosed. It is also designed to guarantee that the people have the right to know and control how their personal information will be used, as well as the right to correct any inaccurate entries contained in their information.

(p.169) The Council gave further detail of the content of information privacy protections required from the state, and the extent to which the right of information privacy may be limited:

> Although the right of privacy is fashioned on the basis of preserving human dignity and respecting free development of personality, the mere restriction imposed on the said right does not necessarily lead to infringement upon human dignity. The Constitution does not make the right of information privacy absolute, which means that the State may forcibly acquire necessary personal information in light of public interest by enacting unambiguous laws as far as such laws do not transgress the scope contemplated by Article 23 of the Constitution. In deciding whether the law at issue satisfies the requirements of Article 23 of the Constitution, one should comprehensively take into consideration the public interests to be served by the State's collection, use and disclosure of personal information, and the infringement upon the individual whose right of information privacy is invaded. In addition, different standards of scrutiny should be applied to different cases by looking to whether the personal information to be collected concerns confidential and sensitive matters or whether the information, though neither confidential nor sensitive, may nonetheless easily lead to a complete personal file when combined with other information. Furthermore, in order to ensure a person's individuality and moral integrity, and to protect one's right of information privacy, the State shall also make sure that any and all personal information legitimately obtained by the State be reasonably used and properly maintained and secured. Thus, the

> purposes of the State's collection of the information shall be specifically prescribed by law. After all, failing this, the people will be unable to learn in advance why their personal information will be collected and how the State will use such information so as to enable them to further determine that the competent authorities are collecting their personal information in a manner that is consistent with legally prescribed purposes and are using the same in a reasonable manner.

The Council found that the legislative provisions in dispute amounted to 'compulsory fingerprinting for the purpose of record keeping'. It explained why this was inconsistent with 'constitutional intent to protect the people's right of information privacy' and thus unconstitutional:

> Fingerprints are biological features of an individual's person, which are characterized by personal uniqueness and lifetime unchangeability. As such, they will become a form of personal information that is highly capable of performing the function of identity verification once they are connected with one's identity. Because fingerprints possess such trait as leaving traces at touching an object, they will be in a key position to opening the complete file of a person by means of cross-checking the fingerprints stored in the database. As fingerprints are of the aforesaid characteristics, they may very well be used to monitor an individual's sensitive information if the State collects fingerprints and establishes databases by means of identity confirmation. If the State intends to engage in mass collection of the people's fingerprinting information, such information collection should use less intrusive means substantially related to the achievement of a compelling public interest, which should also be clearly prescribed by law, so as to be consistent with the intent of Articles 22 and 23 of the Constitution.

Attempts to include 'crime prevention' as a legislative purpose of the Household Registration Act 1931 were impermissible 'because the system of separation of household administration and police administration has been reinstated since the end of the Period of National Mobilisation for Suppression of the Communist Rebellion'. This pro-privacy decision was also made under circumstances of high political conflict, in response to a petition filed with the Council by Democratic Progressive Party (DPP) legislators, **(p.170)** supported by over 100 human rights, legal, civic reform, and social groups.[41] In both of these cases, the petitions for review were filed by more than one-third of the members of the Legislative Yuan, in accordance with the Constitutional Interpretation Procedure Act 1948.

The Council returned to the issue of privacy in 2007, referring again to 'self-control of personal information' when it considered the one explicit mention of privacy in Taiwan's Constitution:[42]

> Article 12 of the Constitution provides: 'The people shall have freedom of privacy of correspondence.' Its purpose is to protect the people's right to choose whether or not, with whom, when and how to communicate and the contents of their communication without arbitral [sic – 'arbitrary'?] invasion by the State and others.

> The freedom of privacy of correspondence is one of concrete modes of right to privacy that the Constitution guarantees.

At issue was the constitutionality of article 5-II of the Communication Protection and Monitoring Act 1999 which provided: 'During criminal investigations, the writs of communication monitoring…are issued by prosecutors upon applications from judicial police authorities or by virtue of the prosecutors' own authority.' This provision was held to be in violation of article 12 because:

> It did not require that the writ of communication monitoring be in principle issued by an impartial and independent judge. It charged the prosecutor and judicial police officers, who are responsible for criminal investigations, with the concurrent duties of applying for and issuing the writ of communication monitoring. Such provision can not be regarded as reasonable and legitimate

The Council has continued to issue significant decisions concerning privacy issues, such as whether a law restricting the act of stalking by a journalist violated the Constitution.[43] For the last decade, the decisions of Taiwan's Council of Grand Justices are arguably the strongest and most detailed articulation of the protection of data privacy of any constitutional court in Asia (although recent decisions in South Korea are very strong), particularly as they are based on an implied privacy right.

2.3. General law protections of privacy

A significant development has been the inclusion in the Civil Code since 1999 of explicit protection for privacy through a very general and comprehensive privacy tort in article 195:

> If a person has wrongfully damaged to the body, health, reputation, liberty, credit, privacy or chastity of another, or to another's personality in a severe way, the injured person may claim a reasonable compensation in money even if such injury is not a purely pecuniary loss. If it was reputation that has been damaged, the injured person may also claim the taking of proper measures for the rehabilitation of his reputation.

(p.171) Damage to 'reputation', 'credit', and 'privacy' may easily overlap, but this will not cause problems. The provision is notable for recognizing non-pecuniary loss,[44] and for allowing claims for remedies other than or in addition to damages. Under article 197, claims must be brought within two years 'from the date when the injury and the person bound to make compensation became known to the injured person', or 10 years from when the wrongful act was committed.[45] There are very few Supreme Court decisions related to infringement of privacy, but they can be significant. The highest award of compensatory damages for non-pecuniary loss involving infringement of privacy arose when a well-known author and TV host disclosed during a TV show the home and mobile telephone numbers, and home address of a member of Taiwan's Legislature. He also urged the audience to call or write to the legislator to harass him. In 2004 the court held that the defendant infringed on the legislator's privacy and awarded NT$3,000,000

(about US$90,000) in damages.[46] No clear jurisprudence on article 195 has yet been developed by Taiwan's courts.[47] There are also some privacy protections in the Criminal Code and the telecommunications laws.

2.4. Sectoral legislation

Taiwan's only significant data privacy legislation is its general legislation, discussed below. It does not have significant separate sectoral legislation, such as credit reporting legislation. There are 'Regulations Governing Authorization and Administration of Service Enterprises Engaged in Interbank Credit Information Processing and Exchange', but it is claimed that the emphasis of this law is on setting standards for consent, with little about how data is to be processed and used, and no penalty guidelines.[48] Taiwan has had a Freedom of Government Information Law since 1995, and this provides individuals with rights of access to their personal information held by government bodies. The previous data privacy law provided similar rights from 1995 until 2012.

3. Data privacy legislation in Taiwan

Taiwan's new Personal Information Protection Act 2010 (PIPA), in force only since October 2012, is much stronger in scope, principles, and enforcement provisions than the previous Computer Processed Personal Data Protection Act 1995–2012 (CPPDPA), but does not include a separate data protection authority. How strongly it will be enforced remains to be seen.

3.1. Computer Processed Personal Data Protection Act 1995–2012 (CPPDPA)

Taiwan's Computer Processed Personal Data Protection Act 1995–2012 (CPPDPA) was pioneering data protection legislation in Asia, and was influenced by the OECD privacy Guidelines. The CPPDPA consisted of six chapters: I General Provisions; II Data Processing by Public Agencies; III Data Processing by Non-Public Agencies; IV Damage Compensation and Other Remedies; V Penalties; and VI Supplementary Provisions. It had limited coverage, dealing generally with the public sector, but only eight specified private sector **(p.172)** areas in Part III. It had many other inherent defects including limited coverage of types of data, lack of notice requirements, limited rights of data subjects, and limited penalties, leading commentators to conclude that the CPPDPA was ineffective. Peng found it 'insufficient and flawed';[49] Tang pointed to 'many defects';[50] Chuang says it was 'full of loopholes'.[51] Specific criticisms include vague provisions,[52] limited scope, lack of any general supervisory agency with enforcement being left to the ministries responsible for each industry sector,[53] and lack of evidence that it was enforced or observed.[54]

3.2. New legislation—Personal Data Protection Act 2010

The Executive Yuan (Cabinet) proposed measures to strengthen the CPPDPA as early as 2000.[55] A Bill was introduced in 2005, and the Minister of Justice revived calls for its passage in 2007. The Executive Yuan presented yet another Bill to the Legislative Yuan in January 2009.[56] Legislative pressure increased again after the August 2008 discovery of a very large identity theft ring.

The Personal Data Protection Act (PIPA), enacted 26 May 2010 but only in force from 1 October 2012, is in effect a new piece of legislation. Due to concerns over how it would be implemented and pushback from the financial industry, the PIPA was not brought into force until 1 October 2012, with three particularly controversial articles not brought into force (discussed in the next section). The Enforcement Rules (the 'PIPA Rules') promulgated by the Ministry of Justice (MOJ) comprising 33 articles also came into force on the same day.[57]

3.3. Proposed amendments and articles not in force

In September 2012 the Executive Yuan proposed to the Legislative Yuan an amending Bill that dealt with three main issues: (i) relaxation of notice requirements for information already collected (article 54); (ii) exceptions to restrictions on consensual use of sensitive information broadened to include consent of subject and public interest;[58] and (iii) decriminalization of use and collection of personal information without intent to profit.[59] However, article 41 was brought into force, despite considerable opinion in Taiwan that violations not for profit should not be criminalized.[60] The Executive Yuan may have acted unconstitutionally in not bringing articles 6 and 54 into force:

> **(p.173)** The Executive Yuan's decision to hold back Articles 6 and 54 has occasioned controversy over the constitutionality of declaring parts of a bill operative. Taiwan's Constitution states that the Executive Yuan, which is the supreme organ of executive power, should send an enacted law back to the Legislature for reconsideration if the Executive Yuan believes that the enacted law will be difficult to carry out. Since the Constitution provides an express mechanism (reconsideration) for dealing with impracticable laws, many believe that the Executive Yuan acted unconstitutionally.[61]

In December 2012, some legislators also proposed an alternative draft Bill to amend article 6 by adding 'the consent of the subject' as an absolute requirement for all public or private entities to collect, process, and use any sensitive information, and also limits the purposes for which public entities can do so.[62] During 2013 the MOJ made no attempt to bring these provisions forward, and the new session of the Legislative Yuan has not yet examined them.[63] They seem to be 'frozen' indefinitely,[64] making the final content of the PIPA still somewhat uncertain.

According to media reports,[65] the government was also considering other future amendments to the PIPA. A delegation from the Ministry's Department of Legal Affairs has visited the European Union to learn about efforts to protect personal information in response to social media and cloud computing, and MOJ officials have suggested that the 'right to be forgotten' and a right of erasure should be added to the PIPA. But given the MOJ's lower profile on the previous amendments, this is now less likely.

3.4. PIPA—scope and core concepts

The key concepts underlying the PIPA will be examined before its privacy principles are considered.

Sectoral scope and exemptions

The PIPA distinguishes between a 'public agency' ('a central or local government agency or administrative juristic person that exercises public authority pursuant to law') and a 'non-public agency' ('a natural person, juristic person, or group other than those mentioned' in the definition of public agency), which we could also call a 'private agency'. There are some distinctions between the obligations between the two types of agencies, but otherwise the Act is comprehensive in its scope. The extraterritorial scope of the Act is discussed later under cross-border issues.

There are only two general exemptions from the Act, but (as is normal) there are more specific exceptions from specific principles. 'Collection, processing, or use of personal data by a natural person for purely personal or family activity purposes'[66] is an internationally standard exemption. However, an exemption for 'collection, processing, or use in a public place or public activity of audio-visual data that is not combined with any other **(p.174)** personal data'[67] is a confusingly worded exemption that may cover the operation of CCTV, and photography/video in public places or of (undefined) 'public activity'.

'Personal data', 'personal data file'

The definition of 'personal data' lists numerous categories, and also includes 'other data that could directly or indirectly identify that person',[68] which seems to give it considerable breadth. 'Personal data file' means 'a set of personal data that is systematically built and can be searched or arranged' by automated or non-automated means. Other terms are defined by reference to one or other of these concepts, so the distinction is significant.

To clarify the meaning of the information which may be used to identify a person indirectly, article 3 of the Enforcement Rules expressly provides that information still qualifies as protected personal information if the use of the information alone cannot identify a natural person, but when used in comparison, combination, or connection with other information, the person's identity can be identified. The intention is to remove the risk that 'Given the complexity of [contemporary] society, some information, while not expressly indicating the name, when disclosed is still sufficient to identify the person'.[69] 'Personal information files' includes 'backup files'.[70]

'Collection', 'processing', and 'use'

The obligations depend on which of three related terms (each defined in article 2) are used to specify them. 'Collection' means 'obtaining personal data by any means', an unusually broad definition encompassing collection by observation and extraction from books or databases, from third parties, and from unsolicited or transactional information. 'Processing' means 'the recording, input, storage, editing, correction, reproduction, searching, deletion, output, linking, or internal transfer of data for purposes of building or using a personal data file'. It is therefore very broad but does not include collection, and it also does not explicitly include internal decision-making or actions based on use of personal data, nor the external disclosure of personal data in contrast with 'internal transfer'. 'Use' means 'any utilisation of collected personal data other than processing',

with 'utilisation' seeming to encompass what in other jurisdictions is referred to as both 'internal use' and 'external disclosure'. 'Processing' therefore does not include 'use', and 'use' does not include 'processing'—and 'collection' is separate from either. Harm to data subjects will most often arise from 'use' of their personal data, so it may be expected that more strict obligations will apply to 'use'. 'Use' also does not seem to be limited to personal data in personal data files (in contrast to 'processing') but may apply to personal data not held in such files, though it is not certain that this is what is intended. The expression 'collect, process, or use' is therefore the most comprehensive description of what can or cannot be done with personal **(p.175)** data, and it or variants are used in various places in the PIPA where comprehensiveness is desired.[71]

'Consent'

The PIPA provides that, with exceptions, collection and processing of personal information requires written consent from the person concerned,[72] and additional, separate written consent is required when the personal information collected is used for purposes other than the specified purpose. Consent can be given by electronic record, 'pursuant to the Electronic Signatures Act'.[73] which only requires for such written consent that 'the content of the information can be presented in its integrity and remains accessible for subsequent reference', and that use of an electronic record is with the consent of the other party,[74] and not any stricter requirement such as of use of a digital signature.[75] If both types of consent are to be made in the same written document, the document must make clear that this is occurring and require second consent to be confirmed,[76] so as to avoid the person concerned unknowingly giving blanket or 'bundled' consent.[77]

'Public interest'

The PIPA includes a number of provisions allowing exemption from obtaining the written consent of the person concerned or from informing the person concerned if the collection, processing, or use of the personal information is made for the purposes of public interest and also meets certain criteria. The Enforcement Rules do not define this term. According to Chen, the MOJ explains that 'public interest' is an uncertain legal concept and can be defined differently for different industries and different areas of application, and so the experts from whom it took advice were inclined to leave it undefined.[78]

Responsibilities of controllers and processors

Processors are covered by the provision deeming anyone retained to collect, process, or use personal data to be 'considered the commissioning agency within the scope of the law'[79] so that vicarious liability for their actions remains with the commissioning agency (controller). This applies wherever any legal person, group of persons, or natural person is commissioned by a government or non-government agency. Data subjects are to exercise their rights against the commissioning agency. Article 4 is not explicit as to whether processors are liable to comply with all aspects of the law, but that is the best interpretation, and is consistent with the fact that the Act does impose specific obligations on processors.

The Enforcement Rules set out the duties and responsibilities of the commissioning agency (controller), requiring them to exercise proper monitoring and supervision over the commissioned entity (processor),[80] specifying a minimum list of supervision and regular **(p.176)** verification tasks.[81] If the commissioned entity (processor) believes that the extent to which it is instructed to process personal information, or an instruction by the commissioning agency, violates the law, it is required to inform the commissioning agency of this immediately. As Chen notes,[82] a business cannot hire a professional third party to implement security protection measures on its behalf, and assume this will release it from its responsibilities as a commissioning agency. The commissioning entity must fully understand its obligations under the PIPA to diligently supervise the hired institution and perform them carefully.[83]

4. Data privacy principles in Taiwan

Each of the general data privacy principles in the PIPA will be examined, distinguishing between those of general application, and those applicable to only the private sector or the public sector. Principles applicable only to particular categories of personal data are examined later.

4.1. General requirements for processing

All types of agencies are subject to the general obligations in articles 5–14 (including the data subject rights in articles 10–14 discussed below), but there are also obligations specific to public agencies in articles 15–18 (Chapter II) and to private agencies in articles 19–27 (Chapter III). Article 5 states the most general obligation as: 'Collection, processing, or use of personal data shall respect the rights and interests of the subject, shall be done in an honest and good-faith manner, may not exceed the scope necessary for the specific purposes, and shall have a legitimate and reasonable relation to the purposes of collection'. The requirements of good faith, necessity (relative to purpose), and 'reasonable' relation to purpose of collection therefore suffuse everything that can be done with personal data. Any requirement for consent to processing must come from elsewhere in the PIPA.

4.2. Purpose specification and collection limitations

Public agencies are under less stringent obligations concerning their collection or processing of personal data, but have stricter obligations imposed on its use.[84] They are required to have 'specific purposes' for collecting or processing personal data, and the processing would therefore be required to have the 'legitimate and reasonable relation to the purpose of the collection'. In addition, public agencies may only collect or process personal data in accordance with the scope necessary for the exercise of their statutory duties, or with the subject's written consent, or where 'there is no injury to the rights and interests of **(p.177)** the subject'.[85] This last exemption might seem unduly broad and subjective, undermining the first two exceptions, but it must be borne in mind that a 'reasonable relation to the purpose of the collection' is still required. While there is no requirement of consent for processing (it is only one ground for justification), nevertheless, any processing does require one of these three justifications. In summary, processing injurious to the data subject is illegal unless necessary for a statutory duty

(or with consent).

The private sector also has more strict obligations for use of personal data than for its collection and processing. Private agencies can only collect and process personal data with the written consent of the subject, or under one of six other conditions: express legal provisions; contractual or quasi-contractual relationships; data already voluntarily or lawfully made public; certain anonymous research uses; a broad 'related to public interests' ground; or if 'obtained from a generally available source'.[86] This last ground will not apply if the subject has 'has a material interest in the prohibition of processing or use of the data that obviously is more deserving of protection'. If collectors or processors know that this exception applies, they must on their own initiative delete or cease processing of the data. They must also do so on request.

4.3. Use and disclosure limitations ('purpose limitation'/finality)

Public agencies may only use or disclose personal data in accordance with the scope necessary for the exercise of their statutory duties and 'in conformity with the specific purposes of collection' (not merely having a 'reasonable relation' to it). There follows a lengthy list of allowed uses of personal data by public agencies not in conformity with the specific purpose of collection (secondary uses), including exceptions for uses based on express legal provisions, national security, and other public interests, avoiding danger or harm to the interests of others, the subject's interests (avoiding danger to the subject's life, body, or property and benefiting the rights and interests of the subject), and written consent of the subject.[87] Public agencies must also comply with an 'openness' provision requiring public disclosure on a website of the types of personal data files they keep.[88]

Private agencies have similar restrictions on use of personal data (either internal or by disclosure) and are allowed similar secondary uses as public agencies.[89] Additionally, there are special provisions for direct marketing uses, allowing consumer opt-out, and requiring the provision of a method of opting out at the 'initial time' marketing is done. Of greatest importance, however, is the exception for uses outside the purpose of collection 'to promote public interests'. When coupled with the exception for collection and processing 'related to public interest',[90] these provisions are interpreted as a broad 'media exemption'. Another exemption 'where it is necessary to prevent harm on the rights or interests of other people' is also extremely broad.

4.4. Data quality obligations and user rights

All data users have a positive duty to 'maintain the accuracy' of personal data, and to correct or supplement them on their own initiative.[91] Data subjects also have the right to request corrections or supplementation. Where data users have corrected or supplemented personal data, they must inform prior recipients of that data after it has been corrected or **(p.178)** supplemented. Data users are also required to cease the processing or use of personal data in a number of circumstances: (a) where the accuracy of data is disputed, unless the processing or use is necessary for duties or business and the dispute is specifically noted; (b) wherever there is collection, processing, or use in violation of the Act; and (c) where the purpose of collection has ceased to apply.

4.5. Data security obligations—confusing standards

Public agencies are only required to 'designate dedicated personnel' to handle security matters[92] but there is no stated standard of security of personal data that they are required to achieve. In contrast, private sector organizations are required to 'adopt appropriate security measures', and regulations detailing such security standards (and requiring adoption of security plans) can be made by the 'central competent authorities' for each industry sector.[93] There is therefore a danger of a proliferation of different standards. Article 5 requires of both the public and private sectors that collection, processing or use of personal data 'shall respect the rights and interests of the subject', so a general obligation to take reasonable security precautions may be implied from this. The Enforcement Rules set out 11 types of security measures that may be utilized to comply with these various statutory requirements, which should follow 'the principle of appropriate proportionality'.[94]

4.6. Data breach notification—with limitations

If a public or private sector agency 'violates any provision' of the PIPA, 'such that personal data is stolen, disclosed, altered, or otherwise impaired', then 'the agency, after investigating, shall notify the subjects by an appropriate means'.[95] This was the first enforceable data breach notification enacted in Asia, although the Korean provision was the first implemented. However, it has significant limitations. The obligation does not apply to all 'data breaches', only to those where the agency has breached a provision of the Act. So, theft of data by a third party where it could not be held that the agency was in breach of its security or other obligations, would not be covered, and this is a significant defect. However, the notification requirement could apply not only where an agency failed to discharge its security obligations, but also where it breached some other provision of the PIPA, such as by disclosing personal data to third parties where it should not have done so, or where it made inappropriate use of data. Since failure to notify where appropriate is itself a breach of the PIPA, damages could potentially result from over-defensive failure to notify. The strength of Taiwan's data breach provisions are also impaired by lack of an obligation to inform the relevant supervisory authority, and by lack of clarity concerning to what extent agencies can delay notification by claiming they are still 'investigating'.

The Enforcement Rules clarify what is meant by 'an appropriate means'.[96] When personal information is stolen, revealed, altered, or subject to other infringement, the guiding principle is that the notice be given in a 'proper manner' that guarantees promptness. The notice can thus be given in writing, by telephone, fax, electronically, or in any other manner sufficient to communicate the problem, if it is made promptly. Notice should in principle be given separately to all persons concerned. However, if it takes enormous expense to give notice, the entity may, having considered the technical feasibility and the **(p.179)** protection of the privacy of the persons concerned, give notice through the Internet, news outlets, or in any other manner sufficient to make the information available to the public.

4.7. Data retention (deletion/'anonymization')

Data subjects are entitled to request data users 'to delete' their personal information,[97]

defined as making the information 'disappear' from the file.[98] Data users must cease the processing or use of personal data, or delete it, where the purpose of collection has ceased to apply, or time limits have expired.[99] There is considerable ambiguity about when data users have an obligation to delete or anonymize the data, rather than just discontinue processing it.

4.8. Sensitive data

Under article 6, which has not been brought into force, the default position applicable to both public and private sectors is that 'Personal data related to medical treatment, genetics, sexual life, health examinations, and criminal record may not be collected, processed, or used'. Four exceptions are allowed: where expressly provided by law; where necessary for performance of statutory duties or obligations; where the personal data has voluntarily or lawfully been made public; and for certain research purposes (for which regulations are to be made). There is no exception for the consent of the data subject. Where an exception to article 6 applies, it seems that the applicable provisions would then be the general provisions relating to all personal data (articles 5–9 and the subject rights). Since article 6 does not yet apply, these general provisions for all personal data now apply to sensitive data as well. There are definitions in the Enforcement Rules[100] of 'medical record', 'medical treatment', 'genetic information', 'sexual life', 'health check', and 'criminal record'.

Chen[101] summarizes the definitions as follows (used with permission):

> • *Medical record:* Any medical history or record produced by a medical service provider when performing professional practice in a medical institution or other institution engaged in the practice of medicine. Medical records include: medical records produced by physicians performing professional practice in accordance with the Physicians Act, all medical examination and test report information, and any other records produced by medical service providers when performing professional practice.
> • *Medical treatment:* Any personal information, other than a medical record, that is generated in whole or in part from clinical examination, diagnosis, and therapy made for the purposes of treating, curing, or preventing physical diseases, injuries, or disabilities, or from prescription, medication, application of technique, or treatment made for therapeutic purposes and based on clinical examination or diagnosis results.
> • *Health check information:* An umbrella term for information generated in part or in whole from clinical examination taking the form of medical treatment that is given not mainly for the purpose of diagnosis of a particular disease but to persons looking healthy from outside and without any obvious disease symptoms.
> • *Sexual life:* Having consulted the Australian Privacy Act 1988 and the recommendation proposed in 2007 by the Australian Law Reform Commission (ALRC) for amending the definition of 'sensitive information' in the Privacy Act, the MOJ defines **(p.180)** personal information about sexual

life as consisting of information in relation to a person's 'sexual orientation and practices'.
• *Genetic information:* Messages from a unit of heredity consisting of a segment of human DNA that controls specific functions of the body.
• *Criminal record:* A record that a person has been subject to deferred prosecution, ex-officio non-prosecution, or conviction by a court in a final and irrevocable judgment.

The two Bills still before the Legislative Yuan propose different amendments to article 6. The Executive Yuan's Bill adds medical records as a type of sensitive personal information, and adds two exceptions to the prohibition on collection of sensitive information listed in article 6.[102] The alternative Bill adds 'the consent of the subject' as a necessary requirement for all public or private entities to collect, process, and use any sensitive information, a much more strict approach, and requires public entities to only collect, process, and use any sensitive information for one of four specified purposes.[103]

4.9. Areas of special concern not covered

The following areas of special concern in data privacy, and often covered in the legislation of other countries, are not specifically covered in the Taiwanese legislation: automated decisions ('sensitive processing'); interconnection of files ('data matching'); direct marketing; credit reporting; identity information; use of publicly accessible data ('public registers'); or the Internet.

4.10. Principles concerning cross-border issues

The PIPA inherits from its predecessor CPPDPA weak controls over data exports, but there are some additional protections for data concerning Taiwanese nationals. There is no known instance of enforcement of the very limited CPPDPA provisions for data transfer restrictions.

Extraterritorial scope

This extraterritorial effect of the PIPA is extensive, but only in respect to Taiwanese nationals: it 'also applies to collection, processing, or use outside of the territory of the ROC by a public agency or non-public agency of personal data of nationals of the Republic of China'.[104] We must assume that this only applies to agencies that have otherwise become subject to the PIPA, because if that was not so it could apply to any company anywhere that ever processes data about a Taiwanese national, irrespective of its lack of connection with Taiwan. This could not be intended. However, even with this limitation, it is a significant extension of protection to Taiwanese citizens when their personal data is exported from Taiwan for processing in other jurisdictions (such as the PRC) by a company already bound by the PIPA.

(p.181) Data transfers out of Taiwan (data exports)

Data exports ('international transmission') by private organizations ('non-public agencies') *may* be restricted under the PIPA by 'the central competent authority for the relevant industry',[105] but this is not an automatic prohibition on exports. The authority may

restrict exports which 'involve a material national interest' or are subject to treaty provisions. More significantly, it may do so if 'the receiving nation lacks sound laws and regulations to adequately protect personal data, such that the rights and interests of subjects are likely to be injured', or if an export is 'by a circuitous means to evade' such a prohibition. The use of the undefined term 'adequately' does of course suggest that a standard consistent with the EU Data Protection Directive 1995 is intended. But the key factor is that this is an export prohibition at the discretion of Taiwanese government agencies, and is at the very weak end of the spectrum of export restriction laws. However, this is mitigated somewhat by the extraterritorial provisions protecting Taiwanese and those concerning liability of principals for overseas agents. 'International transmissions' are defined to mean 'transnational (cross-border) processing or utilisation of personal data'[106] so it would seem that data that remains in Taiwan but is processed or used in any way from outside Taiwan is covered. However, 'collection' is not included, so if a person's data is collected from them by an entity outside Taiwan (such as over the Internet), this might not be covered.

Data transfers into Taiwan (outsourcing practices and protections)

Unlike some other Asian jurisdictions (e.g. the Philippines and India) there are no specific provisions exempting outsourced processing in Taiwan from some or all data privacy provisions. The PIPA applies to such processing.

5. Principles concerning rights of data subjects in Taiwan

The data subject rights discussed in this section 'may not be waived in advance nor limited by special agreement'.[107] Overall, this is a strong package of data subject rights.

5.1. Notice and consent requirements

Whenever personal data is collected 'from a subject' (solicited or unsolicited) the collector must 'explicitly notify' the subject of the collector's name, purpose of collection, classification of data collected (this determines the relevant industry sector), 'period(s), region(s), counterparty(ies), and method(s) of use of the personal data', 'rights exercisable by the subject…and method of exercise', and the effect on the subject's rights of not providing the data.[108] A key question here is how precisely subjects will be advised of the 'method of exercise' of their rights, particularly to whom they should make complaints in a system where there is no central data protection authority. This is a potential area of weakness.

There are also overly broad exemptions from this notification obligation.[109] There are five justifiable exemptions (in line with international standards): where another law exempts from the obligation to notify; where collection is necessary for the performance of a statutory duty or obligation; where notification 'would impair the exercise of statutory duties by a public agency' and (perhaps) 'would impair a material interest of a third party'; **(p.182)** and where the subject is fully aware of the contents of the notification. However, the exemption from notification, merely because collection is necessary for the performance of a statutory duty or obligation, effectively eliminates notification from a vast range of transactions and observations without any requirement of justification, in

both public and private sectors.

Where personal data is collected other than from the subject, the notice required by article 8 must be given before processing or use of the data (or concurrently, in communications with the subject[110]). Additional exceptions are provided, including that the personal data has voluntarily been made public by the subject or otherwise has already lawfully been made public, or the impossibility of notifying the subject (or their legal guardian), or statistical or research uses with anonymized results, or collection for 'public interest news broadcasting purposes'. The situations exempted from notification where data is collected from the data subject (discussed in the previous paragraph) are also exempted here. Broad exemptions from notice in relation to collection from third parties are more justifiable than when collection is from the data subject.

Article 54, which has not been brought into force, provides that, in relation to previously collected personal data, notification would be required within one year from the PIPA coming into force, without which any processing or use of the data will violate article 9. This provision may be amended, by the Bill proposed by the Executive Yuan, to a requirement that they be notified before their pre-PIPA personal information is used.[111]

The notice under any of these provisions may be given in writing, by telephone, fax, electronically, or in any other appropriate manner.[112] However, it must be done separately to each person and not by public announcement, including for the notifications in relation to previously collected data.[113]

5.2. Access and correction

Access rights are provided, subject to exceptions where national interests, or the execution of statutory duties, would be impaired.[114] There is also what seems an over-broad exception where access 'would impair a material interest of the collecting agency or a third party', with no requirement that this be balanced against the importance of access to the data subject. Collecting agencies (public or private sector) are given explicit discretion over whether to charge fees.[115] Data subjects have the right to request corrections or supplementation.[116]

5.3. Blocking

Article 11 requires data users to cease the processing or use of personal data in a number of circumstances: (a) where the accuracy of data is disputed, unless the processing or use is necessary for duties or business and the dispute is specifically noted; (b) wherever there is collection, processing or use in violation of the PIPA; and (c) where the purpose of collection has ceased to apply. These are positive obligations of data users, and may also be requested by data subjects. Data subjects do not, however, have the right to require cessation of processing of their data at any other times. **(p.183)**

6. Enforcement and remedies in Taiwan

The PIPA, like its predecessor CPPDPA, does not create a separate data protection authority (DPA). Whether the MOJ will play a central coordinating role remains to be seen. Potentially of greatest importance under the PIPA are the extensive provisions in

Chapter IV for damages actions, and for 'class action' collective litigation. However, in the first year of the PIPA's operation, it is disputes between individuals, not between individuals and businesses, that have resulted in litigation.

6.1. Ministerial enforcement—compliance orders and fines

The PIPA still has no single oversight body. The wording of the Act suggests that the MOJ is the agency responsible for coordinating its enforcement, but does not make its role completely clear. The MOJ is mentioned in three provisions. It is the sole competent authority for drafting the Enforcement Rules.[117] The MOJ sets the rules under article 6 concerning sensitive information in conjunction with the government authority in charge of each main relevant industry.[118] The specific purpose and the classification of personal information stipulated in the PIPA is to be prescribed by the MOJ in conjunction with the government authority in charge of a particular industry.[119]

Ministries can order private sector agencies to take corrective measure within a specified time, and can subject them (as an alternative to criminal prosecutions) to an administrative fine by the central competent authority for a particular industry. For breaches of more important provisions, fines can be between NT$50,000 and NT$500,000 (about US$3,000 to US$15,000), and for other provisions between NT$20,000 and NT$200,000 (US$1,200 to US$12,000).[120] Where such an administrative fine is imposed on an organization, someone who represents the organization is also to be fined a similar amount unless they can prove they fulfilled their duty to prevent such a breach.[121]

There are no obvious transparency mechanisms to reveal how the PIPA will operate: no obligations to report complaints and their resolution, nor to deliver annual reports and so on. Without them, the Taiwanese data protection legislative regime could be as opaque as the Japanese system. Chen considers that it is possible that administrative enforcement under the PIPA will become more systematic and that the MOJ will provide statistics regularly, as Taiwanese government agencies do for their core competencies.[122] She notes that it has not done so in the Act's first year of operation, even to the extent of gathering statistics on enforcement activities.[123]

Appeals against ministerial or local government orders

Business data controllers and data subjects have a right of appeal against ministry or local government authority orders, if the orders directly affect them. An administrative fine under article 48 would be an example of an order that 'directly affects' the business or individual data subject. An appeal is first filed with the ministry (or other public body) and considered by legally trained staff. If it is rejected, the business or individual gains standing to file an **(p.184)** action against the 'administrative disposition', in Taiwan's administrative courts.[124] Private parties often prevail in such actions, as Google did in a 2013 consumer law dispute.[125]

Administrative enforcement of the PIPA in its first year

The PIPA is enforced by three different type of authorities:[126] (i) central government

authorities (i.e. the MOJ); (ii) authorities dealing with specific industries (for instance the Financial Supervision Commission dealing with the banking industry); and (iii) local government bodies having authority over a particular subject matter (such as local tax authorities or the customs authority).[127] Also, because of the general character of the PIPA, both industry-specific authorities and local government bodies had issued over 40 guidelines by December 2013 as to how the PIPA will be enforced in their particular domain.[128] In this respect, the approach is rather similar to that taken in Japan up to 2014 (but which may now be changing). Also, as Chen observes, while the private sector is supervised by public agencies responsible for various sectors, no single ministry or other organization (such as a DPA) is responsible for supervising how governmental agencies observe the PIPA.[129] In this sense also, the Taiwanese system is no more developed than that of Japan.

The MOJ has had a very limited role in these activities, but has published a number of other guidance documents. These include forms for relevant authorities to report activities related to the PIPA to the MOJ;[130] however, no details of any responses were published on the MOJ website in 2013.[131] The MOJ has published an online 'handbook' compiling all the existing sources of law in relation with the PIPA,[132] which is intended to be updated. The MOJ has also published a report listing all its databases containing personal information, perhaps to encourage other authorities to imitate it. In summary, the first year of the PIPA's operation gives relatively little indication that the MOJ will take a significant coordinating role in making the PIPA's operation more transparent than the previous Act, or more consistently applied.

There are also concerns that the PIPA is being used by the government 'to backtrack on recent moves toward greater transparency', as Chen puts it:[133]

> One of the recurring criticisms of the PIPA is that it has become, in practice, a convenient excuse for the executive branch to refuse to provide citizens with previously public information on grounds that it is personal information. For example, Judicial Yuan has issued regulations prohibiting recording the statements of any person who appears in court without their written **(p.185)** permission.[134] Another example was the Control Yuan's decision to remove historical financial information reported by politicians under Taiwan's sunshine laws from its website.[135]

Lack of administrative enforcement under the CPPDPA

There were no significant examples of administrative enforcement actions by the responsible ministries in the nearly 20 years that the CPPDPA was in force. Enforcement of the CPPDPA was haphazard and intermittent at best. The main reason was that no single agency had the responsibility of enforcing it. Instead, the authority to sanction was fragmented among the various government agencies which supervised the limited number of industries or sectors to which the CPPDPA applied. The Ministry of Communications was responsible for sanctioning telecommunications enterprises that violated the CPPDPA, the Department of Health was responsible for hospitals, the

Financial Supervisory Commission (FSC) was responsible for financial services, and so on. None of these agencies saw the policing of compliance with data protection laws as a core role. It is still an open question whether anything has changed in this respect under the PIPA.

6.2. Individual remedies available from the courts

For claims against any type of agency, injuries other than to property, including to reputation, may be claimed. If claimants cannot prove actual damage, they may ask the court to assess damages between NT$500 and NT$20,000 (US$17 to US$670). Where multiple persons are injured from the same event (such as a mass data spill) the aggregate damages are capped at NT$200 million (about US$6.7 million) unless it is proven that the infringer's profits exceeded NT$200 million in which case the higher amount of the profit can be recovered.[136] There is a limitation period for commencement of actions of two years from when both damage and defendant are known, or five years from when the damage occurs.[137] Claims are also governed by the State Compensation Act 1980 (against public agencies) and the Civil Code against private sector agencies. There are complex provisions concerning which district court has jurisdiction.[138]

Onus of proof

Public agencies have strict liability for 'injuring the rights of a subject' through breaches of the PIPA, with exceptions for damage due to 'natural disaster, accident, or other force majeure'.[139] Private sector agencies, in contrast, are liable unless they can prove that they did not breach the provisions of the PIPA 'wilfully or negligently'.[140]

Civil cases in the PIPA's first year

Since the PIPA came into force there have been major data breaches by organizations such as Far Eastern International Bank and Nokia Taiwan, but no authorities have taken any public action, and no individual consumers have started actions against these companies.[141]

(p.186) However, in its first year of operation, because the PIPA allows individuals to take court action directly (without waiting for action by ministers or a DPA), there have already been a number of matters decided involving disputes between individuals. The previous CPPDPA only regulated the so-called 'eight major industries', but the PIPA also regulates the actions of individuals when they are not within the exception for personal and family affairs. the PIPA also gives individuals standing to take direct court action.

In one of a number of cases arising from disputes involving housing complexes, the chairman of the management committee of a housing complex posted documents from courts relevant to a lawsuit against previous officeholders in the complex, containing personal information such as their birth dates, national ID numbers, and addresses. The defendant alleged that this was done to inform the local community of the circumstances of the case because residents had expressed great concern. The court found that in the absence of consent from the plaintiff, the defendant's actions constituted infringement of the PIPA, and that even though there was no malicious intent, the civil law principle that

one must be held liable for one's actions applied and the defendant was ordered to pay 5,000 NTD (US$170) to each of the plaintiffs for mental suffering (in contrast to their much larger claims for damages of over 120,000 NTD (US$4,080)).[142]

6.3. Collective rights of civil action before the courts

The provisions for class action litigation by representative bodies[143] require that 'the rights of multiple subjects are injured by the same causal facts'. Such representative bodies may be incorporated foundations or incorporated public interest associations[144] and can commence an action once they have received written consent from at least 20 injured subjects. There are procedures for such actions to be publicized and other potential claimants invited to join the action. There are similar foundations for consumer protection and the protection of securities investors, usually government funded and controlled. The representative bodies have to comply with strict requirements: (i) a foundation with assets of NT$10 million (US$340,000) or an association with at least 100 members; (ii) articles including protection of personal data; and (iii) incorporation for at least three years. The representative body must disburse damages received to those who authorized it to litigate, after deduction of litigation expenses (but with no remuneration), and must act through a lawyer.[145]

According to Chen,[146] no qualified association has been incorporated, nor have preparatory steps been taken to do so. Once a qualified association has been established, it must operate for at least three years before it has standing to bring a class action on behalf of a group of plaintiffs. If an established body such as a consumer organization considers taking an action under this section, the question would arise of whether data protection was part of the organization's core mission, and if that were not so, their standing would be likely to be challenged. Therefore, even if there were a group of individuals willing to bring such a suit today, it may not be possible for them to receive support from any existing association. It is unknown how long it will take for individuals to be able to receive support in personal data cases for collective actions.

(p.187) 6.4. Criminal offences

Chapter V of the PIPA has extensive provisions for court prosecutions of offences and 'administrative fines' against private sector agencies, which can be imposed by the central competent authority for a particular industry. Breaches which cause damage to another person, can be punished by imprisonment up to two years or fines of NT$200,000 (about US$6,700), and where there is intent to profit, this can increase to five years or NT$1 million (US$33,820).[147] This also applies to unlawful impairment of accuracy of a personal data file, with intent to gain a benefit.[148] These offences can be committed by a ROC national from outside Taiwan,[149] but otherwise crimes must occur within Taiwan. Where committed by a civil servant, the penalties are increased by 50 per cent.[150] The Executive Yuan's Bill decriminalizing violations of the PIPA not committed for profit has not been passed, and (as shown in the next section) prosecutions are occurring in such situations.

Criminal cases in the PIPA's first year

The following are some typical examples of criminal cases decided in 2013.[151]

A bank employee used the bank's system to access information regarding the bank accounts of her former boyfriend. The district prosecutor had charged the bank employee of violation of the PIPA articles 41(1) and 20(1), but the court dismissed the matter, in accordance with article 45, because the former boyfriend had not lodged a complaint.[152]

An individual was convicted after disclosing private information about the complainant through faxes sent in the course of a dispute about a water leak. The defendant was convicted under article 41(1) of the PIPA for using personal information outside the scope of the purpose of collection and under article 310(2) of the Criminal Code for slander, and sentenced to two months' detention convertible to a fine.[153]

The complainant and a married couple had a dispute arising out of interference in family relations, adultery, and an abortion. The defendant wife posted disparaging messages under an alias on the Internet (both on Facebook and on Wretch, a now-defunct Taiwanese blogging platform), disclosing the alleged adultery and abortion, and other personal information of the complainant. The court found that the Facebook and Wretch websites were public Internet platforms, and so this was not exempt use of personal information because it was not for 'purely personal or family activity purposes'.[154] The disclosure contravened articles 19 and 41 of the PIPA (protection of personal data and divulgation of private information respectively). Her publications also constituted aggravated slander under article 310(2) of the Criminal Code. The Court did not enter a final judgment because defendant and complainant reached an out-of-court settlement.[155]

In another case taking the same approach, but resulting in a conviction, a defendant who had disclosed the complainant's name and pictures of his residence on Facebook, (plus defamatory statements) was sentenced to 40 days' detention or 1,000 NTD per detention day (US$34). The court relied on article 41(1) of the PIPA, which sanctions **(p.188)** non-governmental agencies for using personal information outside the scope of the specific purpose of collection.[156]

Enforcement of the CPPDPA by the courts (civil and criminal) 2001–2011

Despite the lack of ministerial enforcement, there was some enforcement of the CPPDPA via the courts. Over the 10 years 2001–11, Taiwan's high courts decided about 30–40 civil claims for damages under the CPPDPA. Only three were successful. The largest award of damages was NT$80,000 (about US$2,700), with awards of NT$20,000 to NT$50,000 (US$1,200 to US$3,000) in the other two cases. In the first case, an insurance company's employee sent one customer A's personal information to customer B. In the other two cases, the company failed to implement measures to protect data or implemented inadequate measures, this caused it to disclose customer data wrongfully (i.e. without consent). In the third case, the bank's failure to adequately protect customer data allowed a third party to find the customer data with an Internet search.

During that 10-year period about 100 criminal cases under the CPPDPA reached the high courts with convictions in about 60 per cent of cases. In many of the cases, the violation of the CPPDPA is a lesser included offence and the sentence imposed is for the greater offence under other legislation (criminal breach of trust, fraud, etc.). The most common violation was for failure to apply for a licence and thereby unlawfully collecting and selling personal data for profit.[157]

Connolly gives examples of judicial protection of privacy interests in Taiwan, though not necessarily stemming from the data protection legislation, which resulted in very strong penalties.[158] In the *Citibank Case*[159] negligent security affecting credit card records resulted in Citibank being 'prohibited from issuing any new credit cards for a month and ordered to unplug all of its online banking services for at least three months to allow the ministry to inspect security before reinstating the services'. In the *Yu Li International Marketing Corporation Case*[160] a criminal prosecution for large-scale illegal sale of personal information resulted in prosecution of 32 civil servants and civilians, and compensation ranging up to US$3,000 per customer (based on the amounts set out in the CPPDPA), available to all telecommunications customers whose information had been sold.

6.5. Strong pre-PIPA enforcement by financial regulator

Before the PIPA came into effect, and separate from the data protection law, there were important administrative enforcement actions on privacy-related grounds by Taiwan's financial services super-regulator, the FSC,[161] which imposed very substantial fines (by Taiwan's frugal standards) in 2009 and 2010 against banks, and on two insurance brokers **(p.189)** and one life insurance company in 2012. The penalties were not based on the CPPDPA, but on the FSC's regulations requiring internal controls at financial institutions. The banks were fined NT$4,000,000 (US$130,000) for failing to implement required data security measures resulting in disclosures of personal information about bank customers.[162] In contrast, the FSC normally fined banks from NT$20,000 to NT$100,000 (US$666–US$3,300) for violations of the CPPDPA, in its role as the government authority for that sector. The insurance brokers were fined NT$600,000 (US$20,000) each because they had illegally released personal information about policy holders to a life insurance company to help the life insurer market its policies. The life insurance company was also fined NT$100,000 (US$3,300) for violating the CPPDPA. The maximum fines under FSC's own rules are much higher than those which were available under the CPPDPA.

6.6. Systemic enforcement measures under the PIPA

Other than the issuing of guidelines by ministries, the PIPA does not address issues of systemic enforcement, through measures such as requiring Privacy Impact Assessments, registration of categories of data systems more likely to be dangerous, or inspections. Its enforcement measures are purely reactive.

7. Co-regulation and self-regulation in Taiwan

Business organizations are now starting to become active in promoting a 'privacy mark'.

Other aspects of self-regulation do not seem significant in Taiwan, and there is no provision in the PIPA for the development of co-regulatory codes (as distinct from ministry guidelines).

7.1. Taiwan's Data Privacy Protection Mark

Taiwan has a trustmark system,[163] the Data Privacy Protection Mark (DP Mark), which was launched in 2012. To develop a set of best practices for industry, the Department of Commerce under the Ministry of Economic Affairs, the agency responsible for electronic commerce, commissioned the Science and Technology Law Institute, part of the government-sponsored Institute for Information Industry to develop the 'Taiwan Personal Information Protection and Administration System' (TPIPAS). Private organizations that meet the TPIPAS standards are able to use the DP Mark. The TPIPAS Rules were made on 4 September 2012 and are now formally enforceable.[164] The system is, in effect, one of co-regulation. Since 2012, seven significant consumer-oriented companies[165] and one major financial organization have received the DP Mark certification. To use the DP Mark, a company must submit to a period of guidance by a 'Guidance Institution'. **(p.190)** After completing the period of guidance, the candidate company is evaluated by a 'Certification Institution' and the mark is finally issued by an 'Accreditation Institution'. The Institute also serves as the 'Certification Institution' for these initial participants and the Ministry of Economic Affairs is the 'Accreditation Institution'. There are training courses for the personnel of the companies wishing to receive DP Mark certification.[166] It is too early to evaluate the DP Mark.

8. Taiwan—More obligations, questionable enforcement

The PIPA has considerably expanded the obligations formerly imposed by the now repealed CPPDPA, and its privacy principles do generally meet international standards. New obligations include those in relation to notice, and to sensitive data. The data breach notification requirements require companies subject to the Taiwanese law to adjust to an obligation of uncertain scope. Increased penalties and exposure to actions for damages also add considerable risk to the implications of these expanded principles. Overseas companies involved in any sector of the Taiwanese economy have to pay more attention to data protection issues, due to the much broader scope of the legislation in the private sector. The extraterritorial scope of the PIPA, and its potential application to data exports, are also significant.

While the PIPA is without question a considerable improvement on the CPPDPA, it is still an open question whether the enforcement of the PIPA (including its transparency of operation) will be a significant improvement on CPPDPA. The ministry-based model of administering and enforcing data privacy laws, in contrast to the use of a dedicated DPA is now in decline in Asia (see Chapter 17), even in Japan. Whether Taiwan can demonstrate that it can work remains to be seen, but there is limited indication of strong enforcement as yet. There seems little evidence of enforcement against companies or agencies, with both civil and criminal actions being mainly about disputes between private parties.

The lack of government activity in privacy enforcement, continued under the PIPA, contrasts with Taiwan's strong constitutional protections for privacy, and the actions of the courts to uphold and expand them.

Notes:

([1]) For APEC, WTO, and some other purposes, it is known as 'Chinese Taipei'. Historically and geographically it has been known as Ilha Formosa ('beautiful island').

([2]) A very readable history of Taiwan is Jonathan Manthorpe, *Forbidden Nation: A History of Taiwan* (Palgrave Macmillan 2009).

([3]) Francis Pike, *Empires at War: A Short History of Modern Asia Since World War II* (I B Tauris 2011), p. 277.

([4]) Pike, *Empires at War*, p. 126.

([5]) T-S. Wang, ch. 4 'Taiwan' in Poh-Ling Tan (Ed.), *Asian Legal Systems: Law, Society and Pluralism in East Asia* (Butterworths, 1997).

([6]) Pike, *Empires at War*, p. 689.

([7]) Pike, *Empires at War*, p. 280.

([8]) Pike, *Empires at War*, p. 690.

([9]) Wang, ch. 4 in Tan (Ed.), *Asian Legal Systems*, p. 133.

([10]) Wang, ch. 4 in Tan (Ed.), *Asian Legal Systems*, p. 133.

([11]) C. Lo, ch. 3 'Taiwan—External Influences Mixed with Traditional Elements to Form Its Unique Legal System' in E. Ann Black and Gary F. Bell (Eds.), *Law and Legal Institutions in Asia: Traditions, Adaptations and Innovations* (Cambridge University Press, 2011), p. 94.

([12]) Wang, ch. 4 in Tan (Ed.), *Asian Legal Systems*, p. 139.

([13]) See Wang, ch. 4 in Tan (Ed.), *Asian Legal Systems*, pp. 136–8 for a summary.

([14]) A separately elected National Assembly had deliberative and other powers, but not legislative or veto powers, and has in effect been abolished since 2005: For details, see Lo, ch. 3 in Black and Bell (Eds.), *Law and Legal Institutions in Asia*, p. 102.

([15]) Lo, ch. 3 in Black and Bell (Eds.), *Law and Legal Institutions in Asia*, p. 99.

([16]) As the Constitutional Court, it also decides on the constitutional validity of political parties.

([17]) Lo, ch. 3 in Black and Bell (Eds.), *Law and Legal Institutions in Asia*, p. 103.

([18]) Electronic Privacy Information Center and Privacy International, 'Republic of China (Taiwan)' in *Privacy & Human Rights 2006* (EPIC and PI, 2006) <http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Republic-29.html#Heading12110>, p. 945.

([19]) EPIC and PI, 'Republic of China (Taiwan)' in *Privacy & Human Rights 2006*, footnote references omitted.

([20]) Council of Grand Justices, *Are the relevant provisions of Article 8-II and III of the Household Registration Act, stating to the effect that the new ROC identity card will not be issued without the applicant being fingerprinted, unconstitutional?*, JY Interpretation NO-603 [2005] TWCC 16 <http://www.asianlii.org/tw/cases/TWCC/2005/16.html> (hereinafter the 'Fingerprinting Decision').

([21]) The Council of Grand Justices noted that Taiwan ID cards were required for purposes such as to vote in elections or referenda; to receive a passport; for labourers to apply for the payment of retirement pension; to be admitted to some state-administered examinations; and to apply for a professional licence for business passenger vehicles. They said that, more often than not, a person may be requested to produce his Taiwan identity card as proof of his identity in ordinary private activities like opening of a bank account, or a company's hiring of an employee.

([22]) EPIC and PI, 'Republic of China (Taiwan)' in *Privacy & Human Rights 2006*, p. 946, footnote references omitted.

([23]) Certificate Authority of MOI, 'Events' (MOICA, 2014) <http://moica.nat.gov.tw/en/history_1.html>.

([24]) C.C. Lai and E.L. Chiu (transl. J. Clegg), 'Limiting the Misuse of Credit Data' (TAHR, 16 May 2011) <http://%20www.tahr.org.tw/node/734>.

([25]) Lai and Chiu, 'Limiting the Misuse of Credit Data'.

([26]) Wang, ch. 4 in Tan (Ed.), *Asian Legal Systems*, p. 150.

([27]) Lo, ch. 3 in Black and Bell (Eds.), *Law and Legal Institutions in Asia*, pp. 114–15.

([28]) Taiwan Association for Human Rights (TAHR) website <http://www.tahr.org.tw/>.

([29]) 'MOFA's Fingerprinting Plan is Anti-Human Rights' <www.tahr.org.tw/taxonomy/term/47>.

([30]) Lai and Chiu, 'Limiting the Misuse of Credit Data'.

([31]) EPIC and PI, 'Republic of China (Taiwan)' in *Privacy & Human Rights 2006.*

([32]) 'Taiwan: Initial State Report on ICCPR & ICESCR' (International Federation for Human Rights (FIDH), 20 April 2012) <http://www.fidh.org/Taiwan-Initial-State-Report-

on>.

([33]) Wang, ch. 4 in Tan (Ed.), *Asian Legal Systems*, p. 145.

([34]) Lo, ch. 3 in Black and Bell (Eds.), *Law and Legal Institutions in Asia*, p. 98; Lo notes some exceptions (not relevant here) concerning double taxation, extradition, and like matters intended to be directly applied.

([35]) EPIC and PI, 'Republic of China (Taiwan)' in *Privacy & Human Rights 2006*, p. 1042; S. Peng, 'Privacy and the Construction of Legal Meaning in Taiwan' (2003) 37(4) *The International Lawyer*.

([36]) Peng, 'Privacy and the Construction of Legal Meaning in Taiwan', p. 1042.

([37]) JY Interpretation NO-509, [2000] TWCC 11 (concerning criminalization of defamation) JY Interpretation NO-535, [2001] TWCC 16 (concerning 'police checks').

([38]) Council of Grand Justices, *Has the Legislative Yuan, by enacting the Act of the Special Commission on the Investigation of the Truth in Respect of the 319 Shooting, gone beyond the scope of its legislative authorities? Are any of the relevant provisions contained therein unconstitutional?*, JY Interpretation NO-585 [2004] TWCC 15 (15 December 2004) <http://www.asianlii.org/tw/cases/TWCC/2004/15.html> (hereinafter the '319 Shooting decision').

([39]) The '319 Shooting decision' refers to the attempted assassination of Taiwan's President and Vice President on the eve of the 2004 elections; for details see Manthorpe, *Forbidden Nation*, chs. 1 and 20.

([40]) Council of Grand Justices, 'Fingerprinting decision': 'Are the relevant provisions of Article 8-II and III of the Household Registration Act, stating to the effect that the new ROC identity card will not be issued without the applicant being fingerprinted, unconstitutional?' J.Y. Interpretation NO-603 [2005] TWCC 16 (28 September 2005) <http://www.asianlii.org/tw/cases/TWCC/2005/16.html>.

([41]) R. Chang, 'Grand Justices Throw Out Fingerprinting' (*Taipei Times*, 29 September 2005) <http://www.taipeitimes.com/News/front/archives/2005/09/29/2003273639>.

([42]) Council of Grand Justices, *Is Article 5-II of the Communication Protection and Monitoring Law, promulgated and implemented on July 14, 1999, unconstitutional?*, J.Y. Interpretation NO-631 (20 July 2007) <http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=631>.

([43]) Council of Grand Justices, *Does Article 89, Paragraph 2 of the Social Order Maintenance Act restricting the act of stalking by a journalist violate the Constitution?*, J.Y. Interpretation NO-689 (29 July 2011) <http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=689>.

([44]) See Peng, 'Privacy and the Construction of Legal Meaning in Taiwan'.

([45]) *Civil Code* <http://law.moj.gov.tw/eng/LawClass/LawAll.aspx?PCode=B0000001>.

([46]) Information provided by Chui-Ling Chen of Winkler Partners (email, 28 March 2013).

([47]) There are many lower court cases concerning art. 195, but almost all concern the non-privacy issues it also covers.

([48]) Lai and Chiu, 'Limiting the Misuse of Credit Data'.

([49]) Peng, 'Privacy and the Construction of Legal Meaning in Taiwan'.

([50]) D. Tang, 'Taiwan Proposes Amendments to its 1995 Data Protection Act', *Privacy Laws and Business International Newsletter* (February 2009) pp. 19–20; Peng, 'Privacy and the Construction of Legal Meaning in Taiwan'.

([51]) T-R. Chuang, 'Personal Data Protection in Taiwan: Whose Business?' (2003) 2(1) *National Policy Quarterly* 53 (in Chinese with English abstract) <www.iis.sinica.edu.tw/~trc/public/publications/npq03/>.

([52]) Tang, 'Taiwan Proposes Amendments to its 1995 Data Protection Act'; Peng, 'Privacy and the Construction of Legal Meaning in Taiwan'.

([53]) Tang, 'Taiwan Proposes Amendments to its 1995 Data Protection Act'.

([54]) Tang, 'Taiwan Proposes Amendments to its 1995 Data Protection Act'; Hui-Ling Chen, 'Enforcement of Taiwan's Data Privacy Law: Rules Proposed' (2011) 114 *Privacy Laws and Business International Report* (December 2011), pp. 24–6 (hereinafter Chen 'Enforcement Rules').

([55]) Tang, 'Taiwan Proposes Amendments to its 1995 Data Protection Act'.

([56]) Tang, 'Taiwan Proposes Amendments to its 1995 Data Protection Act'.

([57]) Enforcement Rules of the Personal Information Protection Act (2012) (amended), Ministry of Justice (26 September 2012) (in English) <http://law.moj.gov.tw/eng/LawClass/LawAll.aspx?PCode=I0050022>; see Chen, 'Enforcement Rules' for commentary on the draft Rules.

([58]) PIPA (Taiwan), art. 6(d–f).

([59]) PIPA (Taiwan), art. 41. See Winkler Partners, 'Amendments to Long-Delayed Data Protection Law Proposed' (17 April 2012) <www.winklerpartners.com/?p=3099>.

([60]) Email communication from Hui-ling Chen, 20 December 2013.

([61]) Hui-Ling Chen, 'Taiwan's PIPA into Force, with Controversial Sections Removed'

(2011) 121 *Privacy Laws and Business International Report*, p. 28.

([62]) Chen, 'Taiwan's PIPA into Force'.

([63]) 'Revision of PIPA Under the Spotlight: Three Controversial Articles of the Law Still Waiting to be Examined by the Legislative Yuan' (IT Home Online, in Chinese, 2013) <http://www.ithome.com.tw/privacylaw/article/82788>.

([64]) Information provided by Hui-ling Chen, Winkler Partners (email, 20 December 2013).

([65]) Winkler Partners, 'Taiwan Ministry of Justice Considers Right to be Forgotten and of Erasure' (23 August 2012) <http://www.winklerpartners.com/?p=3415>.

([66]) PIPA (Taiwan), art. 51.1.

([67]) PIPA (Taiwan), art. 51.2.

([68]) PIPA (Taiwan), art. 2.

([69]) The draft Rules also stated in art. 3 that 'the same does not apply if it is difficult to inquire, or it takes enormous expense or time to identify the person through the information', but this was deleted in the final version; see Chen, 'Enforcement Rules'.

([70]) PIPA Rules, art. 5. The draft Rule 5 also included 'log files' derivative information that is generated during the collection, processing, or use of personal information that does not belong to the data subject whose personal information is collected, including but not limited to name of user accessing files, access time, code of device used, Internet Protocol (IP) address, visited URLs, etc., that can be used to compare and to validate the authority used to access files. However, according to a Ministry of Justice explanation, this was removed on the basis that the information concerned was already covered by the definition of 'personal information' and this provision was redundant. See Chen, 'Enforcement Rules' for details of the draft provision.

([71]) PIPA (Taiwan), arts. 3, 4, 5, 6, 11, 21, and 51.

([72]) PIPA (Taiwan), arts. 15 and 20.

([73]) PIPA Rules, art. 14.

([74]) Electronic Signatures Act 2011, art. 4 (Ministry of Justice, Taiwan) <http://law.moj.gov.tw/Eng/news/news_detail.aspx?id=944>.

([75]) See Chen, 'Enforcement Rules'.

([76]) PIPA Rules, art. 15.

([77]) Chen, 'Enforcement Rules'.

([78]) Chen, 'Enforcement Rules'.

([79]) PIPA (Taiwan), art. 4. Another translation referred to their being 'as one and the same as the commissioning agency'.

([80]) PIPA Rules, art. 8.

([81]) The following list paraphrases Chen, 'Enforcement Rules': the extent, type, and purpose of the intended collection, processing, or use of personal information, and the duration; the necessary measures to be taken by the commissioned entity to adequately maintain security (or 'safety maintenance'), as specified in art. 12 of the Enforcement Rules; if there is subcontracting, ensuring that the agreed subcontractor is used; upon violations by the commissioned entity or its employees of legal or regulatory provisions to protect personal information or of the terms of the commission agreement, the matters to be notified to the commissioning agency and the remedial measures to be taken; the extent of the commissioning agency's authority to issue instructions to the commissioned entity 'reservation instructions'; the return of personal information storage media and the erasure of personal information recorded and held by the commissioned entity after the termination or rescission of the commission relationship.

([82]) Chen, 'Enforcement Rules'.

([83]) This paragraphs paraphrases Chen, 'Enforcement Rules'.

([84]) PIPA (Taiwan), arts. 15 and 16.

([85]) PIPA (Taiwan), art. 15.

([86]) PIPA (Taiwan), art. 19.

([87]) PIPA (Taiwan), art. 16.

([88]) PIPA (Taiwan), art. 17.

([89]) PIPA (Taiwan), art. 20.

([90]) PIPA (Taiwan), art. 19.

([91]) PIPA (Taiwan), art. 11.

([92]) PIPA (Taiwan), art. 18.

([93]) PIPA (Taiwan), art. 27.

([94]) PIPA Rules, art. 12.

([95]) PIPA (Taiwan), art. 12.

([96]) PIPA Rules, art. 22. This paragraph paraphrases Chen, 'Enforcement Rules', with permission.

([97]) PIPA (Taiwan), art. 5(5).

([98]) PIPA Rules, art. 6.

([99]) PIPA (Taiwan), art. 11.

([100]) PIPA Rules, art. 4.

([101]) Chen, 'Enforcement Rules'.

([102]) The first proposed exception would permit collection of sensitive information 'with consent of the subject' (so that consent will authorize collection of any personal information, even if sensitive), and the second would also permit collection which is 'necessary to serve and protect public interests': Chen, 'PIPA in Force'.

([103]) Collection necessary to prevent harm to the life, person, liberty, or property of the subject or other persons; collection necessary to conduct civil litigation or other civil proceedings, criminal proceedings, or remedial procedures for administrative disputes related to the subjects; collection for purposes of public health, crime prevention, or scientific knowledge; and as otherwise expressly required by law: Chen, 'PIPA in Force'.

([104]) PIPA (Taiwan), art. 51.

([105]) PIPA (Taiwan), art. 21.

([106]) PIPA (Taiwan), art. 2.6.

([107]) PIPA (Taiwan), art. 3.

([108]) PIPA (Taiwan), art. 8.

([109]) PIPA (Taiwan), art. 8-II.

([110]) PIPA (Taiwan), art. 9.

([111]) Chen, 'PIPA in Force'.

([112]) PIPA Rules, art. 16.

([113]) Chen, 'PIPA in Force'.

([114]) PIPA (Taiwan), art. 10.

([115]) PIPA (Taiwan), art. 14.

([116]) PIPA (Taiwan), art.14

([117]) PIPA (Taiwan), art. 55.

([118]) PIPA (Taiwan), art. 6(2).

([119]) PIPA (Taiwan), art. 53.

([120]) PIPA (Taiwan), arts. 47–49.

([121]) PIPA (Taiwan), art. 50.

([122]) Chen, 'Enforcement Rules'.

([123]) Email communication from Hui-ling Chen to the author, 20 December 2013.

([124]) Administrative Appeal Act (Taiwan), art. 1 and art. 92 (definition of 'administrative disposition').

([125]) In the Taipei High Administrative Court, Google succeeded against the Taipei City government which had fined it for allegedly violating Taiwan consumer protection laws by not providing a seven-day return period for apps sold on its online store: Jamie Yap, 'Google Wins Lawsuit Against Taipei Government' (ZNet, 28 December 2012) <http://www.zdnet.com/google-wins-lawsuit-against-taipei-government-7000009212/>.

([126]) Most of this part is based on Graham Greenleaf and Hui-Ling Chen, 'Data Privacy Enforcement in Taiwan, Macau, and China' (2012) 117 *Privacy Laws & Business International Report*, pp. 11–13.

([127]) All of this section paraphrases information provided by email from Hui-ling Chen to the author, 20 December 2013.

([128]) For example, the Financial Supervision Commission Guidelines relating to the protection of personal information management, issued 22 August 2013.

([129]) Hui-ling Chen, 'Taiwan's PIPA: One Year On' (2014) 128 *Privacy Laws & Business International Report*.

([130]) See for instance information with respect to reporting by relevant authorities of statistics of enforcement (MOJ, October 2013) <http://www.moj.gov.tw/public/Attachment/37811193966.xlsx>.

([131]) See MOJ website <http://www.moj.gov.tw/ct.asp?xItem=311820&ctNode=28156&mp=001>.

([132]) See MOJ Handbook, *Legal rules and other relevant texts pertaining to the protection of personal information* (MOJ, August 2013) on <https://www.moj.gov.tw/public/Attachment/31011536015.pdf>.

([133]) Chen, 'Taiwan's PIPA: One Year On'.

([134]) Regulations Governing Court Room Recording, Use, and Preservation (Judicial Yuan, 25 October 2013).

([135]) See Liberty Times, 1 September 2013 <http://www.libertytimes.com.tw/2013/new/sep/1/today-p5.htm>.

([136]) PIPA (Taiwan), art. 28.

([137]) PIPA (Taiwan), art. 30.

([138]) PIPA (Taiwan), art. 33.

([139]) PIPA (Taiwan), art. 28.

([140]) PIPA (Taiwan), art. 29.

([141]) This and the following paragraphs paraphrase with permission Chen, 'Taiwan's PIPA: One Year On'.

([142]) (102) *Fengjian Zi* No. 164.

([143]) PIPA (Taiwan), arts. 32 and 34–40.

([144]) As defined in art. 32.

([145]) PIPA (Taiwan), arts. 39 and 40, respectively.

([146]) Chen, 'Taiwan's PIPA: One Year On'.

([147]) PIPA (Taiwan), art. 41.

([148]) PIPA (Taiwan), art. 42.

([149]) PIPA (Taiwan), art. 43.

([150]) PIPA (Taiwan), art. 44.

([151]) These cases are summarized, with permission, from Chen, 'Taiwan's PIPA: One Year On'.

([152]) (102) *Yi Zi* No. 1343 criminal judgement (Taoyuan District Court).

([153]) (102) *Shenjian* Zi No. 1059 (Taipei District Court).

([154]) PIPA (Taiwan), art. 51(1).

([155]) (102) *Yi Zi* No. 317 (Taiching District Court).

([156]) (102) *Jian Zi* No. 1199 (Tainan District Court).

([157]) CPPDA (Taiwan), art. 19.

([158]) Chris Connolly et al, 'Privacy breach sanctions in the Asia-Pacific region' (Galexia, July 2007) <http://www.galexia.com/public/research/articles/research_articles-art45.html>.

([159]) Connolly, 'Privacy breach sanctions in the Asia-Pacific region', cites B. Wright, 'The Costs of Not Securing Personally Identifiable Data' (2004) 4 *Information Systems Control Journal* <http://www.theprosandthecons.com/articles/isaca2004.pdf> and J. Huang, 'Ministry Punishes Bank for Online Security Leaks' (*Taipei Times*, Taipei, 26 November 2003) no longer available online.

([160]) Connolly et al., cite S-F. Teng, 'Personal Data under Threat' (*Taiwan Panorama*, July 2004).

([161]) The FSC is modelled in part on the UK's Financial Services Authority, and is a very aggressive and pro-active regulator.

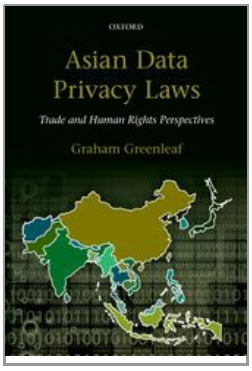
([162]) According to media reports, the 2010 case involved a hacker attack on E.Sun Bank in which a hacker was able to insert a trojan computer program to exploit a security weakness. Although no losses were reported by the bank's auditors, the hacker was able to obtain personal information regarding some 10,000 account holders. There are very few details available about the breach of security systems at Taishin Bank in 2009, but it appears to be related to disclosure of credit card transactions and card-holder personal information. Neither Taishin nor E.Sun appear to have exercised their right to file administrative and legal appeals against these fines.

([163]) This paraphrases with permission, parts of Hui-Ling Chen, 'Taiwan Launches Data Privacy Protection Mark' (2012) 115 *Privacy Laws & Business International Report*, p. 13.

([164]) TPIPAS Rules (only in Chinese) <http://www.tpipas.org.tw>; information provided by Winkler Partners, Taipei.

([165]) 7-NET; ICHIBA; books.com.tw; FamilyMart FamiPort; GOHAPPY; Sinya; and PayEasy.

([166]) See list of courses on <http://www.tpipas.org.tw/resource_doc.aspx?no=134>.



Asian Data Privacy Laws: Trade & Human Rights Perspectives
Graham Greenleaf

Print publication date: 2014
Print ISBN-13: 9780199679669
Published to Oxford Scholarship Online: December 2014
DOI: 10.1093/acprof:oso/9780199679669.001.0001

China—From Warring States to Convergence?

Graham Greenleaf

DOI:10.1093/acprof:oso/9780199679669.003.0007

[–] Abstract and Keywords

The People's Republic of China (PRC) has enacted five significant legislative instruments concerning data privacy since 2011, two of them originating at the highest level, the Standing Committee of the National People's Congress. It has only become apparent since late 2012 that China is now moving away from a patchwork 'sectoral' approach to data privacy, toward a more coherent structure, with similar principles applying across most of the private sector. Reported cases concerning enforcement are becoming more common, particularly in criminal law and tort law. Ministries involved in both telecommunications and consumer affairs have key roles. Eventually, an overall national law may emerge, probably with no single specialized administrative body in charge (no 'data protection authority'), but convergence is looking more likely. In the small field of data privacy China has made considerable advances toward the rule of law, in both the public and private sectors.

Keywords: data protection, privacy, Asia, PRC, China, Ministries, criminal law, tort

1. China—introduction and contexts

In the People's Republic of China ('PRC' or 'China'), the years 2007–2011 could be called the 'warring states' period in the development of data privacy protections. In Chinese history, the Warring States Period from the early 5th century BC ended with the unification of China by the Qin emperor in 221 BC. The modern 'states', by analogy, were the many fiefdoms in the bureaucracies of the People's Republic of China, who it appeared could not reach consensus on how data privacy should be regulated. This 'warring states' hypothesis is that the direction China will take in relation to data privacy is uncertain and contested, and likely to remain that way. It was seen as recently as 2011 as creating:[1]

> a prospect that personal information protection law may continue in a patchwork, piece-by piece form. That remains the case today [in 2011], and developments since August 2009 have in fact reinforced this pattern. Developments since August 2009 have positioned personal information protection laws in China as a consumer protection law and regulations, a tort law, a medical records regulation, a social insurance law, a credit reference regulation, and even as an anti-money laundering banking regulation. Provisions related to personal data are therefore now ever more scattered among various Chinese laws and regulations which primarily and originally were intended to address particular subject matter, and therefore only touch personal data as an aspect of addressing their original particular subject matter. As a result, there still is no clear, single definition of personal data under Chinese laws and regulations.

Taking this approach, it seemed there would be no 'Qin emperor' to unify China's privacy laws, but (rather like the USA) China would continue to have a patchwork quilt of non-comprehensive and inconsistent sectoral provisions. The alternative scenario, apparent only since late 2012, is that China is now moving away from such a patchwork approach toward a more coherent structure, with similar principles applying across at least most of the private sector. This view is supported by similarities in five legislative instruments since 2011, two of them originating at the highest level, the Standing Committee of the National People's Congress. It may still take some time for an overall national law to emerge, and still perhaps with no Qin emperor in charge, but convergence is looking more likely.

Before examining the details of that convergence, and the other aspects of China's legal protections of privacy that support it, this section provides some necessary background

on China's legal and political system, and the surveillance context in which data privacy laws operate.

(p.193) 1.1. Historical and political context

Details of China's history and political system are readily available to non-specialists,[2] and only some very basic points can be provided here. The history of the People's Republic of China begins, in many respects, with the defeat of Japan in World War II and the following victory by the Communist Party of China led by Mao Tse Tung in the civil war against the Nationalist forces led by Chiang Kai Shek, the ruling party in the previous Republic of China, and the proclamation of the People's Republic of China in 1949. Seminal events of the following decades are as noted by Wang:[3]

> Chinese society has undergone tremendous change since 1949, including the socialist transformation of the economy in the 1950s, the Cultural Revolution in the 1960s and 1970s, the Tiananmen Square event in 1989, the abandonment of the planned economy in favour of capitalism, the market economy and privatisation during the reform era of 1979 to the present, accession to the World Trade Organization (WTO) in 2001, and the Beijing Olympic Games in 2008. The only thing that has not changed is the CPC's tight control of political power. In this sense, China is a de facto single party state, although there are eight other registered political parties.

To that list of landmark events one could add the tragedy of the Great Leap Forward in the 1950s, the PRC taking China's seat in the United Nations (UN) in the 1970s, the reunification of Hong Kong and Macau with the mainland at the turn of the century, access to both the Internet and to overseas travel and education, and China becoming the world's second largest economy by the end of its first decade. The operation of democratic centralism, the instrument of 'tight control', means that China is not a democracy. The result is a non-democratic but largely politically stable, increasingly prosperous, country with a vast and rapidly expanding middle class and consumer economy. The development of this 'new' China, particularly of the last two decades, is the main reason that the content of this chapter is surprisingly complex, while the increasing reliance by China on law, and the rule of law, as the preferred means of government is the second reason.

1.2. The Chinese legal system

China's legal system is not only complex but often difficult to understand by those coming from a Western legal perspective, particularly that of the common law. The standard introduction to the PRC legal system by Chen gives a very detailed guide,[4] and less detailed introductions are also available.[5] Many sources are available on the Internet in English (usually in unofficial translations).[6]

Legislation is the primary source of law in the PRC. The hierarchy of legal norms in the PRC, according to the Legislation Law, is as follows, considerably simplified:[7]

(p.194) (i) The current Constitution of 1982 is the fundamental law of the state.

All laws should be made in accordance with it, but courts cannot declare that a law is unconstitutional.
(ii) Laws made by the National People's Congress (NPC). Only it can enact 'basic laws' and amend the Constitution.
(iii) Laws made by the Standing Committee of the NPC (SC-NPC) are also entitled to be called 'laws'. The Standing Committee is the second-highest legislative organ in China, after the full NPC, and has extensive legislative powers.[8] It makes 80 per cent of all laws. Decisions (*jueding*) by the Standing Committee are legislation.[9] It can amend laws made by the NPC.
(iv) Administrative regulations (or simply 'regulations') made by the State Council, the highest authority in the executive branch (government), are made for the purposes of administrative management or in order to implement laws.
(v) Local regulations and rules made by ministries of the State Council, or other authorized bodies (e.g. the State Bank of China) should not technically be called 'regulations', but this term is used in some cases in this chapter (e.g. 'MIIT Regulations').
(vi) Legislation made at the local level is the lowest tier, including by people's congresses, standing committees or governments, in provinces and in specially designated cities and autonomous areas.

The role of the Supreme People's Court (SPC) in the PRC, in relation to giving 'interpretations' and in the categories of decisions it makes, is unique among legal systems, but is of limited relevance to a study of data privacy laws until there is more case-law on the topic.[10] Although they are not a formal source of law in the PRC 'it seems that some judicial decisions of the Chinese courts do generate legal norms and have persuasive or even binding force in practice'.[11] Decisions of the SPC are distributed within the court system, with selected cases published in an annual Gazette and considered as authoritative and in practice binding on lower courts. Decisions of superior courts also tend to be followed by the courts immediately below them.[12] The SPC issues 'interpretations' but these are best considered as aspects of the SPC's quasi-legislative function,[13] not as the making of law via decided cases as in common law countries. Two types of 'interpretations' in the Chinese legal system may be distinguished: (1) 'legislative interpretations' promulgated by the SC-NPC, which are clarifications or supplements to laws made by the NPC or SC-NPC, and (2) 'judicial interpretations' promulgated by the SPC, where the court 'may interpret points of law arising from the concrete application of the law in the adjudicative work of the courts'.[14] The SPC can also provide 'replies' to lower courts on matters referred to the SPC for clarification. Examples of the SPC's judicial interpretations include the *Qi Yuling Case* and the SPC Provisions on government data (see sections 2.1 and 6.1 of this chapter).

(p.195) Another unique aspect of China's court system is the role of 'adjudicative committees' (the AC),[15] whereby a committee of senior judges within a court, that does not hear the argument in a case, may nevertheless make the final decision in the case, not the judges hearing it. This is more likely to occur in significant or sensitive cases. This controversial practice may or may not occur in data privacy cases before courts. It is significant to discussions concerning the extent and development of the rule of law in

China. The judicial system as a whole now has constitutional and other legal guarantees of 'judicial independence' from outside interference, but individual judges do not have judicial independence.[16]

On the question of the extent to which China is developing the rule of law (as distinct from 'rule by law') since the late 1970s, Wang takes a positive 'glass half-full' approach:[17]

> Despite all the problems in China's legal reconstruction, an optimistic view suggests that China is still steadfastly building a legal system that meets the most basic elements of the rule of law

However, he argues that, since 2007 and the Presidency of Hu Jintao there has been something of a turn away from emphasis on 'Western' concepts such as the supremacy of the rule of law and constitutionalism, and a renewed emphasis on the leading role of the Party and emphasis on 'Chinese characteristics'.[18] Other scholars see much the same.[19] Chen, while remaining optimistic about the overall trajectory of PRC legal change, cautions that 'Marxist-Leninist ideology converges with Confucianism in a sense: they share a common distrust of, or lack of respect for, the rule of law'.[20]

1.3. State surveillance in China

The political control of the Communist Party is underpinned by a complex surveillance system touching all aspects of Chinese society, of which only some basic elements can be mentioned in this section. China introduced the hukou system of household registration in 1958 and it remains a key control on population mobility despite the introduction of a number of generations of ID cards. China introduced a laminated paper ID card in 1985. Legislation for a second-generation card was enacted in 2004, including provisions aimed at preventing abuse by officials (see section 6.1 of this chapter). Its initial releases included a digitized photograph but no other biometrics, and includes data on a microchip which can be read by RFID devices.[21] China's legal system gives government agencies extensive access to personal data held by the private sector, with one recent study identifying over 20 laws authorizing access or requiring reporting.[22] As occurs elsewhere, otherwise privacy-protective legislation may include surveillance requirements, such as the 2012 Decision of the Standing Committee of the NPC on 'electronic information' (see section 3.1 of this chapter) which includs 'real name' provisions which will clearly enhance state surveillance capacities **(p.196)** by requiring that online pseudonyms may be used only if the Internet Service Provider (ISP) or content host can identify the person behind the pseudonym.[23]

2. Privacy protection in the general Chinese law

This section considers privacy protections under aspects of Chinese law of general application: constitutional and treaty protections; criminal law; and the civil law including tort law.

2.1. Constitutional protections

China's Constitution states the fundamental rights and duties of citizens, including in various articles, freedom of the person, personal dignity and freedom, and privacy of

correspondence by citizens, as well as the prohibition on unlawful search of, or intrusion into, a citizen's residence (articles 33–40).[24] However, as will be explained, the details of these rights are not of direct legal relevance to the protection of privacy, because the Constitution itself is generally regarded as non-justiciable.

It is perhaps a coincidence that the most significant case concerning the protection of constitutional rights, *Qi Yuling v Chen Xiaoqi*, is a case concerning privacy, or to be more specific, identity theft. At least for the moment, discussion of protection of privacy via constitutional rights also ends with that case. Plaintiff Qi Yuling, a 28-year-old female from Shandong Province, and the defendant, Chen Xiaoqi, graduated from high school in the same year. Qi did better in the examinations, but Chen fraudulently obtained Qi's notice of admission to a business school, and she and her father falsified identity documents so that she could pass herself off as Qi and obtain admission in Qi's place. Three years later she graduated and obtained employment. Qi found that she could not pursue an education, and commenced action. The lower Shandong courts held that Qi's rights under the General Principles of the Civil Law had been infringed (an early case on privacy protection under the General Principles), but she was dissatisfied, believing that the remedy did not adequately reflect her loss of a right to an education, and consequent losses. The Shandong Appeal Court referred the matter to the SPC.

The SPC said in its reply to the Shandong court:[25]

> After study, we hold, on the facts in this case that Chen Xiaoqi and others have violated the fundamental right to receive education enjoyed by Qi Yuling in accordance with the provisions of the Constitution by means of violating rights in a person's name. This has produced the result of actual damages. Commensurate civil liability applies.

The Constitution had not been raised in the lower courts, but the SPC had itself raised 'the right to receive education' stated in article 46 of the Constitution, and based its decision upon it. The decision had in effect suggested for the first time that rights stated in the Constitution could be justiciable and the basis of civil liability.

(p.197) However, in 2008 the SPC officially withdrew its reply to the Shandong court, stating only that it was no longer in use (or application), but without giving reasons.[26] This is taken to confirm that it is not possible for individuals to raise constitutional rights in China's courts in civil disputes. The rights stated in articles 33–40 cannot be used to vindicate privacy interests in civil actions before Chinese courts. It is also accepted in Chinese legal theory that it is not the role of courts (including the SPC) to determine whether legislation is 'unconstitutional'. Only the National People's Congress Standing Committee has this function.[27] Soon after the decision in *Qi Yuling*, it was described as 'China's *Marbury v Madison*',[28] and while it can be argued that this is a misleading analogy in many ways, the case (and the analogy) continues to be very controversial,[29] but for reasons which have only to do indirectly with the protection of data privacy.

2.2. International obligations

China still has not ratified the International Covenant on Civil and Political Rights 1966 (ICCPR) (Article 17 of which protects privacy), although it signed the ICCPR in 1998.[30] Nor is it a party to the first Optional Protocol to the ICCPR, which allows individuals to make 'communications' (complaints) to UN human rights bodies. The PRC Constitution does not state whether international law is a source of PRC law, and according to Chen '[t]here is no consensus as to the extent to which international law, and, in particular, relevant treaty provisions can be directly applicable in the PRC in the absence of implementing provisions in domestic legislation'.[31] China participated in the development of the Asia-Pacific Economic Cooperation (APEC) Privacy Framework (2003–05) through its privacy subgroup, but has not yet indicated that it will be involved in the APEC Cross-border Privacy Rules (CBPR) system.

2.3. Criminal law

China has enacted criminal provisions at the national level prohibiting the 'unlawful' disclosure or obtaining of personal information under certain circumstances.

Seventh Amendment to the Criminal Law (2009), article 253(a), etc.

The addition of article 253(a) to the Criminal Law by the Seventh Amendment, enacted by the SC-NPC in 2009, was the first occurrence of direct protection of personal information by the criminal law in China.[32] A sentence of up to three years' criminal detention, and a monetary penalty, can be applied wherever any government institution or a financial, telecommunication, transportation, education, or medical organization, or one of its **(p.198)** employees, violates state regulations by selling, or by other illegal means providing to others, personal information obtained by the employee during his or her performance of duties or provision of services. The same penalties may apply when any person (not necessarily an employee) has obtained the information by theft or other illegal means. It is necessary that the theft or access has severe consequences or the circumstances are 'severe' (which is undefined) before an offence occurs. Where an organization commits any of these offences a monetary penalty applies, and the person directly responsible and anyone else indirectly responsible are liable to be punished. The article does not define what kinds of information would be considered 'personal information'.

Article 253(a) refers to 'a state organ or an entity in such a field as finance, telecommunications, transportation, education or medical treatment', a list of industries is followed by an 'etc.' catch-all, which, in light of subsequent reported cases including, most notably, the *Roadway Case* (discussed below), suggests that article 253(a) is intended to cover all industries with access to large amounts of personal data, such as a marketing company like Roadway.[33]

Other provisions criminalize various actions in relation to computer information systems:[34] 'intrusions' into them; use of 'other technical means' to 'obtain data stored, processed or transmitted' by them; or 'exercising illegal control' over them. Penalties differ between 'serious' and 'very serious' circumstances. Anyone providing programs or tools for these purposes may be treated similarly. While these are general 'computer crime' provisions and not necessarily related to misuse of personal data, they can clearly also be used in

that context.

Illegal disclosure or sale of personal information (SC-NPC Decision 2012)

China's highest level data privacy law repeatedly singles out illegal disclosure or sale of personal information, implying that the most harsh penalties should be applied to such actions, but without in itself creating a criminal offence. The first clause of the SC-NPC Decision 2012 (see section 3.1 of this chapter) provides that '[n]o organization or individual may steal or otherwise illegally acquire a citizen's personal electronic information, or sell or unlawfully provide a citizen's personal electronic information to others'. This provision makes it clear that illegal acquisition is on the same footing as disclosure. The references to 'steal', 'illegally', and 'unlawfully' still tend toward circularity, leaving open the question of whether the boundaries of legality are the same as the purpose of collection. However, there does seem to be a more clear prohibition against selling people's 'personal electronic information'. Elsewhere in the 2012 Decision, and in the Consumer Law 2013, the controllers or processors are required not to disclose or sell or illegally provide personal information to others.

Examples of enforcement

The first prosecution under article 253(a) involved a defendant from Zhuhai who 'illegally purchased a detailed log of telephone calls made by high-ranking local government **(p.199)** officials, then sold it to fraudsters who used it to impersonate the officials over the telephone', obtaining transfers of money from their friends or relatives because of an alleged emergency situation. He was sentenced to 18 months in prison and fined.[35]

The most significant prosecution under article 253(a) is where Dun & Bradstreet's Chinese subsidiary, Shanghai Roadway D&B Marketing Services Co. Ltd., was fined one million yuan (US$160,640) and four former executives were sentenced to up to two years each in prison, and also fined, for illegally buying information on Chinese consumers.[36] The personal information purchased from insurance companies, banks, and other marketers allegedly involved 150 million Chinese consumers. Dun & Bradstreet subsequently sold the company.

Prosecutions are not, however, limited to large-scale data theft. In an identity theft case, Wang Zhengrong paid yuan 50,000 (US$10,000) to organize an identity swap between her daughter and the victim, so that her daughter could be admitted to university. The victim discovered the fraud when attempting to open a bank account, but found that she could not obtain her graduation and professional certificates because they had already been issued to Wang's daughter. Wang was sentenced to four years' imprisonment, on charges of forging official documents and seals, and her daughter's university degree revoked.[37] The issues in the case were the same as in the *Qi Yuling* constitutional law case (see section 2.1 of this chapter).

The following examples of court decisions under article 253(a) are a small sample of the more typical prosecutions involving sale and purchase of personal information in commercial quantities, with both prison sentences and suspended sentences resulting.

• A defendant who had obtained photocopies of the identity cards of 2,000 people either through illegal purchase or exchange on the Internet, and then sold the information, was found guilty of the crime of unlawfully accessing personal information of third parties and sentenced to a one-year prison term and a fine of 1,000 yuan (US$160), applying provisions of the PRC Criminal Law.[38]
• Twenty-three defendants, employees of a telecommunications company, illegally sold personal information including personal phone numbers of the company's subscribers. The court found that the sale infringed the legitimate rights and interests of the subscribers and caused serious damages and imposed jail terms ranging from 6 to 30 months.[39]
• Defendant Xu spent 500 yuan (US$80) to purchase over one million items of customer purchase information concerning a particular store from Zhang, who was prosecuted separately. Xu was convicted under article 253(1) and (2) of the Criminal Law for **(p.200)** illegally obtaining personal information, and given a suspended one-year sentence and a fine of 1,000 yuan (US$160).[40]
• In a similar case, Bai, in charge of personnel at a technology company, authorized the marketing manager (prosecuted separately) to purchase more than one million items of customer information for marketing purposes for 900 yuan (US$146). Bai later made a voluntary confession. The company was fined 30,000 yuan (US$5,000) and Bai was fined 10,000 yuan (US$1,600) and given a six-month suspended sentence.[41]

2.4. Civil law, including the Tort Liability Law

The civil law protection of privacy in China is now addressed specifically by the Tort Liability Law (TLL) 2009. To understand it first requires consideration of some aspects of case-law under the General Principles of Civil Law (GPCL), which may also be of continuing relevance, including to the application of the TLL. Like many civil law countries in Asia, China now has a civil law right of privacy through these statutes, though its boundaries are uncertain. In contrast, no common law country in Asia has developed a tort of invasion of privacy, or its approximation via extending the law of breach of confidence.

General Principles of Civil Law and privacy protection

The GPCL does protect a 'right of reputation',[42] and further states in the same provision:

> The personality of citizens shall be protected by law, and the use of insults, libel or other means to damage the reputation of citizens or legal persons shall be prohibited.

Other provisions provide specific protections to aspects of a person's name, portrait, and honour.[43] The GPCL does not contain an independent privacy right, but decided cases suggest it does provide some privacy protection. Ong refers to two interpretations by the Supreme People's Court[44] which show that, under the GPCL, various forms of disclosure of personal information are to be treated as an invasion or infringement of the right to reputation. Consequently 'privacy is not recognised as an independent right' but is merged with the right to reputation.[45] 'This means that a victim of an invasion of privacy

cannot sue to protect his privacy unless the invasion of privacy has also harmed his reputation.'[46] This approach was restated in the 1990s.[47] However, where harm to privacy interests could be established as part of damage to reputation, from at least 2001 compensation for emotional damage was available.[48] Ong discusses various cases which show that Chinese **(p.201)** courts were often willing to provide compensation for public disclosures of personal information which the plaintiffs wished to keep private. There have been ongoing differences between courts concerning the extent to which some previous disclosure of the information (and whether it was consensual or not) might cause plaintiffs to lose the ability to sue in relation to subsequent disclosures. In at least one decision, *Jiang Fenglan*, the court distinguished privacy from reputation, and although the facts did show that the disclosures (concerning workplace harassment) had lowered the plaintiff's social standing, her action was upheld on the basis that her rights of personality (protected by article 101) were infringed.[49]

Wang Fei Case and public disclosure of private facts

The most significant privacy-related decision under the GPCL, and one which is very widely discussed because of the prominence it gave to the phenomenon (not restricted to China) of 'human flesh search engines', is *Wang Fei v Zhang Leyi, Daqi.com and Tianya.cn*.[50] In 2008. Wang Fei's wife committed suicide after discovering his extramarital affair. Her university friend Zhang Leyi created a website which disclosed details of Wang Fei, including his address, family details, photographs, and other information, as well as articles about and by his deceased wife. The two web servicessued hosted this website as well as discussions about the website, including exchanges of information about Wang Fei. As a result, Wang Fei was tracked down and harassed, received death threats, and both he and his current partner were forced to resign from their jobs.

The aspect of the court's decision in the *Wang Fei Case* that may be of continuing importance, both under the GPCL and possibly even more so also under the more recent TLL, which is clearer in not requiring that interferences with privacy be related to reputation, is the court's explanation of what privacy means. As Ong explains:[51]

> According to the court, privacy means private life, information, space, and peace of private life related to a person's interests and personality that he does not intend to share with others. Therefore, the right to privacy is infringed by the disclosure or publication of private information that a person does not want to disclose to others concerning his private life, private areas, or domestic tranquillity and connected with his interests or his body.

The court went on to identify five factors important in determining whether privacy had been infringed: '(a) the manner by which the private information was acquired; (b) the manner in which the information was disclosed; (c) the scope of disclosure; (d) the purpose of disclosure; and (e) the consequences of disclosure'.[52]

The court also held that Internet information service providers had a duty to ensure that the information they provided was lawful, and 'upon discovery of such unlawful information must immediately remove the unlawful publication, keep relevant records of

the publication, and report the alleged unlawful information to the relevant authorities'. Similar duties are now explicitly prescribed under the TLL article 36 (see the following section), but are obviously not limited to that law. The result of the case was that the court required Zhang Leyi to pay 5,000 yuan (US$732) damages and Daqi.com to pay 3,000 yuan (US$438) damages to Wang Fei. Tianyi.com was found not liable because it had taken the **(p.202)** disputed content off its website before the proceedings commenced. The court found that the harm to the plaintiff was foreseeable, and that there was direct causality between the actions of the plaintiffs and the damage.[53]

Although the *Wang Fei Case* arose before the TLL was in effect, its analysis of the elements necessary for a tortious infringement of privacy interests may well have continuing relevance, given the lack of definition of 'privacy' in the TLL, and pending further relevant interpretations issued by the Supreme People's Court.

Right of privacy under the Tort Liability Law 2009, article 2

The PRC TLL which came into force in July 2010[54] includes a right to privacy in its list of protected 'civil rights and interests', but without defining further what is meant by 'privacy'. Article 2 provides that those 'who infringe upon civil rights and interests shall be subject to the tort liability according to this Law'. Civil rights and interests is then defined to 'include the right to life, the right to health, the right to name, the right to reputation, the right to honor, right to self image, right of privacy…and other personal and property rights and interests'.

It seems likely that some violations of personal information or data privacy will be violations of 'privacy' under article 2. Reported case decisions may further clarify the extent to which this is so. The extent to which the factors discussed in the *Wang Fei Case* will be relevant to that may be significant. Medical institutions also have additional obligations to protect patient's privacy.[55] Compensation is not restricted to pecuniary losses under the TLL, but is also available to compensate 'a serious mental distress'.[56] This was also the case for the GPCL.[57] Thomas notes that the TLL 'places civil litigation firmly at the heart of the law of tort in China', rather than a stress on regulation by state agencies, or any significant role for intermediaries.[58]

Privacy cases that have arisen under the TLL are few as yet, but already of a very different nature from those that have arisen under the GPCL. Examples of the very few known actions under article 2 of the TLL[59] indicate that it is primarily being used to resolve disputes between individuals, rather than against corporations.

Perhaps the most significant decision involved a family dispute over an advance for investment purposes which resulted in the plaintiff successfully suing his sibling for the return of the money. Guangzhou TV learned of the dispute from the court hearing and produced and broadcast a programme about it. The parties were not identified, and three family photos shown in the programme had all been obscured. The programme makers telephoned the plaintiff for an interview. The plaintiff contended that his sibling violated his right to privacy by providing photos of him and his mobile phone number to Guangzhou TV without his consent, and that the station should not have used the **(p.203)**

information. The lower court found that the photos and phone number were the plaintiff's private information and should not have been provided to Guangzhou TV without consent. However, the defendant sibling only disclosed the information to Guangzhou TV rather than more generally. Guangzhou TV also obscured the photos and did not publicize the plaintiff's phone number. The court found for the defendants, holding that there was no violation of article 2 of the TLL because the element of publicity was not established. The decision was upheld on appeal, with costs against the plaintiff.[60] The court seems to have read article 2 narrowly, by finding a requirement of publicity in relation to the disclosure and use of the phone number.

In a potentially significant case on visual surveillance, the defendants, living adjacent to the plaintiff in Xuhui District, Shanghai, installed two surveillance cameras, connected to their home computer, in the public areas between the two residences. The cameras were capable of collecting and recording the plaintiff's personal information. The lower court held that the defendants had violated the plaintiff's right to privacy and ordered removal of the cameras pursuant to articles 2, 3, and 15 of the TLL. Its decision was upheld on appeal and the defendants ordered to remove the cameras within five days.[61]

In a 2013 case the defendant found an envelope in his mailbox containing nine nude photos of the plaintiff, a colleague, and subsequently gave the envelope to Yang, a colleague of them both. Yang gave the photos back to the plaintiff, who broke down on seeing them. She had taken the photos herself on her mobile phone. The court held that the defendant's disclosure of the photos to a third party (Yang) was a violation of the plaintiff's article 2 TLL right to privacy and ordered the defendant to apologize, and pay 250 yuan (US$40) costs, but also found contributory negligence by the plaintiff and dismissed her other claims.[62]

The privacy rights in the Tort Liability Law therefore do not seem to have had a major commercial impact as yet, but it appears to be useful in inter-personal conflicts. Use of the Criminal Law article 253(a) is more common than civil litigation.

Responsibilities of IISPs for torts—Tort Liability Law 2009 article 36

'Network service providers', who may well be the same as Internet Information Service Providers (IISPs) (see section 3.3 of this chapter), have special obligations to prevent or stop tortious actions (for example, breaches of article 2) occurring through use of their network services. Article 36 provides as follows:

> Article 36 A network user or network service provider who infringes upon the civil right or interest of another person through network shall assume the tort liability.
>
> Where a network user commits a tort through the network services, the victim of the tort shall be entitled to notify the network service provider to take such necessary measures as deletion, block or disconnection. If, after being notified, the network service provider fails to take necessary measures in a timely manner, it shall be jointly and severally liable for any additional harm with the network user.
>
> Where a network service provider knows that a network user is infringing upon a civil right or interest of another person through its network services, and fails to

take necessary measures, it shall be jointly and severally liable for any additional harm with the network user.

(p.204) 'Network' or 'network service provider' are not defined, but it seems likely that the latter will be similar to 'IISPs', which includes both ISPs and content providers.

3. National private sector data privacy laws in China—sources and scope

This section surveys the sources of data privacy regulation relevant to all or most of the private sector (including consumer transactions, and all information and communications service providers via the Internet[63]). The privacy principles that emerge from these sources are discussed in the next section, and the measures to enforce them follow. Laws affecting all public sector bodies are then covered. Then the various sectoral and provincial laws are discussed.

Five key national legislative instruments setting out data privacy principles of broad application have been enacted from December 2011 to October 2013: 2011 MIIT Regulations, 2012 SC-NPC Decision, 2013 MIIT Guidelines, 2013 MIIT Regulations, and 2013 SC-NPC Amendments to the Consumer Law. The 2007 draft Bill should also be kept in mind for comparative purposes. This section outlines each of these sources, the extent of their authority, and the scope of their application. The data protection content of each of these sources of data privacy law is analysed in the next section. The Ministry of Industry and Information Technology (MIIT) is taking the leading role among ministries in the area of personal information protection.

3.1. 'Electronic information'—Decision of the SC-NPC

The SC-NPC is China's second-highest legislative body. Its Decision[64] 'on Internet Information Protection' ('2012 SC-NPC Decision'), promulgated 28 December 2012,[65] is the highest level law in China to deal specifically with data protection issues (see section 1.2 of this chapter concerning the hierarchy of laws in China). Its 12 clauses are drafted in very general terms, on the basis that it will be implemented by more specific regulations, as has been the case. This Decision has become the primary source or baseline for subsequent privacy regulation of 'electronic information' in China.

The Decision's first article defines what it (and regulations made under it) aim to protect: 'The State protects electronic information capable of personal identification and involving a citizens' privacy',[66] and then states in general terms the prohibition of the illegal acquisition or provision of such information by anyone. This clause, and the rest of the Decision are broader than the 'Internet' context suggested by its title. The remaining articles apply to all 'Internet service providers and other enterprises and institutions that collect or use citizens' personal electronic information in the course of their business'.[67] Although this includes the entities referred to as IISPs that had been regulated in 2011,[68] the scope of the Decision **(p.205)** is not restricted to these. It applies to companies in all industries, including, potentially, 'bricks and mortar' companies dealing with electronic personal information, such as that which is collected at point of sale and stored electronically. This scope means that the Decisions may potentially act as a 'gap filling' law, providing standards for industries without specific data privacy regulations, or as a basis

for the development of sector-specific implementing regulations (such as the 2013 MIIT Regulations).[69] Since the Decision, its key terminology (i.e. the general principles set out in article 2), has been adopted in other laws, including the 2013 amendments to the Consumer Law.

3.2. Consumer law—amendments by the NPC Standing Committee (2013)

The NPC Standing Committee amended the PRC's Law on the Protection of Consumer Rights and Interests in 2013[70] ('Consumer Law 2013') to include provisions on protection of personal information, along with other amendments. The privacy principles included in the 2013 Amendments are almost identical with those in the 2012 SC-NPC decision. China's second-highest legislative body is therefore being completely consistent in the data privacy principles it applies in different sectors, thus underlining the great significance of the 2012 Decision. These are the first significant amendments to China's consumer protection law since its passage in 1993. The Amendments apply to the use of consumers' personal information by all industries (companies that provide goods or services within China), in both online and offline situations. This law applies to all consumer transactions, not only to those in the Internet and telecommunications sectors where the MIIT Regulations apply.

3.3. IISPs—MIIT Regulations (2011)

From 15 March 2012 businesses providing 'Internet information services' in China were required for the first time to comply with a relatively comprehensive data privacy law, which can be briefly called the Internet Information Services Regulations,[71] made as a Decree of the MIIT.[72] The Regulations ('MIIT Regulations 2011') apply to '[a]ll those that are engaged in Internet information services and/or activities relating to Internet information services' in the PRC.[73] The expression 'Internet Information Services Provider' (IISP) is then used throughout. Although 'Internet information service' is not defined in the Regulation, the term 'IISP' is broader than it might at first seem, being a term drawn from regulations issued by the State Council in 2000[74] that simply refers to parties providing information to Internet users over the Internet.[75] Its application is not limited to Internet companies whose principal business is online (therefore **(p.206)** requiring a licence from the MIIT) but also applies to those whose online activities are more limited, including those providing e-commerce services, social media, online advertising, and mobile services.[76]

3.4. Internet/telecommunications—MIIT Regulations (2013)

The MIIT issued the Telecommunications and Internet Personal User Data Protection Regulations (the '2013 MIIT Regulations') in 2013,[77] which covers both IISPs and telecommunications business operators ('TBOs'),[78] and is intended as an implementing regulation for the 2012 SC-NPC Decision. These ministry regulations are also made under the Telecommunications Regulations 2000,[79] a higher level of legislation made by the State Council. Many aspects of these 2013 Regulations are similar to the MIIT Regulations 2011, including the requirements of minimum collection of information, notice, and data breach notification (although the details differ somewhat), but other aspects add a significant number of new or stronger forms of regulation, as discussed in the next section. The 2013

MIIT Regulations state that its rules regarding notice and consent will supersede any other law or regulation on this topic, which would appear to include the relevant provisions of the MIIT Regulations 2011.

3.5. Information systems generally—MIIT Guidelines (2013)

China added another significant layer of regulation of data privacy[80] in information systems, the Information Security Technology—Guidelines for Personal Information Protection Within Public and Commercial Services Information Systems,[81] released by the Standardization Administration of the MIIT in 2013 ('2013 MIIT Guidelines').[82] 'Guiding Technical Documents' are for voluntary reference and unenforceable against the targeted subjects. Rather than 'Mandatory Standards' and 'Recommended Standards', these are the weakest of three types of standards, intended for situations where formal standards are premature.[83]

(p.207) In theory, these voluntary guidelines are not as important as the other regulatory instruments covering part of the same territory (primarily Internet IISPs). However, these 2013 Guidelines apply to a much broader range of businesses, and they cover key issues (such as data exports, sensitive data, and subject access and correction rights), and provide some details not covered in the earlier instruments. They could also assist in indicating to courts the standard that should be applied in other laws, possibly including the Tort Liability Law, or in criminal law.[84] As official guidelines issued by the MIIT within its sphere of competence, it would be unwise for businesses operating in China to ignore them, even if formal sanctions do not directly follow breaches.

The scope of the Guidelines is broader than any other Chinese privacy instrument except perhaps the 2012 SC-NPC Decision. The Guidelines 'regulate all or part of the process of processing personal information through information systems'.[85] 'Information systems' are defined as 'computer information systems' but otherwise defined broadly, including such aspects as 'mobile communications terminal' and 'network'.[86] The computer information system need not be connected to the Internet. The document 'applies to all kinds of organizations and institutions other than the government agencies and other institutions which exercise public management responsibilities'.[87] So the Guidelines apply to the private sector broadly, not only to IISPs, the subject of the 2011 Regulation.

The Guidelines set out obligations in three overlapping ways: first as a description of responsibilities of each type of party;[88] second as a set of 'basic principles';[89] and third as a description of obligations arising throughout the life cycle of personal information, in four phases.[90] It is like three data protection laws for the price of one, and will no doubt cause some confusion to companies required to comply with them.

The Guidelines set out eight 'basic principles' that a 'Personal information administrator' should follow (discussed in the next section). They then set out detailed procedures that should be followed throughout four 'phases' (collection; processing; transfer; deletion) of the life cycle of personal information.[91] These procedures do reflect both the stated responsibilities of the different parties, and the eight 'basic principles', but in some respects they go further and add details not found in those versions. The analysis of data

privacy principles later in this chapter refers to matters covered in both these 'life cycle procedures' and the 'basic principles', as well as to the obligations of parties discussed above. All three must be considered.

Overall, these Guidelines are most comprehensive and better organized than the 2011 Regulations or 2012 Decision. Their significance remains somewhat mysterious. Will they continue to only have a shadowy existence as a set of voluntary guidelines, but sometimes influencing other laws or standards and their application? Or, given their very careful structure and considerable detail, are they a model for a future Chinese data protection law, once an enforcement structure is added? Livingston[92] seems ambivalent, and both possibilities may be correct:

> **(p.208)** The Guidelines also may reflect an evolving consensus by China's policy-makers regarding data privacy that may be further extended in subsequent binding legislation. In particular, the voluntary nature of the Guidelines, along with the creation of the industry self-regulatory group…may indicate that China intends to place greater emphasis on self-regulatory efforts in its emerging data privacy protection framework.

Subsequent regulations in 2013 and 2014 have also supported self-regulatory efforts.

3.6. Draft Personal Information Protection Act (2007)

In 2006/7, a comprehensive national draft Personal Information Protection Act ('2007 draft Bill'), drafted at the Institute of Law at the Chinese Academy of Social Sciences, was under consideration, covering both the private and public sectors, and including reasonably comprehensive sets of data privacy principles, apparently influenced by both the international 'basic principles' and the stronger 'European' principles. It did not, however, include a national data protection authority (DPA), but instead adhered to the 'ministry-based model' of enforcement. This was the first important attempt to draft a national data privacy law for China. This approach no longer seems to be favoured, which is perhaps not surprising in light of the post-2007 scepticism about following Western models.[93] Detailed analysis of this draft Bill is available elsewhere,[94] but it is noted here where its proposals still go beyond what is currently implemented in China.

4. Private sector in China—data privacy principles

China's data privacy principles are found distributed across the five key instruments described in the previous section: 2013 SC-NPC Amendments to the Consumer Law; 2012 SC-NPC Decision; 2013 MIIT Regulations; 2011 MIIT Regulations; and 2013 MIIT Guidelines. They are analysed here in accordance with the usual division of privacy principles. The principles are in effect cumulative, despite their slightly differing scope. The main aim of this section is to bring out that cumulative effect, so as to indicate the overall direction in which China's data privacy regulation is heading.

4.1. General statements of principles, and 'fair processing' principles

Both the 2012 SC-NPC Decision and the Consumer Law 2013 state very similar brief sets of principles, so they are the highest statement of overall data privacy principles yet found

in Chinese law. Two other comparable concise sets of principles are in the 2013 MIIT Guidelines and the 2007 draft Bill.[95]

(p.209) Consumer law—Amendments by the NPC Standing Committee (2013)

The revised law now provides in article 29 that:[96]

> The operators, collecting and using consumers' personal information, shall follow the legal, legitimate and necessary principles, express the purposes, methods and scope of using information, and obtain the consent of consumers. When collecting and using personal information of consumers, operators shall make public their rules for information collection and use, and use personal information only in accordance with agreements with consumers, or in accordance with applicable laws.
>
> Operators and their staff shall treat the collected consumer personal information in a strictly confidential manner, must not disclose, sell or illegally provide to others. Operators shall take technical measures and other necessary measures to ensure information security, and to prevent disclosure or loss of consumer personal information.
>
> In the circumstances that the information disclosure or loss occurs or may occur, immediate remedial measures shall be taken.
>
> If operators have not received consent or request from consumers, or if consumers have expressed rejection explicitly, the operators shall not send commercial information to such consumers.

Eight 'basic principles' (MIIT Guidelines 2013)

The Guidelines set out eight 'basic principles' that a 'Personal information administrator' should follow.[97] Their titles are listed below, with a quotation or paraphrase of their content as needed. It is included here because it is both current and detailed.

> a) *Clear purpose principle*—'handle personal information with certain, clear and reasonable purposes, do not expand the scope of uses and not change the purpose of handling personal information without the knowledge of the subject of personal information'.
> b) *Minimum & sufficiency principle*—'only handle the minimal information that is relevant to the purpose of (information) handling. Once such a handling purpose is achieved, personal information should be deleted/removed in the shortest possible time period.'
> c) *Public notification principle*—'In a clear, easily understandable and appropriate manner, truthfully inform the subject of personal information of the purpose of handling personal information, the scope of the collection and use of personal information, personal information protection measures, and other information.'
> d) *Personal consent principle*—'before handling personal information, [they] shall obtain the consent from the subject of personal information' (but without specifying whether express or tacit consent).
> e) *Quality assurance principle*—'ensuring that the confidentiality, integrity and

availability of personal information are all up to date'.
f) *Safety guaranty principle*—Security measures are to be appropriate to 'the likelihood and severity of damage'.
g) *Good faith fulfilling principle*—This largely repeats principles (a) and (b), adding compliance with legal requirements as another requirement.
(p.210) h) *Clear responsibility principle*—Requires clear definition of responsibilities, taking of appropriate measures, and recording processing so as to facilitate retrospective investigation.

Apart from the absence of references to data subject rights of access, correction, etc., this is a clear and quite strong statement of basic data protection principles. However, it does not cover all the obligations that are included elsewhere in the Guidelines, including when express consent is needed, special safeguards for sensitive information, additional restrictions on overseas data exports, data breach notification obligations, and the rights of data subjects.

'Fair processing' principles

A different approach in two of the laws is to state one very general 'fair processing' principle, rather than a list of principles. The data privacy principles in the MIIT Regulations 2011 in articles 11–14 require that IISPs 'shall provide services in accordance with the principles of equality, free will, fairness and good faith'.[98] In the Consumer Law 2013 operators are required to 'follow the legal, legitimate and necessary principles'.

4.2. Definitions—'personal' and 'sensitive' data

'Personal data'

The two SC-NPC laws do not define either 'personal information' or 'electronic information'. The MIIT Regulations 2011 define 'user's personal information' as 'any information that relates to a user and that separately or in combination with other information may be used to identify the user'.[99] This is similar to the definition of personal data used in laws in other countries, and clearly implies that this is broader than information collected from the user, such as information collected from third parties or information generated by the IISP itself from transactions with the user. The 2013 MIIT Guidelines define 'personal information' similarly.[100]

In the 2013 MIIT Regulations, the definition of 'personal user data' may be broader than the previous conventional definitions that are based on the capacity to 'identify a user', because it also includes 'other information, as well as the time, and place of the user using the service and other information, collected by [TBOs] and [IISPs] in the process of providing services'.[101] This provision is ambiguous. Does it mean that 'call data' information is by itself regarded as 'personal user data', or only when it is collected in conjunction with data with the capacity to identify? If it is the former, China is taking a significant step beyond the data privacy laws of most countries.

(p.211) Sensitive personal information

Chinese laws have not yet made much of a distinction between 'sensitive' and other personal data. However, the 2013 MIIT Guidelines have an explicit division of personal

information into 'general personal information', which is all personal information except 'sensitive personal information', which is defined as follows:[102]

> Namely, the information that would have an adverse impact on the subject of personal information if disclosed or altered. The specific contents of sensitive personal information of various industries shall be determined in accordance with the main desires of the subject of personal information accepting the services and the unique characteristics of the individual industry. For example, the sensitive personal information may include identity card numbers, mobile phone numbers, race, political viewpoint, religion, or biometric information, fingerprint and so forth.

4.3. Collection limitations—minimality, consent, and methods

PRC law is consistent in limiting collection to what is necessary for purpose ('minimal collection'). The SC-NPC Decision 2012 and the SC-NPC Consumer Law 2013 each only include a passing reference that in collecting personal data the organizations covered 'shall follow the principles of…necessity'. The MIIT Regulations 2011 and Guidelines 2013 both require minimal collection, and MIIT Regulations 2013 add a requirement of consent. In the MIIT Regulations 2011, collection is limited not to relevant information, but by the higher standard of minimal collection: 'Without the user's consent [an IISP]…shall not collect any information other than that required for its provision of service…' except as otherwise required by law.[103] In the MIIT Guidelines 2013, the 'Minimum & sufficiency' basic principle is that data controllers should 'only handle the minimal information that is relevant to the purpose of (information) handling'. The life cycle procedures also require minimal collection (with the relevant form of consent).[104]

The two SC-NPC laws require operators to obtain the consent of consumers in relation to collection, without being more specific. The MIIT Regulations 2013 specify that IISPs and TBOs 'may not collect or use personal user data' 'without user permission'.[105] This blunt requirement does not differentiate between data collected from the person concerned and that collected from third parties. No PRC legislation specifies what actions a data controller must take to demonstrate consent.

The MIIT Guidelines 2013 also limit methods of collection:[106] hidden or indirect methods of collecting information are prohibited; and collection of sensitive personal information from minors or persons with limited capacity requires consent of their guardian.

4.4. Notification of purpose of collection

Notifications of various matters to the data subject at the time of collection are required by all forms of regulation, with the Guidelines imposing the most detailed requirements. Where personal data is collected from third parties, it is not clear that notice must be given. According to the SC-NPC Decision 2012 (repeated in the Consumer Law 2013), an IISP must 'clearly explain the purpose, method and scope of collection and use of the information'. The MIIT Regulations 2011 require that the user must be expressly given **(p.212)** notice of the purpose ('use') for which the information is collected: 'When an Internet information service provider collects any User's Personal Information after obtaining the user's consent, such provider shall expressly inform the user of the means

by which such User's Personal Information will be collected and processed, as well as the content and use of such information'.[107] No such notification is required when information about users is collected from third parties.

The MIIT Guidelines 2013 set out nine categories of matters that are to be notified to the data subject before collection,[108] covering purpose, means, and content of collection; duration of retention; security measures; risks; consequences of non-provision; contact details of the administrator; and complaint channel. Circumstances where data is 'transmitted or entrusted to another organization' must be expressly notified, including purpose, content, and contact information of the receiver. No distinction is made between receivers within China and overseas. Whether 'another organization' includes intra-company transfers overseas is unclear, but will be covered by the data export limitations in any event.

4.5. Limits on use and disclosure—'finality' or not?

Although the two SC-NPC laws do not clearly require the 'finality' principle (uses and disclosures limited to the purposes of collection, with defined exceptions), the MIIT Regulations 2011 and Guidelines 2013 do more clearly adopt the finality principle. The SC-NPC Decision 2012 and the Consumer Law 2013 are vague, stating that IISPs may not 'use information in a manner that violates the provisions of laws and regulations, or the agreement of the parties without the approval of the individual whose information is collected'. It is therefore still unclear to what extent China's Internet privacy laws have fully adopted the finality principle, as the highest legal instruments are not yet clear.

The MIIT Regulations 2011 limit the use of the information collected to the purpose for which it was collected, stating that an IISP 'shall not use any User's Personal Information for purposes other than its provision of service'.[109] Whether 'use' also includes disclosure (provision of information to others) is not clear from the context. Concerning disclosures to others, article 13(2) is even more strict, stating that an IISP shall not 'provide the information uploaded by a user to others without the user's consent, except as required by laws or administrative regulations'. These two provisions therefore leave uncertain whether an IISP is limited in whether it can disclose information about its users which it has generated itself or it has collected from third parties. There is a further specific restriction that an IISP shall not 'transfer the information uploaded by a user without authorization or in the guise of the user's name, or deceive a user into transferring, or mislead or force a user to transfer, the information uploaded by such user'.[110]

The MIIT Regulations 2013 are not so clear. They say that 'without user permission' providers 'may not collect or use personal user data', and they require providers to 'notify users about the objective, method and scope of information collection and use',[111] so use beyond the purpose of collection requires consent.

The MIIT Guidelines 2013 include a stronger approach to finality in the 'Clear purpose' basic principle which requires data controllers to 'handle personal information with certain, clear and reasonable purposes' and states that they must 'not expand the scope of uses

and not change the purpose of handling personal information without the **(p.213)** knowledge of the subject of personal information'. Also, in Part 5 'Security of Telecommunications', article 66 protects communications against inspection of their content except where provided for by law[112] (where the exceptions allowed are substantial), and against disclosure by TBOs to third parties.[113] There are various separate provisions criminalizing the illegal sale or disclosure of both private sector and public sector personal information (see section 2.3 of this chapter).

4.6. Data quality

Obligations on data controllers to maintain the quality of user data (timeliness, relevance etc.) are still somewhat vague at all levels of regulation. Clause 2 of the SC-NPC Decision 2012 only imposes on IISPs requirements to 'follow the principles of lawfulness, timeliness and necessity', saying nothing else about requirements to maintain data quality. The Consumer Law 2013 sections are similar.

In the MIIT Regulations 2011, there are no requirements on IISPs to maintain the quality of user data (timeliness, relevance, etc.) except that they must not 'modify or delete the information uploaded by a user without authorization for no justifiable reason'[114] or 'do any other things that may harm the information updated by any user'.[115] The 2013 Regulations also contain no such requirements. The MIIT Guidelines 2013 'Quality assurance' basic principle requires data controllers to 'ensure that the confidentiality, integrity and availability of personal information are all up to date'.

4.7. Security of data

All levels of regulation include generally expressed security obligations, but the security standard to be adopted is no more precise than the requirements in the Guidelines that security measures be appropriate to 'the likelihood and severity of damage'. The 2012 SC-NPC Decision includes very general obligations on IISPs to strengthen their system's security provisions, to prevent it being 'disclosed, damaged or lost'.[116] But there is no clear indication whether this is an absolute liability, or whether negligence is required for breach. The Consumer Law 2013 says the same.[117] In the MIIT Regulations 2011 there is a general obligation on IISPs to 'properly keep' User's Personal Information[118] and an additional obligation that only applies to information uploaded by users, to 'strengthen their system security protection, legally safeguarding the security of information uploaded by users, and ensure users' ability to use, modify and delete the information updated by them'.[119] The MIIT Regulations 2013 have somewhat more detailed security protection provisions than in other laws, but not in the sense of specifying standards, merely listing which aspects of a business must pay attention to security.[120] Other provisions prohibit **(p.214)** 'using a telecommunications network to steal or damage a third party's information'[121] and require a 'sound internal security system'.[122] The MIIT Guidelines 2013 in the processing Guidelines reiterate the security and express consent requirements, and availability obligations.[123] The 'Safety guaranty' basic principle (f) requires data processors to take security measures appropriate to 'the likelihood and severity of damage'.

Data breach notification

Data breach notification to the relevant authorities is required at every level of regulation, but only the 2013 Guidelines also require that the data subject be notified. The SC-NPC Decision 2012 requires that where personal data is 'disclosed, damaged or lost, remedial measures shall be immediately adopted' (cl 4), and that the IISP 'shall immediately cease transmitting the information and adopt measures to remove and handle it, retain relevant records, and report to the relevant competent agency' (cl 5). The Consumer Law 2013 is similar but with less detail.

The MIIT Regulations 2011 have a broad provision requiring data breach notifications to the authorities:

> when any User's Personal Information kept by [an IISP] has been leaked or may be leaked, it shall immediately take remedies therefore; in the event that such leakage has resulted in or may result in any serious consequence, the [IISP] shall immediately report such event to the Telecommunications Authority that granted the provider its Internet information service permit or filing, and shall cooperate with the relevant authority in investigating and dealing with the event.[124]

Taken literally this does not require any notification to the data subjects. However, it is apparently the usual practice of the MIIT to request IISPs to notify data subjects when User's Personal Information kept by the IISP has been leaked or may be leaked. For example, when there were large-scale personal data leaks from IISPs in 2011, the MIIT issued a notice to all IISPs in the PRC requesting them to notify and remind users to change their user name and passwords. The notification method required may include website announcement, email, phone calls, and SMS. The MIIT Regulations 2013 add specific requirements of immediate report to and cooperation with the 'relevant telecommunications management organ' wherever 'grave consequences' are possible, and where 'especially grave', violations must be reported to the MIIT.[125]

The MIIT Guidelines 2013 set out in detail the responsibilities of an administrator, and add a requirement (previously not found) to notify data subjects when anything adverse to their interests happens to their personal information, and to report 'major incidents' to the relevant department.[126]

4.8. Accountable data controller and privacy policy

An accountable data controller is required at all levels of regulation. The SC-NPC Decision 2012 says that a citizen 'has the right to require the Internet service provider' to remedy various types of privacy breaches (cl 8). The MIIT Regulations 2011 had already required an IISP to 'prominently publicize its effective contact details, accept complaints from users **(p.215)** and other [IISPs], and respond to complaints within 15 days after receiving it'.[127] The MIIT Guidelines 2013 'Clear responsibility' basic principle (h), requires 'clear definition of responsibilities, taking of appropriate measures, and recording processing so as to facilitate retrospective investigation'. The data subject's right to complain or enquire to the administrator is repeated in the description of the responsibilities of the 'subject of the personal information',[128] which adds that an alternative avenue of complaint is to 'the administrative department that is responsible for personal information protection' (which

otherwise remains undefined).

The 2012 SC-NPC decision required that IISPs 'make their rules for collection and use publicly available', and the MIIT Regulations 2013 expand on this: TBOs and IISPs must 'formulate personal user data collection and use rules, and publish these in their business or service premises, websites, etc'.[129] This is much the same as saying that they must publish a Privacy Policy.

4.9. User rights?—access, correction, blocking, and deletion

All of China's data privacy laws primarily address the obligations of the administrator of personal information, and do not clearly state the rights of the subject of that information on such matters as access and correction, though they do concerning compensation. The 2013 Guidelines, for the first time, clearly assume and imply rights of access and correction in the obligations they place on administrators.

The SC-NPC Decision 2012 says nothing about access and correction, but does state rights of blocking and deletion (cl 8):

> 8. A citizen who discovers Internet information that discloses an individual's identity, broadcasts an individual's private affairs or otherwise infringes on his/her lawful rights and interests, or who suffers harassment from commercial electronic information, has the right to require the Internet service provider to delete the information or take other measures necessary to stop it.

The MIIT Regulations 2011 require that IISPs must 'ensure users' ability to use, modify and delete the information updated by them'.[130] But this does not cover other personal data originating from third parties. The requirement on a data controller to accept complaints from users and respond to them within 15 days does not in itself seem to imply rights of access and correction. In relation of information uploaded by users, IISPs are required 'to ensure users' ability to use, modify and delete the information updated by them',[131] so there is a deletion right in relation to this more limited class of information. The MIIT Regulations 2013 say that collection and use of personal data must cease when a user cancels an account,[132] but there is no requirement here or elsewhere that the data be deleted.

The MIIT Guidelines 2013, for the first time, clearly assume and imply rights of access and correction in the obligations they place on administrators. They set out what administrators must do when data subjects 'require for inspecting their personal information',[133] and that they must 'modify or supplement' the information when 'the subject of personal information finds that its personal information is flawed and requires modifications'.[134] It is probable that these rights will be read into the existing laws, in light of these Guidelines. The guidelines for the deletion phase[135] add a further user right, to seek timely deletion of **(p.216)** personal information 'for proper reasons'; obligations to delete where purposes of collection are completed, or de-identify where some continued handling is needed; and procedures for deletion in case of bankruptcy or insolvency.

Despite the 2013 Guidelines, the weakest element of China's data privacy laws remains the omission of the normal 'user rights' in relation to a person's own personal information, such as access and correction (except in the non-enforceable Guidelines), blocking of use, and deletion/de-identification (sometimes found). If users do not have the ability to obtain access to their own personal information and to ensure it is correct, then one of the fundamental elements of a data privacy law is missing.

4.10. Data export limitations

None of the current Chinese privacy instruments at any level say anything about exports overseas of personal data, except the voluntary Guidelines of 2013 (also the 2007 draft Bill). There are at present no general restrictions on the private sector to be found in other laws, though laws concerning state secrets or other specific matters could be quite restrictive, as may provincial laws.[136]

Despite the lack of existing legal restrictions, MIIT Guidelines 2013 article 5.4.5 is very explicit:

> Absent express consent of the subject of the personal information, or explicit legal or regulatory permission, or absent the consent of the competent authorities, the administrator of personal information shall not transfer the personal information to any overseas receiver of personal information, including any individuals located overseas or any organizations and institutions registered overseas.

It should be stressed that these are only voluntary guidelines, and there have been no attempts to require businesses to adhere to them. Nevertheless, businesses need to consider that the Guidelines suggest a very strong restriction:[137] without express consent from the data subject, personal data cannot be transferred overseas unless there is some law permitting this (there are none of general application) or there is 'the consent of the competent authorities'. While notice and implied consent is generally sufficient in relation to 'general' (non-sensitive) personal information, this is not so for data exports, for which express consent is required. There is no exception for intra-company transfers, and no provision for binding corporate rules. Use of cloud computing facilities by China-located companies may involve use of a server which is 'overseas', but is there a 'transfer…to any overseas receiver'? The transfer phase guidelines[138] reiterate consent and security requirements, and that the administrator, before transferring personal information, must define the responsibilities of the receiver of the information. It would therefore be prudent for data controllers to advise data subjects of the potential transfer of data overseas and to obtain their consent, and to clarify the obligations of overseas processors.

(p.217) ### 4.11. Direct marketing opt-out

The Consumer Law 2013 article 29 and the 2012 SC-NPC Decision article 7 both require that operators must not send commercial communications without consent, and must comply with express requests not to send such communications. These direct marketing limits are not found in either the 2011 Regulations or the 2013 Guidelines.

4.12. Controller responsibilities concerning processors

The respective responsibilities of data controllers and processors are not addressed in the SC-NPC Decision and the Consumer Law, and remain somewhat unclear. The MIIT Regulations 2013 require IISPs and TBOs to supervise and manage data protection when they utilize third party processing facilities, and they 'may not entrust agents who do not conform to personal user data protection requirements'.[139] This could impose a strict liability on data controllers for the actions of their processors (wherever they are located), or it could be read as merely requiring due diligence in selecting and supervising processors. It would be necessary to see how this is administered in practice.

The MIIT Guidelines 2013 give the most detailed indication of where Chinese law may be heading on the controllers/processors distinction. An 'administrator of personal information' is defined as 'the organizations and institutions, which determine the purpose and manner of personal information processing, actually control personal information and use information system to process personal information'.[140] All three conditions must be satisfied, so a mere data processor (in EU terminology) will not be an 'administrator'. The responsibilities of an administrator are set out in detail and make it clear that a great deal of planning and supervision is required concerning personal information.[141] Notable inclusions are requirements to notify data subjects when anything adverse to their interests happens to their personal information; to report 'major incidents' to the relevant department; and to 'collaborate with a third party testing and evaluation agency to assess the personal information protection status of information system' (discussed below).

The 2013 Guidelines make a distinction between such an 'administrator' and a 'receiver of personal of personal information', defined as 'the individuals, organizations and institutions, which obtain personal information from information system, and handle obtained personal information in accordance with the willingness of the subject of personal information'.[142] That the 'receiver' is what would elsewhere be described as a 'data processor' is clear from the description in the Guidelines of a receiver's role: 'When the acquisition of personal information is for the purposes of information processing commissioned by the other party, personal information receiver shall, in accordance with the technical guidance documentation and the commission contract, process personal information, and immediately delete personal information after the processing task is completed.'[143] This would be even clearer if article 3.5 referred to the 'instructions of the administrator of personal information' rather than 'the willingness of the subject of personal information', but it nevertheless does make sense: the receiver/processor must not process personal information contrary to the purposes for which the data subject has consented.

In the 2013 Guidelines, a 'third party testing and evaluation agency' is defined simply as a 'professional evaluation agency, which is independent from the personal information **(p.218)** administrator',[144] with its responsibilities described as 'conducting the testing and evaluation on information systems' to 'provide evidences/basis for a personal information administrator to evaluate, supervise and guide the protection of personal information'.[145]

5. Enforcement provisions concerning the private sector in China

The enforcement methods in the 2011 MIIT Regulations are diverse, but primarily at the

initiative of the Telecommunications Authorities. They do not include civil damages provisions, but these may be provided by other aspects of Chinese law, read in conjunction with these Regulations. Enforcement is not addressed by either the 2012 SC-NPC Decision, or the 2013 Guidelines (because of their voluntary nature).

5.1. Authorities involved in enforcement

At the 2008 National People's Congress, a decision was made to establish a new Ministry of Industry and Information Technology (MIIT). It has absorbed a number of the offices and ministries that participated in earlier discussions on personal information protection legislation. The MIIT has since become the main driver of data privacy developments in China. The 2013 SC-NPC Amendments to the Consumer Law provide that the State Administration of Industry and Commerce (SAIC), which regulates China's consumer market, will now have a role alongside MIIT in regulating information privacy. Their jurisdictions will overlap in relation to consumer e-commerce, and how they will coordinate remains to be seen.

The 2012 SC-NPC Decision does not specify which authorities will enforce the requirements it establishes. It says that 'relevant competent agency' will use its existing powers ('carry out its duties within the scope of its mandate in accordance with law') in order to 'prevent halt and investigate' (cl 10) the criminal conduct referred to in clause 2, 'as well as other Internet information-related criminal conduct'. IISPs must cooperate and provide technical support.

The MIIT Regulations 2011 provide for the supervision and administration of IISPs by the MIIT and 'the communications administration authorities of all provinces, autonomous regions and municipalities directly under the central government' who are collectively referred to as the 'Telecommunications Authorities'.[146] Businesses may therefore have to deal with Chinese authorities at multiple levels of government in relation to these Regulations.

The MIIT Regulations 2013 provide a requirement of annual 'self inspection' of security measures, and response to what is found.[147] They include greater detail regarding how supervision and inspection by 'telecommunications management organs' is to be carried out.[148] Also, failure by telecommunications management organs to impartially administer the Regulations is to be punished, and is also a crime by individual public officers.[149]

The creation of a separate DPA, or other body with national responsibility for administration or enforcement of the obligations and remedies in relation to privacy has not been proposed, even in the 2007 Draft Bill.

(p.219) 5.2. Administrative orders, penalties, and adverse publicity

Under the 2012 SC-NPC Decision, individuals have a specific right to file a complaint with 'the relevant competent agency' concerning any criminal conduct, and the agency must 'process it promptly in accordance with law'.[150] Agencies are not required, it seems, to investigate and mediate in civil actions, or make orders for compensation, but the individual concerned can take civil action (see section 5.3 of this chapter). Clause 11 then

provides:

> Conduct violating this decision shall be subject to penalties, such as warnings, fines, confiscating unlawful gains, revoking licenses or cancelling registrations, terminating websites, prohibiting responsible employees from engaging in the network services business and recordation in social credit files and public announcements. Conduct that constitutes a violation of public security management shall be subject to public security management penalties in accordance with law. Conduct that constitutes a crime shall be investigated for criminal liability in accordance with law. Conduct that infringes a citizen's civil rights and interests shall be subject to civil liability in accordance with law.

The 2013 Amendments to the Consumer Law provide for administrative enforcement in relation to the same types of infringement (those 'who have infringed consumers' personal dignity, liberty, or right of personal information protection') as can give rise to civil actions under article 50 (see 5.3 of this chapter). The 'department in charge of industrial and commercial administration or other relevant administrative departments' is then required to take one or more of the following forms of enforcement, 'based on the circumstances':[151] (a) order the operators to rectify their acts; (b) issue a warning; (c) issue a fine of up to 500,000 yuan (US$82,250), where there are no illegal earnings; (d) confiscate illegal earnings, or impose a fine 10 times the illegal earnings; (e) order the operators to suspend operations for rectification; or (f) rescind their business licences if the circumstances of their offences are serious.

Breaches of any of the privacy-related provisions in the MIIT Regulations 2011 may result in a Telecommunications Authority ordering the IISP to take corrective actions, and giving the IISP a warning, and a concurrent fine of between RMB10,000 (US$1,250) to RMB30,000 (US$4,750) may be imposed. The Telecommunications Authority is required to make a public announcement if it does so.[152] Breaches of article 13 may also result in legal liability under other laws.[153] A Telecommunications Authority may, before it makes a decision on a matter, require an IISP to suspend an activity and the IISP must comply.[154] If a Telecommunications Authority concludes in an investigation that a violation may have 'an extraordinarily material effect', the event must be reported to the MIIT. IISPs are also required to report other IISPs to the relevant Telecommunications Authority if they become aware of activities which may cause 'a material impact on the interests of users'.[155]

Although not fully co-extensive, these three laws between them provide seven types of enforcement actions by ministries: (i) issuing of warnings; (ii) orders for rectification and/or cessation of processing; (iii) administrative fines; (iv) confiscation of profits/illegal earnings and possible punitive fines; (v) adverse publicity, including public announcements, and reports to the MIIT; (vi) employment prohibitions and adverse entries in employees' social credit files; and (vii) suspension/termination of business operations, **(p.220)** websites, or licences. There is in general a right of appeal against such administrative actions.[156] Ministries can also prosecute for criminal offences.

5.3. Civil damages

The 2012 SC-NPC Decision states that 'conduct that infringes a citizen's civil rights and interests shall be subject to civil liability in accordance with law' and 'a person whose rights have been infringed can initiate litigation in accordance with law'.[157] The Amendments to the Consumer Law 2013 also provide for civil liability for infringements of these principles: 'Operators, who have infringed consumers' personal dignity, liberty, or right of personal information protection in accordance with law, shall stop such infringements, restore consumers' reputation, offer apologies, and pay damages.'[158] Official consumer associations will also now be able to commence court actions on behalf of consumers, including where the rights of very large numbers of consumers are infringed, such as in large-scale data breaches. A form of class action will therefore be more likely. The MIIT Regulations in 2011 and in 2013 did not include any specific provisions concerning the payment of civil damages when a breach of an article resulted in harm.

It is likely that the civil liability specifically provided for the SC-NPC Decision and in the Consumer Law could be pursued under the Tort Liability Law (see section 2.4 of this chapter). It is also possible that the breach of the MIIT 2011 or 2013 Regulations could be the basis for a damages action under the Tort Liability Law.

5.4. Adverse publicity as a sanction

The MIIT Regulations 2013 provide that violations must be logged by the telecommunications management organs in the 'social credit register' of an IISP or TBO, and published,[159] an unusually strong 'name and shame' sanction. Fines may be similarly published.[160]

5.5. Co-regulation and self-regulation by trade associations

In the MIIT Regulations 2013 there is explicit encouragement to telecommunications and internet 'sector associations' to introduce complementary self-regulatory measures,[161] and there is similar 'encouragement' in the 2013 MIIT Guidelines.[162] MIIT's China Software Evaluation and Test Center (CSTC) announced in January 2013 the formation of a 'Personal Information Protection Alliance' of internet companies, industry associations, and standards testing and evaluation centres, which is to develop industry self-regulation and possibly play a consultative role in future legislation.[163] Similarly, the members of the Alliance are encouraged to 'launch personal user data protection self-discipline work',[164] which probably means educating their users how to protect their own personal data.
(p.221)

6. Public sector personal information in China

There is no comprehensive data privacy law dealing with China's public sector, including its national public sector. However, a number of recent national laws have a considerable impact on the public sector at all levels, and provide a partial set of data privacy rights relating to access, correction, and security, but without principles related to such matters as collection, retention, use, and disclosure of public sector data. Provincial and local data privacy laws may also be relevant (see section 7 of this chapter).

6.1. Regulations on Open Government Information—access and correction rights

The State Council promulgated the Regulations on Open Government Information in 2007,[165] giving Chinese citizens rights of access and correction to personal information at all levels of government.[166] Government agencies are required to disclose certain categories of government information on their own initiative,[167] but these categories are not directly relevant to personal information. However, individuals may also file information requests 'based on the special needs of such matters as their own production [and] livelihood', with government bodies at county level and above.[168] It is implied that the information should be provided unless there is a legal basis for withholding it.[169] Questionable cases are to be referred to the department responsible for secrecy at the same administrative level.

Agencies should not disclose matters concerning 'individual privacy', but such information can be disclosed 'with the consent of the rightholder(s) or if administrative organs believe that non-disclosure might have a major impact on the public interest',[170] without indicating how this is to be determined. There is a 'reverse-freedom of information (FOI)' provision requiring that the individuals concerned must first be consulted before information affecting their privacy is disclosed.[171] There is a specific right to have incorrect personal information corrected.[172] Such correction rights are still only found in a minority of FOI or 'right to information' laws around the world.

(p.222) In summary, on paper China's right to information law provides a full set of rights of access and correction, and protection against wrongful disclosure, in relation to personal information. After the first two years of operation of the law, it was reported that it had been used quite substantially by people wishing to obtain their personal information.[173] The extent to which it is valuable in revealing the operation of government is a separate question.

6.2. Laws prohibiting improper disclosures of public sector personal information

China's laws also provide specific and comprehensive protections against wrongful disclosure of, and access to, public sector personal information.

SPC Provision on actions for improper government disclosures

The Provisions on Several Issues regarding the Hearing of Administrative Cases Involving Public Government Information were issued by the Supreme People's Court and came into force on 13 August 2011. These Provisions (a category of law) stipulate that a citizen can file an administrative lawsuit against the government if it considers that government publication of information infringes upon her or his individual privacy. Where the breach is proven, the court is required to render a judgment that the disclosure of such information is illegal and may order the government to take remedial measures.[174] This last court order is very significant, confirming the right of citizens to take action against government agencies for wrongful publication of personal information.

Standing Committee of the NPC Decision 2012

The 2012 Decision of the Standing Committee of the National People's Congress states that that 'State agencies and their employees shall maintain the confidentiality of citizens' personal electronic information learned in the course of carrying out their duties, and shall

not disclose, falsify, damage, sell or illegally provide it to others'.[175] This is the highest level data privacy law affecting China's public sector.

This clause does not explicitly impose any of the obligations in the other clauses of the Decision on State agencies, and therefore lacks detail. It reinforces, and perhaps makes more specific, the Supreme People's Court Provisions in 2011. The SPC Provisions referred to wrongful disclosure, but did not mention actions where a state agency (or its employee) falsifies or damages personal information. Nevertheless, the SC-NPC Decision is a significant advance in the data protection obligations of public sector agencies in China.

(p.223) 6.3. Other data privacy principles and the public sector

Apart from these access and correction rights, and the prohibitions on sale or purchase of government-held personal data, Chinese citizens do not yet have other data protection rights based on principles limiting collection, retention, use, or disclosure of security or personal data. Only the 2007 draft law has proposed such comprehensive rights,[176] and it is unlikely to re-appear. China's data privacy principles for the public sector are therefore substantially incomplete.

6.4. Other laws on specific government information

Sectoral data privacy laws relating to specific categories of government information may affect the private sector and government bodies alike. For example, amendments to the Law on Resident Identity Cards in 2011 require organizations entitled to use ID cards 'such as government agencies, financial institutions, telecommunications service providers, communications providers, educational institutions and medical institutions, and their employees', to keep confidential the information they obtain from such cards when performing duties or providing services. Substantial administrative penalties can result from breaches, and civil liability can result if violations result in damage.[177] Most countries in Asia that have ID cards do not have such provisions penalizing their misuse.

7. Sectoral and provincial laws in China

It is beyond the scope of this chapter to cover comprehensively either the local or sectoral data privacy laws in China. Some examples of such legislation will illustrate how complex and diverse the Chinese legislative structures dealing with privacy have become.

7.1. Provincial and city laws

Various provincial and city administrations have also enacted local data privacy codes, particularly in consumer law. Some examples of such laws, which may now need to be aligned with the 2013 changes to the national consumer law, are:

- Shanghai's Consumer Protection Rules prohibit businesses 'from disclosing to a third party a consumer's personal information' and 'from asking consumers to provide any personal information unrelated to the business transaction at hand'.[178]
- Henan Province's Information Ordinance provides that commercial enterprises must give individuals the right to 'request the amendment or deletion of untrue information'; may not disclose a consumer's personal

information to a third person without the consumer's consent; and must not collect personal information that is unrelated to the consumer's purchase of goods or services.[179]

(p.224) • Jiangsu Province's Regulation of Information Technology 'includes comprehensive provisions on the collection and use of personal information and relevant legal liabilities for violations', and is not limited to a particular sector (e.g. banking) but applies to use of information technology generally. It also criminalizes any use of illegal means (such as theft, black-market purchase, or other fraud) to obtain personal information.[180]

• Xuzhou City (Jiangsu province) Municipal Provisions for Protection of Computer Information System Security prohibit any person from using any computer information system to: provide or publicize another person's private information without consent; steal account numbers, codes, or other information; intercept, alter, or delete others' email or other data; or publicize or send information by false impersonation. Many other provisions are included.[181]

7.2. Sectoral legislation

Businesses operating in China need to check whether there is national or local sectoral data privacy legislation for their industry, such as in the following examples in the important sectoral areas of health, social insurance, and credit information:

• The Basic Norms for Electronic Medical Records (Ministry of Health, 2010) 'prohibit unauthorized review of patients' medical records by other institutions and persons besides the medical personnel that perform the medical activity and quality control personnel' and 'permit the review of medical records, after obtaining consent of the medical institution, for the purpose of scientific research and education'.[182]

• The Social Insurance Law (2010) 'will prohibit governmental authorities and other organizations, as well as their staff, from disclosing personal information which they may obtain in the course of their work' and breaches can result in administrative punishment and civil compensation.[183]

• Regulations and Administrative Measures were issued by the People's Bank of China in 2013 to regulate credit reference agencies.[184] The Regulations 'established a series of rules for the collection, use, processing, disclosure and transfer of personal information by credit reference agencies'. The Measures 'provide more detail, by clarifying and specifying rules for the establishment of credit reference agencies that deal with the personal credit information of individuals'.[185] The Measures require security inspections by qualified third party institutions, and increased surveillance if data leaks occur, among other matters designed to ensure security of credit information. **(p.225)**

8. Conclusions—a complex but coherent advance for data privacy in China

At the same time as there is perceived to have been a 'turn against law', since 2007,[186] in the small field of data privacy China has made considerable advances toward the rule of law, in both the public and private sectors. The five national privacy-related laws since

2012 amount to a substantial body of data privacy law. China's data privacy laws need to be viewed as including the criminal law provisions (particularly article 253(a)) and the TLL 'privacy tort', which are parts of the essential enforcement mechanisms for the subsequent data privacy legislation. The national data privacy laws have only been applied through regulations to the operation of commercial activities involving consumers and users of Internet or telecommunications facilities, but the 2012 SC-NPC Decision has the capacity to be applied more broadly. It is unclear whether it could cover employee information, but some such exclusions also occur in the laws of other countries (see Chapter 17). Sectoral, regional, and municipal laws add to the coverage, and the complexity. Despite uncertainties, the scope of data privacy protection in China is broadening constantly. For the first time, China is approaching a data privacy law for its whole private sector.

8.1. The cumulative effect of the principles

The cumulative effect of these laws, in terms of privacy principles, is that there is increasing consistency, and most minimum privacy principles are included, as are some stronger principles. Still sometimes missing, or not explicit, are data subject rights of access and correction. 'Finality' in relation to subsequent uses and disclosures is not fully established. On the other hand, minimum collection principles are strict, data breach notification is required at all levels, and marketing uses are not supposed to occur without consent. These are principles with flaws, but not only the minimum possible.

8.2. A choice of methods of enforcement

China has developed a wide range of different forms of enforcement to protect privacy: criminal prosecutions for illegal sale or purchase of personal data; individual rights of action via a privacy tort (of uncertain scope), which will probably also be used to enforce legislative standards; and administrative actions by responsible ministries. All of these approaches allow individuals access to court or administrative remedies. Ministerial compliance orders, fines, and adverse publicity, are part of the standard toolkit. Constitutional rights relevant to privacy cannot be the basis of civil actions. At present, the most frequently used enforcement method is the criminal law, but in terms of impact the profusion of MIIT regulations and guidelines, and sectoral laws, may have considerable effect even without enforcement actions. At a future stage, individual tort actions, and ministry enforcement of privacy principles, may come to the fore. In any event, we can conclude that even without a comprehensive data privacy law, the range of enforcement methods potentially available is very substantial. The one element that does not seem likely to appear is a coordinating data protection authority separate from ministries.

(p.226) Evidence of enforcement is present in the considerable number of criminal prosecutions, and some civil actions under the Tort Liability Law are also occurring. There is as yet evidence of enforcement actions being taken under the various data privacy laws enacted since 2012, but it is still very early for such enforcement action to have been taken and also to become public. As in some other jurisdictions it a question of 'wait and see', while nevertheless insisting that evidence is required for credibility.

Notes:

([1]) Hunton and Williams LLP, 'A Summary of Developments in Personal Information Protection in China since August 2009' (Hunton and Williams LLP, 16 February 2011) <https://www.huntonprivacyblog.com/2011/02/articles/update-privacy-and-the-protection-of-personal-information-in-china/>.

([2]) John Keay, *China: A History* (Harper Press, 2008); Jonathan Fenby *The Penguin History of Modern China: The Fall and Rise of a Great Power 1850–2009* (Penguin, 2009).

([3]) Jiangyu Wang, ch. 1 'China: Legal Reform in an Emerging Socialist Market Economy' in E. Ann Black and Gary F. Bell (Eds.), *Law and Legal Institutions of Asia*, (Cambridge, 2011), pp. 24–5.

([4]) Albert Chen, *An Introduction to the Legal System of the People's Republic of China* (4th Edn., LexisNexis, 2011).

([5]) Wang, ch. 1 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, pp. 24–61; Vai Io Lo and Xiaowen Tian, *Law for Foreign Business and Investment in China* (Routledge, 2009), ch. 1 'An Overview of the Chinese Legal System'.

([6]) A somewhat outdated guide to online sources is Joan Liu, 'Finding Chinese Law on the Internet' (GlobaLex, 2005) <http://www.nyulawglobal.org/globalex/china.htm>.

([7]) This summary is based on Chen, *An Introduction to the Legal System of the People's Republic of China*, pp. 125–6, and as noted; Wang, ch. 1 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, pp. 33–7.

([8]) The Standing Committee may enact and amend all laws except the basic reserved for the full NPC, and may supplement and amend laws made by the NPC, consistent with their terms. As a subset of the membership of the NPC, it meets a number of times per year, whereas the full NPC is only in session annually: see Chen, *An Introduction to the Legal System of the People's Republic of China*, pp. 131–4.

([9]) Chen, *An Introduction to the Legal System of the People's Republic of China*, p. 134.

([10]) This summary is based on Chen, *An Introduction to the Legal System of the People's Republic of China*, pp. 154–69; Wang, ch. 1 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, pp. 37 and 45–6.

([11]) Chen, *An Introduction to the Legal System of the People's Republic of China*, p. 166.

([12]) Chen, *An Introduction to the Legal System of the People's Republic of China*, pp. 166–7.

([13]) Chen, *An Introduction to the Legal System of the People's Republic of China*, pp. 154–5.

([14]) Chen, *An Introduction to the Legal System of the People's Republic of China*, pp. 154–

5.

([15]) Chen, *An Introduction to the Legal System of the People's Republic of China*, pp. 183–90; Wang, 'China: Legal Reform in an Emerging Socialist Market Economy', pp. 45–51.

([16]) Lo and Tian, *Law for Foreign Business and Investment in China*, p. 18.

([17]) Wang, ch. 1 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, p. 26.

([18]) Wang, ch. 1 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, p. 21.

([19]) Jerome Cohen, Foreword to Chen, *An Introduction to the Legal System of the People's Republic of China*, p. v.

([20]) Chen, *An Introduction to the Legal System of the People's Republic of China*, p. 46.

([21]) For details of the ID cards, see Cheryl Brown, 'China's Second-Generation National Identity Card: Merging Culture, Industry and Technology' in Colin Bennett and David Lyon, *Playing the Identity Card* (Routledge, 2008).

([22]) Zhizheng Wang, 'Systematic Government Access to Private Sector Data in China' (2012) 2(4) *International Data Privacy Law*, pp. 220–9.

([23]) The Decision requires that any services providing access accounts for the Internet, or for fixed or mobile telephone services, or that provide 'information publication services for users' (blogs, websites, social networking services, or any other services allowing user-generated content (UGC)), 'shall require a user to provide his/her real identity when entering into an agreement with the user or confirming the services to be provided' (art. 6). It does not require 'real names' to be used whenever a person is providing information online, it only requires that the ISP or content host must be able to identify who is the content provider.

([24]) Constitution of the People's Republic of China, as amended to 2004 (China Yearbook 2004) <http://english.gov.cn/2005-08/05/content_20813.htm>.

([25]) Translation from 'China's *Marbury vs. Madison*?—Direct Application of the Constitution in Litigation' (*China Legal Change*, 20 September 2001), copy held, no longer available on the Internet.

([26]) 'Decision on Abolishing some Judicial Interpretations (the Seventh Batch) issued before the end of 2007' (Supreme People's Court, 18 December 2008).

([27]) Constitution (China), art. 67, lists as a function of the Standing Committee of the NPC 'to interpret the Constitution and supervise its enforcement'.

([28]) 'China's *Marbury vs. Madison*?'.

([29]) For a very detailed account of the controversies, see Robert J. Morris, 'China's

Marbury: Qi Yuling v. Chen Xiaoqi—The Once and Future Trial of Both Education & Constitutionalization' (2012) 2 *Tsinghua China Law Review* pp. 273–316 <http://tsinghuachinalawreview.org/articles/PDF/TCLR_0202_Morris.pdf>.

([30]) It ratified the International Covenant on Economic, Social and Cultural Rights in 2002 but with a reservation concerning trade unionism.

([31]) Chen, *An Introduction to the Legal System of the People's Republic of China*, p. 169.

([32]) Amendment 7 to the Criminal Law of the People's Republic of China (VII)—2009 (United Nations Office on Drugs and Crime, unofficial translation, undated).

([33]) Scott Livingston, 'Dun & Bradstreet Reportedly Fined RMB $1 Million for Illegally Obtaining Personal Information in China; Four Employees Imprisoned' (Covington and Burling 'Inside Privacy', 10 January 2013) <http://www.insideprivacy.com/international/dun-bradstreet-reportedly-fined-rmb-1-million-for-illegally-obtaining-personal-information-in-china/>.

([34]) Criminal Law (China), arts. 285(2) and (3), inserted by the 2009 Seventh Amendment.

([35]) *Zhou Jianping Case*: First Instance Criminal Judgment No. 612 of 2009, People's Court of Xiangzhou District of Guangzhou Province, Zhuhai City; see Hunton and Williams LLP, 'New Chinese Tort Liability Law Contains Provisions Affecting Personal Data' (Hunton and Williams LLP Client Alert, January 2010).

([36]) Shanghai Zhabei District Court, 28 December 2012; Kathy Chu, 'Dun & Bradstreet Fined, Four Sentenced in China' (*Wall Street Journal*, 9 January 2013) <http://online.wsj.com/news/articles/SB10001424127887323482504578230781008932240>.

([37]) *China v Wang Zhengrong* Shaoyang, Beita District People's Court, 26 October 2009; paraphrase of H. Hong Xue, 'Privacy and Personal Data Protection in China: An Update for the Year End 2009' (2010) 26 *Computer Law & Security Report*, p. 286.

([38]) People's Court, Longgang District of Shenzhen Municipality, 14 October, 2011; paraphrased from P. McKenzie and J. Fang, 'China's Online Data Privacy Rules Coming into Effect; Other Recent Data Privacy Developments in China', *Morrison & Foerster Client Alert*, 23 February 2012.

([39]) Beijing Second Intermediate People's Court, 5 August 2011; see McKenzie and Fang 'China's Online Data Privacy Rules Coming into Effect'.

([40]) People's Court, Shanghai Pudong New District, Case Number (2013) PU Criminal First 1087 (2013); information provided by George Tian.

([41]) People's Court, Shanghai Pudong New District, Case Number (2013) PU Criminal First 86(4) (2013); information provided by George Tian.

([42]) GPCL (China), art. 101.

([43]) GPCL (China), arts. 99, 100, 102.

([44]) Article 140 of the Opinions of the Supreme People's Court on *Several Issues Concerning the Implementation of the GPCL*, 1988, referring to disclosure of personal secrets, and to fabrication of facts; and article 7 of the *Explanation of Several Problems in Reviewing Reputation Right Infringement Cases*, referring to publicizing private information of others, or broadcasting the privacy of others without consent.

([45]) Rebecca Ong, 'Recognition of the Right to Privacy on the Internet in China' (2011) 1(3) *International Data Privacy Law*, pp. 172–9 at p. 172.

([46]) Ong, 'Recognition of the Right to Privacy on the Internet in China', p. 172.

([47]) Supreme People's Court Interpretation Several Questions on Adjudicating Cases of the Rights to Reputation, 1993 and 1998. See Ong, 'Recognition of the Right to Privacy on the Internet in China', p. 172.

([48]) Article 1 of the Supreme People's Court Problems regarding the Ascertainment of Compensation Liability for Emotional Damage in Civil Torts, 2001. See Ong, 'Recognition of the Right to Privacy on the Internet in China', p. 173.

([49]) Ong, 'Recognition of the Right to Privacy on the Internet in China', pp. 173–5.

([50]) Beijing Chaoyang District Court, No. 10930 of 2008.

([51]) Ong, 'Recognition of the Right to Privacy on the Internet in China', p. 175.

([52]) Ong, 'Recognition of the Right to Privacy on the Internet in China', p. 175.

([53]) Ong, 'Recognition of the Right to Privacy on the Internet in China', p. 175.

([54]) Tort Liability Law, Standing Committee of the National People's Congress, 26 December 2009, <http://www.procedurallaw.cn/english/law/201001/t20100110_300173.html>.

([55]) TLL (China), art. 52.

([56]) TLL (China), art. 22.

([57]) 'The court should accept the cases that involve the violation of other people's privacy and harming public interests and social morality when victims request compensation for moral damage to the people's court on the ground of tort': art. 1 of *The Interpretation of the Supreme People's Court on Issues Regarding the Determination of Compensation Liability for Moral Damages in Civil Torts* [Chinese version] at <http://blog.sina.com.cn/s/blog_9b13f5da01016hbs.html>.

([58]) Kristie Thomas, 'PRC Tort Liability Law 2009: Implications for Enterprises Operating in China' (Nottingham Business School, November 2011)

<http://ssrn.com/abstract=2000164>.

([59]) The assistance of Rebecca Ong in providing the English translation of these decision summaries from her own research is gratefully acknowledged, and from which the three decisions discussed are paraphrased.

([60]) *Wu Mingshen v Li Juming and Others* (2011), Guangzhou Intermediate People's Court (on pkulaw).

([61]) *Zhang v Pan & Others* (2011), Shanghai No.1 Intermediate People's Court (on pkulaw).

([62]) *Cao v Wang* (2013), Shanghai Jing'an District People's Court (on pkulaw).

([63]) Usually called 'Internet Information Service Providers' (IISP).

([64]) 'The Decision of the Standing Committee of the National People's Congress on Strengthening Internet Information Protection', adopted at the 30th Session of Standing Committee of the 11th National People's Congress on December 28, 2012; Unofficial English translation by Ishimaru & Associates LLP, at <http://ishimarulaw.com/strengthening-network-information-protectionoctober-china-bulletin/>.

([65]) It became effective immediately: 2012 SC-NPC Decision, art. 12: 'This Decision shall become effective on the day it is publicly announced.'

([66]) 2012 SC-NPC Decision, art. 1.

([67]) 2012 SC-NPC Decision, art. 2.

([68]) 'Internet information service providers' (IISPs), regulated by the MIIT Regulations 2011, are not limited to what are normally called 'ISPs', it also extends to any Internet content providers who collect or use personal data, such as social networking services (SNS), and at least any websites using identified accounts (including some search engines).

([69]) The significance of this broad scope was pointed out by Scott Livingston in email communications.

([70]) The Amendments were passed on 25 October 2013, coming into effect on 15 March 2014.

([71]) 'Several Regulations on Standardizing Market Order for Internet Information Services', Decree of the Ministry of Industry and Information Technology (No. 20), 7 December 2011, in force 15 March 2012. An unofficial English translation by Morrison & Foerster LLP's Beijing Office is available on request from chinamarketingteam@mofo.com.

([72]) The MIIT, as a ministry or department of the State Council, is entitled to make 'departmental rules' in areas falling within its administrative powers, but these rank lower

than laws made by the NPC or its Standing Committee, and must be consistent with those laws.

([73]) MIIT Regulations 2011 (China), art. 2.

([74]) Regulation on Internet Information Service of the People's Republic of China, State Council, 25 September 2000.

([75]) McKenzie and Fang, 'China's Online Data Privacy Rules Coming into Effect'.

([76]) The Regulations also seems to apply to non-profit activities using the Internet because article 2 does not limit its scope to businesses, and the earlier Regulation in 2000 distinguishes 'profitable' and 'non-profitable' Internet information services but applies to both. Article 3 of the Regulation on Internet Information Service of the People's Republic of China (State Council 25 September 2000) provides that 'internet information service is divided into two categories: profitable Internet information service and non-profitable Internet information service'.

([77]) Telecommunications and Internet Personal User Data Protection Regulations (unofficial English translation), issued on 28 June 2013, effective 1 September 2013 <http://chinacopyrightandmedia.wordpress.com/2013/07/16/telecommunications-and-internet-user-individual-information-protection-regulations/>.

([78]) MIIT Regulations (China), art. 2.

([79]) Telecommunications Regulations of People's Republic of China <http://tradeinservices.mofcom.gov.cn/en/b/2000-09-25/18619.shtml>. They create and regulate telecommunications business operators (TBOs), and must be complied with by 'anyone that engages in telecommunications activities or activities related to telecommunications' in the PRC (art. 2).

([80]) Some comment on these Guidelines is from Graham Greenleaf and George Tian, 'China's Third Line Expands Data Protection: The 2013 Guidelines for Personal Information Protection' (2013) 122 *Privacy Laws & Business International Report.*

([81]) The English translation of the 2013 MIIT Guidelines used is by George Tian. They were published on 21 January 2013, effective 1 February 2013.

([82]) A draft of these Guidelines was issued in February 2011 for comment. Industry organizations apparently had some input into the drafting. The draft was issued by the Administration of Quality Supervision, Inspection and Quarantine (AQSIQ) and the Standardization Administration of China (SAC), within the MIIT.

([83]) L. Ross, A. Gao, and K. Zhou (Wilmer Hale law firm), 'China Issues Draft Guidelines On Online Privacy, Announces New Agency To Supervise The Internet', Wilmer Hale website, 24 May 2011, at <http://www.wilmerhale.com/publications/whPubsDetail.aspx?publication=9789>.

([84]) Scott Livingston, 'China Releases National Standard for Personal Information Collected Over Information Systems; Industry Self-Regulatory Organization Established' (Covington and Burling, Inside Privacy, 25 January 2013) <http://www.insideprivacy.com/international/china-releases-national-standard-for-personal-information-collected-over-information-systems-industr/>.

([85]) MIIT Guidelines 2013 (China), art. 1.

([86]) MIIT Guidelines 2013 (China), art. 3.1.

([87]) MIIT Guidelines 2013 (China), art. 1.

([88]) MIIT Guidelines 2013 (China), art. 4.1.

([89]) MIIT Guidelines 2013 (China), art. 4.2.

([90]) MIIT Guidelines 2013 (China), art. 5.

([91]) MIIT Guidelines 2013 (China), art. 5.

([92]) Livingston, 'China Releases National Standard for Personal Information Collected Over Information Systems; Industry Self-Regulatory Organization Established'.

([93]) Wang, ch. 1 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, p. 21.

([94]) Graham Greenleaf, 'China's Proposed Personal Information Protection Act' (2008) 91 *Privacy Laws & Business International Newsletter* pp. 1–6, and pt. II (2008) 92 *Privacy Laws & Business International Newsletter* pp. 11–14, <http://ssrn.com/abstract=2023065>.

([95]) The 2007 draft Bill set out 10 'General Provisions', called 'principles' in art. 2-8, similar to the sets of data protection principles usually found in other national privacy laws. They covered the following (though with different titles): (i) purposes (protecting individual rights and facilitate the orderly flow of personal information); (ii) lawfulness of processing; (iii) user rights of access and correction; (iv) balance of interests (between individual, state and society); (v) information quality ('accuracy, integrity and timeliness'); (vi) information security; (vii) professional duty of processors to protect confidentiality; (viii) data subject's right to remedies (administrative remedies or litigation, including compensation); (ix) scope (conventional definition of 'personal information'); (x) exemptions (security, legislative and judicial agencies; personal and household uses; minimal uses). There is no explicit collection limitation principle, and use and disclosure is only restricted to 'related' purposes.

([96]) Consumer Law 2013 (China), art. 29; unofficial translation by George YiJun Tian.

([97]) MIIT Guidelines 2013 (China), art. 4.2.

([98]) MIIT Regulations 2011 (China), art. 4.

([99]) MIIT Regulations 2011 (China), art. 11. This has a broader scope than references to 'information uploaded by a user' (art. 13), which only refers to matters such as music files uploaded by a user.

([100]) MIIT Guidelines 2013 (China), art. 3.2: 'the computer data, that may be processed by an information system, is relevant to a certain natural person, and that may be used solely or along with other information to identify such natural person'.

([101]) MIIT Regulations 2013 (China), art. 4.

([102]) MIIT Guidelines 2013 (China), art. 3.8.

([103]) MIIT Regulations 2011 (China), art. 11.

([104]) MIIT Guidelines 2013 (China), art. 5.2.

([105]) MIIT Regulations 2013 (China), art. 9.

([106]) MIIT Guidelines 2013 (China), art. 5.2.

([107]) MIIT Regulations 2011 (China), art. 11.

([108]) MIIT Guidelines 2013 (China), art. 5.2.2.

([109]) MIIT Regulations 2011 (China), art. 11.

([110]) MIIT Regulations 2011 (China), art. 13(3).

([111]) MIIT Regulations 2013 (China), art. 9.

([112]) MIIT Guidelines 2013 (China), art. 66: 'Telecommunications subscribers' freedom to legally use telecommunications and the confidentiality of their communications are protected by law. No organization or individual may, for any reason whatsoever, inspect the content of telecommunications, except that public security authorities, the State security authority and the People's Procuratorate may do so in accordance with the procedures stipulated by law in response to the requirements of State security or the investigation of criminal offences.'

([113]) MIIT Guidelines 2013 (China), art. 66: 'No telecommunications business operator or its employees may provide, without authorization, to a third party the content of information transmitted through the telecommunications network by telecommunications subscribers.'

([114]) MIIT Regulations 2011 (China), art. 13(1).

([115]) MIIT Regulations 2011 (China), art. 13(4).

([116]) SC-NPC Decision 2012 (China), art. 4.

([117]) Consumer Law 2013 (China), art. 29.

([118]) MIIT Regulations 2011 (China), art. 12.

([119]) MIIT Regulations 2011 (China), art. 13.

([120]) MIIT Regulations 2013 (China), art. 13.

([121]) MIIT Regulations 2013 (China), art. 58(2).

([122]) MIIT Regulations 2013 (China), art. 60.

([123]) MIIT Guidelines 2013 (China), art. 5.3.

([124]) MIIT Regulations 2011 (China), art. 12.

([125]) MIIT Regulations 2013 (China), art. 14.

([126]) MIIT Guidelines 2013 (China), art. 4.1.3.

([127]) MIIT Regulations 2011 (China), art. 14.

([128]) MIIT Guidelines 2013 (China), art. 4.1.2.

([129]) MIIT Regulations 2013 (China), art. 8.

([130]) MIIT Regulations 2011 (China), art. 13.

([131]) MIIT Regulations 2011 (China), art. 13.

([132]) MIIT Regulations 2013 (China), art. 9.

([133]) MIIT Guidelines 2013 (China), art. 5.3.7.

([134]) MIIT Guidelines 2013 (China), art. 5.3.6.

([135]) MIIT Guidelines 2013 (China), art. 5.5.

([136]) Jiansu Province enacted a Regulation of Information Technology in 2012 which generally requires official approval for data transfers outside the province: Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press, 2013), p. 91, citing W. Scott Blackmer, 'Transborder data flows at risk' (*Lexology*, 20 February 2012).

([137]) The draft Guidelines (2011) were strict in a different way, providing that there should not be transfer of personal data out of China without the express consent of the 'governing administrative authority' (a technical committee under the SAC). The 2007 draft Bill only provided that government agencies in charge of information resources *may* restrict cross-border transfers by private sector bodies under certain conditions: for

details, see Greenleaf, 'China's Proposed Personal Information Protection Act'.

([138]) MIIT Guidelines 2013 (China), art. 5.4.

([139]) MIIT Regulations 2013 (China), art. 11.

([140]) MIIT Guidelines 2013 (China), art. 3.4

([141]) MIIT Guidelines 2013 (China), art. 4.1.3.

([142]) MIIT Guidelines 2013 (China), art. 3.5.

([143]) MIIT Guidelines 2013 (China), art. 4.1.4.

([144]) MIIT Guidelines 2013 (China), art. 3.6.

([145]) MIIT Guidelines 2013 (China), art. 4.1.5.

([146]) MIIT Regulations 2011 (China), art. 3.

([147]) MIIT Regulations 2013 (China), art. 16.

([148]) MIIT Regulations 2013 (China), art. 17.

([149]) MIIT Regulations 2013 (China), art. 24.

([150]) 2012 SC-NPC Decision (China), art. 9.

([151]) Consumer Law 2013 (China), art. 56(9).

([152]) MIIT Regulations 2011 (China), arts. 16, 18.

([153]) MIIT Regulations 2011 (China), art. 16.

([154]) MIIT Regulations 2011 (China), art. 15.

([155]) MIIT Regulations 2011 (China), art. 15.

([156]) Chen, *An Introduction to the Legal System of the PRC*, pp. 293–304.

([157]) 2012 SC-NPC Decision (China), arts. 9 and 10.

([158]) Consumer Law 2013 (China), art. 50.

([159]) MIIT Regulations 2013 (China), art. 20.

([160]) MIIT Regulations 2013 (China), art. 23.

([161]) MIIT Regulations 2013 (China), art. 21.

([162]) The 2007 draft Bill provided for an option to data subjects of complaint resolution by

'self regulatory trade associations', operating under strict conditions set at State Council level, and also guided by local regulators: see Greenleaf, 'China's Proposed Personal Information Protection Act'.

([163]) Livingston, 'China Releases National Standard for Personal Information Collected Over Information Systems; Industry Self-Regulatory Organization Established'.

([164]) MIIT Regulations 2013 (China), art. 7.

([165]) Regulations on Open Government Information (China), State Council Decree 492, 17 January 2007, effective 1 May 2008 (unofficial translation, The China Law Center, Yale Law School February 2009).

([166]) The regulations apply to organizations that are authorized by laws or regulations to exercise the functions of managing public affairs (art. 36).

([167]) Regulations on Open Government Information (China), arts. 9–12.

([168]) Regulations on Open Government Information (China), art. 13.

([169]) Regulations on Open Government Information, art. 14: 'Prior to disclosing government information, administrative organs should examine the government information to be disclosed in accordance with the provisions of the Law of the People's Republic of China on Safeguarding State Secrets and other laws, regulations and relevant state provisions'.

([170]) Regulations on Open Government Information (China), art. 14.

([171]) Regulations on Open Government Information (China), art. 23: 'If an administrative organ believes that the requested government information involves commercial secrets or individual privacy the disclosure of which might infringe upon the lawful rights and interests of a third party, it should write to the third party to seek its opinion. If the third party does not agree to have the information disclosed, the information may not be disclosed. However, if the administrative organ believes that non-disclosure might have a major influence on the public interest, it should disclose the information and notify the third party in writing of the content of the government information they have decided to disclose and the reasons therefor administrative organs should reply to the requests on-the-spot to the extent possible.'

([172]) Regulations on Open Government Information (China), art. 25: 'If citizens, legal persons or other organizations have evidence showing that the government information provided by an administrative organ concerning them is not recorded accurately, they have the right to request the administrative organ to correct the information. If the administrative organ does not have the authority to make the correction, the case should be transferred to the administrative organ that does have such authority, and the requester shall be so informed.'

([173]) Jamie Horsley, 'Update on China's Open Government Information Regulations: Surprising Public Demand Yielding Some Positive Results' (*Human Rights in China*, 15 July 2010) <http://www.hrichina.org/en/content/3247>.

([174]) Paraphrasing Paul McKenzie and Jiungxiao Fang, 'China's Online Data Privacy Rules Coming into Effect; Other Recent Data Privacy Developments in China' (*Morrison & Foerster Client Alert*, 23 February 2012) <http://www.mofo.com/files/Uploads/Images/120223-China-Privacy.pdf>.

([175]) 2012 SC-NPC Decision (China), art. 10.

([176]) The 2007 draft Bill included a set of data privacy principles which applied to government agencies, and allowed complaints to be made concerning disclosure, correction or cessation of use of personal data, and to seek compensatory damages in a court, but they have not reappeared as yet.

([177]) Hunton and Williams LLP, 'New Chinese Legislation Includes Provisions Protecting Personal Information' (Hunton and Williams LLP, 8 November 2011) <https://www.huntonprivacyblog.com/2011/11/articles/new-chinese-legislation-includes-provisions-protecting-personal-information/>.

([178]) Anthony Winton, Alex Zhang, Suzanne Innes-Stubb, and Lucy Xu, 'Data Protection and Privacy in China' (White and Case, March 2012) <http://www.whitecase.com/alerts-02142012-1/#.UyF1GV6BQgI>.

([179]) Winton, 'Data Protection and Privacy in China'.

([180]) Hunton and Williams LLP, 'New Chinese Legislation Includes Provisions Protecting Personal Information'.

([181]) Paul McKenzie and Gordon Milner, 'Recent data protection developments in the People's Republic of China' (Morrison & Foerster LLP, 5 March 2009) <http://www.mofo.com/recent-data-protection-developments-in-the-peoples-republic-of-china-03-05-2009/>.

([182]) Hunton and Williams LLP, 'A Summary of Developments in Personal Information Protection in China since August 2009'.

([183]) Hunton and Williams LLP, 'A Summary of Developments in Personal Information Protection in China since August 2009'.

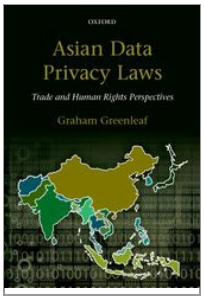
([184]) People's Bank of China, *Administrative Regulations on the Credit Information Collection Sector* (effective 15 March 2013); People's Bank of China *Administrative Measures for Credit Reference Agencies* (15 November 2013, effective 20 December 2013).

([185]) Hunton and Williams LLP, 'People's Bank of China Issues Administrative Measures for Credit Reference Agencies' (Hunton and Williams LLP, 21 December 2013)

<https://www.huntonprivacyblog.com/2013/12/articles/peoples-bank-china-issues-administrative-measures-credit-reference-agencies/>.

([186]) Wang, ch. 1 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, p. 21; see section 1.3 of this chapter.

University Press Scholarship Online
Oxford Scholarship Online



Asian Data Privacy Laws: Trade & Human Rights Perspectives
Graham Greenleaf

Print publication date: 2014
Print ISBN-13: 9780199679669
Published to Oxford Scholarship Online: December 2014
DOI: 10.1093/acprof:oso/9780199679669.001.0001

Japan—The Illusion of Protection

Graham Greenleaf

DOI:10.1093/acprof:oso/9780199679669.003.0008

[–] Abstract and Keywords

Japan has had comprehensive data privacy legislation since 2003, which is the focus of this chapter. Informal methods of conflict resolution play a significant role, as does guidance from ministries, of varying degrees of formality. The privacy principles in Japan's laws are shown to be among the most limited in Asia. The chapter also analyses Japan's range of enforcement mechanisms, and the available evidence of the extent to which they have been used, and to what effect, and finds that evidence of enforcement is very often lacking. The Japanese government has decided to amend its laws. It has already created a form of data protection authority (DPA) to deal only with issues concerning the tax ID system, and has foreshadowed a general purpose DPA. Like elsewhere in Asia, Japan's 'second generation' data protection law may be considerably stronger than the first generation law.

Keywords: data protection, privacy, Asia, Japan, ministries, data protection authority

(p.228)

1. Context of information privacy in Japan

Protection of information privacy in Japan derives primarily from legislation, but case law developments are also relevant. Informal methods of conflict resolution play a significant role, as does guidance from ministries, of varying degrees of formality, on how legislation is to be interpreted and applied. Unlike some of its neighbours (South Korea, Taiwan, and Mongolia) post-war Japanese society has not experienced an internal revolt against authoritarian rule, and its data protection laws are therefore not seen as part of the ‘package of liberties’ often characteristic of post-authoritarian states. However, Japan is the epitome of the bureaucratic state, often admired by Western analysts of administration ‘who marvel at its extremely subtle means of control, its tentacles reaching downward into industry and upward into politics’.[1] One critic concludes that ‘Japan’s bureaucracy can lay claim to being the world’s most sophisticated—several rungs up the evolutionary ladder from the weak, constrained officialdom in other countries’.[2] One of the questions examined in this chapter is whether Japan’s bureaucratic model of administration has delivered anything useful to consumers and citizens in terms of privacy protection over the last decade. What happens in Japan is important for the future of data privacy in Asia: as well as being one of Asia’s longest-established democracies, it has the world’s tenth largest population (about 128 million), and is the world’s third largest economy by nominal GDP.

1.1. Japan—political, historical, and legal context

Japan is a democracy with a bicameral parliament and a constitutional monarchy with an emperor. Japan accepted its impending defeat in World War II when complete destruction was the alternative, and its empire was largely dismantled. The Tokyo War Crimes Trials removed only a small part of the elite responsible for the previous totalitarian state. Allied occupation from 1945–52 attempted to democratize Japan, but contentiously retained the institution of the Emperor.[3] Japan adopted its current constitution in 1947, to a substantial extent imposed on a United States model. The Diet (parliament) comprises the Upper Diet (Sangi-In) and Lower Diet (Shuugi-In). Japanese politics has been relatively stable since the end of the post-war Allied occupation. The conservative Liberal Democratic Party (LDP) has been in power since 1955, except for a short period in 1993 and from 2009 to 2012. The post-war generation has experienced economic prosperity and has not had to react against authoritarian rule. Japan is a unitary state, not a federation, but ordinances passed by 1,742 local government bodies[4] are a significant and complex part of the legal system, including in relation to data privacy.

Japan's legal system and courts have been influenced substantially by German civil law models, and to a lesser extent by French civil law. Following the new 1947 constitution there was substantial influence by the American common law system (particularly in constitutional law and criminal procedure), so that the system became 'coloured by a mixture of German and American models'[5] or even a hybrid of civil and common law. **(p.229)** The Japanese legal system is also characterized by a preference for arbitration, mediation, or conciliation as an alternative to judicial settlement of disputes,[6] and by various administrative practices which provide guidance falling short of formal law.[7] Both practices are significant in Japan's data protection system.

Japan's court system is comparatively simple in structure, with its Supreme Court also being its constitutional court. The court system is divided into levels[8] with eight High Courts (with circuits of several prefectures) and the Supreme Court at the peak. Judicial precedents, particularly those of the Supreme Court, although not legally binding, are of greater significance than in some other civil law countries. The Supreme Court and each lower court are also constitutional courts. Their constitutional decisions concerning freedom of speech and other liberties do affect the development of data privacy.

1.2. Social attitudes to privacy in Japan

There is considerable academic argument about the nature and extent of the Japanese sense of privacy, with recent writers less inclined to claim major differences between Japanese and Western senses of information privacy. Adams, Murata, and Orito, after surveying this debate, hypothesize that 'the Japanese sense of information privacy is as strong as that in Western cultures, and has existed for a significant period, but differs as to the placement of boundaries through which information should not flow, and the types of information that are blocked by those boundaries'.[9] They give examples from 'a rich set of social norms comprising the Japanese sense of information privacy', such as when people who obtained knowledge about others by overhearing it, would act as if they were unaware of it. They conclude that 'the speed with which Japanese society has moved from reliance on social norms to the development of legal protection for information privacy, demonstrates just how strong the Japanese sense of information privacy is'. Laws are simply the 'latest expression' of this sense of privacy.

1.3. International obligations in relation to privacy

Japan is a member of the OECD, and its legislation is influenced by the OECD privacy Guidelines. It is also a member of the Asia-Pacific Economic Cooperation (APEC) but its legislation pre-dates the APEC Privacy Framework. Japan has applied to join APEC's CBPR system.

In Japan, treaties have direct effect as law, upon ratification, without requiring implementing domestic legislation, though the boundaries of this are contested. Although the Cabinet can enter treaties, those treaties within the jurisdiction of the Diet, requiring finance, or of high political significance, require ratification by the Diet.[10] Japan ratified the International Covenant on Civil and Political Rights 1966 (ICCPR) in 1979, and so Article 17 concerning privacy is part of Japanese law, but Japan has not yet ratified the first Optional **(p.230)** Protocol to the ICCPR. Complaints ('communications') cannot therefore be made against Japan to the UN Human Rights Committee.

1.4. Constitutional and civil law protections

Article 13 of the Constitution of Japan (1946) provides that:

> All of the people shall be respected as individuals. The right to life, liberty, and the pursuit of happiness shall, to the extent that it does not interfere with the public welfare, be the supreme consideration in legislation and in other governmental affairs.

The Constitutional provisions have had substantive effects relevant to privacy through case law, such as in Supreme Court decisions limiting wiretapping.[11] However, although decisions of lower courts held that the Juki-net resident registration network infringed article 13 in the absence of the consent of individuals to be included in it, the Supreme Court held otherwise in 2007 in the *Juki-net Case*.[12] The Court confirmed the basis of the protection of privacy under article 13:

> Article 13 of the Constitution provides that citizens' liberty in private life shall be protected against the exercise of public authority, and it can be construed that, as one of individuals' liberties in private life, every individual has the liberty of protecting his/her own personal information from being disclosed to a third party or made public without good reason.[13]

In finding that Juki-net did not infringe this principle, the Court took into account factors such as: the limited information contained in Juki-net and that it 'cannot be regarded as highly confidential information that is related to an individual's inner mind'; it was operated on the basis of laws and regulations and for justified administrative purposes; there was 'no concrete risk' of unauthorized outside access; and that use by the system operators for non-intended purposes (e.g. data matching) was prohibited by law. It held, contrary to the lower court, that the higher protective provisions against change of use found in the legislation governing Juki-net would apply, not the lower standards which more easily allowed change of use found in the Act on the Protection of Personal Information Held by Administrative Organs (PPIHAOA).

There is clearly considerable potential for article 13 to be used to provide protections for information privacy, given the factors that the Supreme Court found relevant in the *Juki-net Case*. Although the Supreme Court first recognized the constitutional right to privacy under article 13 in 1969, the first appearance of a privacy tort under provisions of the Civil Code occurred eight years earlier in a Tokyo District Court case involving a book by the writer Yukio Mishima which allegedly disclosed details of the lives of a prominent couple.[14] Some authors regard this as a transplantation of a concept derived from US tort law which has been 'a roaring success', with numerous privacy tort actions for two decades before the 2003 legislation.[15] Court decisions have confirmed that the privacy tort can protect matters **(p.231)** such as financial affairs, aspects of personal life such as sickness, magazine subscriptions, pension entitlements, and criminal records after the sentence has been served. Further examples are given later in this chapter in discussion of remedies under Japan's privacy legislation.

The first Supreme Court decision recognizing the right to privacy under article 13 of the Constitution involved a ruling that demonstrators had a right not to be photographed by the police without their consent, but the Court found the photography to be justified in this case because of the urgent need to collect evidence of an offence, and the photographs were taken 'by an appropriate method'.[16] Other Supreme Court decisions have found that that the fingerprinting of foreigners did involve privacy issues but was justified on grounds of social welfare,[17] and that a university breached the right of privacy when it submitted to the People's Republic of China (PRC) a list of students, without their consent, who had applied to attend a lecture by the Chairman of the PRC.[18] In this last case, a majority of the Court considered that the university was 'not allowed to disclose more information to others than is necessary' unless this was based on the intention or consent of the persons concerned, at least where there were no special circumstances making consent difficult to obtain. They had a 'rational expectation' that their voluntarily provided information concerning their personal lives would be adequately controlled. Oda considers such cases as examples of 'rights that were not foreseen at the time of enactment of the Constitution but which have gained significance since then'.[19] While not as clear as constitutional decisions in Korea or Taiwan concerning 'informational self-determination', the Japanese Supreme Court decisions go in the same direction.

2. Data privacy legislation in Japan

After a decade of operation of its data privacy law, Japan's government is planning a major overhaul. The development of Japan's data privacy laws can only be understood in the context of the development of its national ID systems.

2.1. Data privacy laws as the price for ID systems

As in many countries, there is a close relationship between the development of surveillance systems in Japan and the development of data protection laws, now in its third iteration.

Juki-net, Keidanren, and the development of Japan's data protection law

The catalyst for privacy being elevated in Japan to an issue of national concern 'was the public and political resistance to the enactment of the *Basic Resident Registers Act 1999*'.[20] This was an attempt to convert the long-established paper-based system of the Resident Basic Register System (which tracks people's movements between residences) into a national electronic network. Juki-net was intended to combine the resident registration databases of 3,200 municipal governments, and give every Japanese citizen an ID number. **(p.232)** Juki-net is restricted by law to only transmitting four pieces of personal data (name, sex, date of birth, and address), plus a randomly generated 11-digit unique number. There is a Juki-net card that enables easy access to local (and some national) services via the web or ATM-like machines at local government offices. Although acquisition of the card is voluntary, having a number is not. The card can have a photo if the person wishes, but that is not included in the Juki-net system. Although it was predicted that it would rapidly be issued to more than half of Japan's population, take up of the Juki-net card has been very limited, amounting to less than 5.1 per cent of Japan's population by mid-2012.[21] Juki-net has not become a very extensive national identification system, and Japan is not at the more intrusive end of the spectrum of surveillance societies.

Prior to 2003, the ruling Liberal Democratic Party could not force the Juki-net legislation through the Diet without an amendment promising a personal data protection law for the private sector (a public sector law having existed since 1988).[22] A Working Group on Personal Data Protection, set up in 1999, proposed a system close to self-regulation, with no penal provisions.[23] The government decided to include penal provisions, and a new committee was established to draw up a revised Bill.[24] Having promised to introduce private sector data protection in order to pass the Juki-net legislation, the government was facing pressure from the Japanese media, which had become generally supportive of this expansion (having been reassured by allowances for journalistic use in the EU Directive). Accordingly the government commenced discussions with representatives of the financial sector, particularly with Keidanren, the representative body for large Japanese commercial and industrial concerns. Adams, Murata, and Orito explain that Keideran issued a policy in September 2000 'which clearly asserts the view that industry self-regulation is the way forward for data protection regulation in Japan, following the US model',[25] similar to the original Committee report to the government. However, after discussions with government, it reversed its position in 2003, and 'perhaps surprisingly threw its considerable political weight behind the development of such a law, provided of course that the regulations to be applied would be agreed with industry cooperation'. In their view:[26]

> the rationale of the members of *Keidanren* seems to have been that their international trading operations with European companies were already subject to significant data protection regulation. With the US having agreed the Safe Harbour agreement with the EU, a similar regime in Japan should not adversely effect trade with the US, while a national legislative data protection regime in Japan would put Japanese companies at a potential competitive advantage in EU trade.

After considerable political controversy, and the withdrawal of the original Bill because it did not include exemptions for the media or for individuals, a package of legislative measures was passed on 30 May 2003 and came into force on 1 April 2005.

(p.233) ID Number Act—the 'tax, welfare and disasters' card and number (2013)

In 2013 Japan has again legislated for a new ID number, to be allocated to all residents, Japanese or foreign, and a photo-ID card with an integrated circuit (IC) chip (for which a person must apply). The Act on Use, etc. of Numbers to Identify Specific Individuals in Administrative Procedures ('ID Number Act', previously known as the 'My Number Act'), was enacted in 2013 and is planned to be operative from January 2016. The government claims that the number is to be used for only three purposes, namely social welfare, taxation, and disaster damage[27] prevention. However, the Act's definition of these permitted uses gives them a very expansive interpretation, allowing a very broad (but finite) range of 'administrative work' to include uses of the ID number.[28] Although the content of the card is to be defined by regulations, there does not seem to be provision for further expansion of uses by regulations. The Act requires that expanded uses be considered after three years, including insurance, mortgage, and health care uses by the private sector, but the government has postponed this reconsideration until October 2018. The potential—in fact, likelihood—of 'function creep' is therefore built into the legislation, but its extent remains to be seen. Although there appear to be limits on

private sector use of the number, there is little in the legislation to prevent production of the card from becoming de facto compulsory, and little which defines how the 'back-end' network and databases will operate.[29] There is also little reason to expect that the Commission set up by the Act to prevent abuses (see section 2.3 of this chapter) will prevent the system's expansion. There is opposition in Japan to the system, including fears that the private sector will obtain access to the system after its expansion, and that it was enacted without serious debate because of pressure on all political parties to enact a massive and wasteful public works programme to deliver windfall profits to the IT industry.[30] Even supporters of the ID number concede that 'many risks abound',[31] but the question is whether it will lead to Japan becoming a more repressive society through a comprehensive bureaucratic surveillance system with private sector uses.

2.2. Legislative structure

Japan's complex legislative structure is based on three main laws related to the protection of personal information, plus ancillary legislation and administrative documents, giving at least nine major sources of law.

The data privacy Acts of 2003

There are three main Acts, all enacted in 2003. Two further minor Acts deal with aspects of administrative systems. **(p.234)**

(1) The Act on the Protection of Personal Information 2003 (PPIA) is the key legislation setting out basic principles and applying them to both the public and private sectors.[32] It says little about the means by which the principles will be enforced.
(2) The Act on the Protection of Personal Information Held by Administrative Organs (PPIHAOA) updates and supersedes Japan's original 1988 public sector privacy Act, which originally governed only the use of personal information in computerized files.[33] The 2003 Act governs paper-based data as well, and also establishes new criminal provisions for government officials who leak personal information without proper justification.[34]
(3) The Act on the Protection of Personal Information Held by Incorporated Administrative Agencies (PPIHIAAA) applies similar principles to incorporated administrative agencies.[35]

Government policies and ministry guidelines

There are three further key legislative elements at the central government level. The Cabinet Order on the Enforcement of the Act on the Protection of Personal Information, revised in 2008 sets out enforcement guidelines.[36] The Basic Policy on the Protection of Personal Information is required by article 7 of the PPIA, and sets out the 'basic direction', and the 'basic matters' to be taken by the state, local public bodies, independent administrative agencies, and 'entities handling personal information'. The Basic Policy was also revised twice, once in 2008[37] and again on 1 September 2009.

Most important in practice are the guidelines set by each ministry, of which at least 40 guidelines[38] have been established in 27 fields.[39] The fields cover quite specific industry sub-sectors.[40] 'Though these guidelines are not binding [on businesses]…most companies accept and abide by the rules.'[41] The issuing of such guidelines is authorized and required by the PPIA in articles 8 and 6(3) (in relation to handling sensitive data). Article 7(1) of the 'Basic Policy' 'requires the government to provide a basic policy concerning the protection of personal information and to attempt consistent enforcement of the measure to secure its protection', and that each minister should enact or revise their guidelines for each business domain.[42]

(p.235) However, the guidelines differed so much in style and wording that in mid-2008 the Cabinet Office established a standardized guideline, and each ministry was then required to revise its guidelines in light of this.[43] This took the form of the Government issuing a 'mutual agreement' (*mo-shi awase*) among the relevant ministries to harmonize the then 37 ministerial guidelines then in place, according to a common policy and form attached to the 'mutual agreement'.[44] The Ministry of Economy, Trade and Industry (METI) Guidelines of 2007[45] were regarded as 'arguably the most widely applicable of the ministerial guidelines due to METI's broad administrative purview'[46] and were further revised in light of the 'mutual agreement'. In 2008 METI organized a study committee, the 'Personal Information Study Group' and released revised guidelines in 2009.[47] Shimpo states that '[t]he characteristics of the METI guideline that distinguish it from other guidelines are that it provides (1) a clarification on the wording of the Act (detailed instructions on how the basic requirements of the Act may be achieved), (2) supplemental pragmatic suggestions for implementation and enforcement (including many examples and cases, particularly in relation to the security obligations under article 20), and (3) a model on

which other ministries can base their guidelines'.[48] In his view '[t]he main purpose of the revision of the METI guideline in 2009 is to achieve its closer correspondence to the intentions of the Act and correct any misunderstandings. Moreover, the revision responds to myths and overreactions to the Act.' The main changes in the 2009 METI guidelines are referred to later as they become relevant.

Municipal laws

Local governments had issued personal data regulations in Japan since the early 1970s,[49] and from the early 1980s the OECD privacy guidelines became the model for local government regulations. The 2003 national legislation assumed that local governments would establish their own regulations, and by April 2006, all 1,742 current local governments had done so.[50] This adds a further level of complexity to Japan's data privacy laws.

2.3. The development of a data protection authority (2007–2014)

Since the new Acts of 2003 there has been a complex series of reports by various committees on their operation and proposals for reform, often phrased in opaque terms. Most discussion and criticism has centred on the absence of any national data protection authority, and many observers agree that the 'biggest problem of the Japanese privacy **(p.236)** regime is the lack of an independent supervisory authority'.[51] As well as hampering the effective operation of the Act, because of lack of central coordination, this absence has complicated Japan's participation in international privacy organizations.

Quality of Life Council report 2007 and Consumer Commission report 2011

The Panel on the Protection of Personal Information under the Quality of Life Policy Council established by the Cabinet Office carried out a review[52] of how the PPIA was operating, as required by article 7. This first significant 'official critique' of the operation of the Japanese law, did not recommend specific legislative changes, though it was critical of the operation of the Act on some points. It concluded that 'it is reasonable to maintain the system in which the relevant minister holds sway', but that the creation of an independent authority was 'a medium or long term task in view of compatibility with international practices'.[53] In 2009 responsibility for the PPIA was transferred from the Cabinet Office to the Consumer Affairs Agency,[54] and a law reform investigation into the PPIA was transferred to the Consumer Commission. The Commission set up an investigatory board, the 'Personal Information Protection Expert Committee' which reported[55] in August 2011. Although almost all its conclusions were only that certain matters 'had to be examined', but with many implied criticisms of the current legislation, the report appeared to recommend an independent supervisory organization to enforce the PPIA, and that the data protection authority for tax and welfare information then under consideration by the government (which became the Specific Personal Information Protection Commission (SPIPC), discussed next) should have the power to manage complaints from data subjects concerning the handling of any personal information, not only complaints concerning the number system. The approach taken in this report has eventually prevailed. Otherwise, the report recommended reconsideration of many key points on which the PPIA has been criticized, but rarely gave clear recommendations.

Specific Personal Information Protection Commission (SPIPC), 2013

As a result of the passage of the ID Number Act, the Specific Personal Information Protection Commission (SPIPC) is established from 1 January 2014, comprising a chair and six members (three full time). They are appointed by the Prime Minister with the consent of both houses of the Diet, for five years, and are required and authorized to act independently.[56] The SPIPC is the first permanent and independent body involved in data privacy in Japan. Its initial functions are limited to matters concerning the operation of **(p.237)** the new tax and social security numbering system (previously proposed to be called 'My Number'), so it is not yet a data protection authority with the scope that a data protection authority (DPA) normally has. A requirement of the new Act is that the government must consider whether the scope of supervision in data protection issues should be expanded, taking into account international developments, within a year of the Act coming into force.[57] This function has now been overtaken to some extent by the announcement of 20 December 2013 (discussed in the following section), but the SPIPC may possibly make a contribution toward the development of a more general Data Protection Authority in Japan before it is superseded.

The SPIPC can give 'guidance and advice regarding specific personal information handling' to 'business operators' using the ID number (and, it is assumed, to the administrative agencies who are its main users). It can make inspections, give opinions to the Prime Minister, and an Annual Report to the Diet. Individual data subjects are able to make complaints to the Commission. It does have powers to make recommendations concerning violations of relevant Acts (involving the ID Number Act), and to give orders if they are not followed

(and to skip the recommendation stage if urgent orders are needed). Failure by business operators to follow such orders constitutes an offence, but only the competent ministers have power to take enforcement actions. It seems that these recommendations and orders can be given to agencies as well as to 'business operators'. The problem with this model of ministerial enforcement of current data privacy legislation is that the ministries have given only a handful of enforcement orders since the legislation commenced (see section 8.1 of this chapter).

Will this independent Commission be any different? The main limitation on the Commission, as its name suggests, is that it has no functions at all in relation to data privacy issues which do not involve the use of the ID number systems, or where the use of the ID number is not a relevant part of a complaint. Of course, after 2016 the uses of the ID number may become ever greater, and an expanded SPIPC (or its successor) could become part of the legitimization of that expanded surveillance. For the purposes of this chapter, there is little more that can be said about the SPIPC, until it becomes clearer as to how it will operate. However, other than its limited scope, it does have most of the usual functions and powers of a normal DPA.

A comprehensive DPA post-2014?

In December 2013 the Japanese government announced its intention to make major reforms to Japan's data privacy laws (see section 10.3 of this chapter). The most important proposed procedural reform is the establishment of an independent supervisory authority (DPA or Privacy Commissioner), which will largely supplant both the new SPIPC (the ID number Commission) and (possibly) the ministerial-based enforcement system. Administrative sanctions and criminal penalties may be enforced by this DPA. The application of the DPA enforcement powers within the public sector may also be addressed. This supervisory authority will be established as an independent authority (called an 'article 3' body),[58] but beyond that its proposed powers and functions are still vague. **(p.238)**

3. Scope of the PPIA

This section now turns to a detailed examination of the Act on the Protection of Personal Information 2003 (PPIA) and the corresponding Acts concerning the public sector (PPIHAOA) and incorporated administrative agencies (PPIHIAAA).

3.1. 'Personal/information' regulated

The PPIA defines 'personal information' as 'information about a living individual which can identify the specific individual by name, date of birth or other description contained in such information (including such information as will allow easy reference to other information and will thereby enable the identification of the specific individual)'.[59] However, 'personal data' is restricted to 'personal information constituting a personal information database',[60] and is therefore limited to systematically organized computer-retrievable data and other data allowing retrieval (see below). The size of such a database also has implications for the applicability of the PPIA (see below). 'Retained personal data' is 'personal data' over which the data controller has the authority to disclose, correct, add, delete, discontinue the use of, or discontinue the provision to third parties (essentially all data controlled by an entity), subject to exemptions which may be specified by a cabinet order.[61] There are similar definitions in the PPHAOA.[62]

The PPIA only applies to 'information about a living individual' and so does not apply to legal persons or deceased persons. However, in one case a company continued to send direct mail to the address of the family of a young man who had recently died. The family requested the company to stop the mailings, but the company said it was only willing to receive such a request from its customer, disregarding the fact that he was deceased. The National Consumer Affairs Centre of Japan (NCACJ) advised that the Act's references to a 'living individual' in the definition of 'personal information', would be taken to refer to the living relatives of a deceased person, with personal information of the deceased now being personal information about them.[63]

3.2. Entities regulated and exempted—business operators and processors

The overall legislative scheme gives comprehensive coverage to both the public sector (including local government) and the private sector. In the PPIA private sector bodies are referred to as 'a business operator handling personal information',[64] which is any 'business operator using a personal information database, etc. for its business', but from the definition of which state and local public bodies and independent administrative agencies have been excepted (as they are covered by other legislation). The PPIA therefore covers most businesses in the private sector, subject to the significant exceptions discussed below. However, it will only cover individuals in relation to those actions where they are acting as a 'business operator'. The PPIHAOA

defines 'administrative organ' broadly in relation to central government agencies.[65]

(p.239) The PPIA only applies to 'business operators', so an individual acting in a purely private or social capacity who uploads information about other individuals onto a social networking site, or onto any other Internet platform (web pages, blogs, email lists, etc.) will not be bound. If individuals are held to be acting in a business capacity in loading information onto any Internet platform, they will still be exempt from the PPIA because of the 'small business' exemption (see below), unless their 'personal information database' identifies more than 5,000 persons.

A 'personal information database' requires the information contained to be 'systematically arranged in such a way that specific personal information can be retrieved by an electronic computer' or designated by cabinet order even though it is not subject to electronic retrieval.[66] The Cabinet Order adds 'a set of information systematically arranged in such a way that specific personal information can be easily retrieved by organizing personal information contained therein according to certain rules, and has a table of contents, an index, or other arrangements that aids in retrieval'.[67] Common examples of a personal information database include a searchable archive of email messages and a rolodex of business cards. In contrast to the rolodex example, a drawer filled with disorganized business cards would not constitute a personal information database because it is not organized for searching.

The 'small business' exemption

In the PPIA, the definition of 'a business operator handling personal information' exempts 'Entities specified by a cabinet order as having a little likelihood to harm the rights and interests of individuals considering the volume and the manner of use of personal information they handle'.[68] This has been interpreted to allow a 'small business exemption', and the Cabinet Order exempts businesses with a personal information database which does not identify more than 5,000 individual persons. It is not known exactly what percentage of Japanese businesses this has the effect of excluding from the operation of the PPIA, but it is often said that the number 5,000 was chosen so that a majority of Japanese companies were exempt and thus discontent with the law was alleviated.

This is a particular problem for individuals dealing with many Japanese companies because they are not in a position to know whether the business holds a personal information database of the requisite size. The number of employees of a company does not indicate whether it will be covered by the PPIA, and there is no provision for including companies that trade in personal information but have a smaller database. On the face of the PPIA, such 'exempt small businesses' do not retain any minimal privacy obligations such as security or providing access on request, they are simply in the 'privacy free zone'. However, the Quality of Life Policy Council reported[69] that the actual administration of the PPIA is more complex:

> Of 35 guidelines for the protection of personal information covering 22 business sectors in total, 14 guidelines obligate small entities to perform certain duties, 17 require that they make an effort to perform certain duties, and four exclude them from the definition of a business entity handling personal information (as at 31 May 2007).

They therefore concluded that the current practices were 'appropriate at present'.[70] Third party location information (e.g. telephone directories or car navigation systems) are not **(p.240)** included in the calculation of 5,000 addresses, and they recommend that 'widely distributed name lists' should also be excluded.[71] These have been excluded by an amendment made by cabinet order.[72]

Other exemptions—media, literary, educational, religious

The following categories of organization are also excluded from the PPIA's operation:[73] media/press organizations and professional journalists, for the purpose of journalism; entities conducting 'literary work'; educational organizations, for 'academic studies'; religious organizations for religious activities; and political organizations for political purposes. However, despite falling outside the privacy principles in chapter 4, these entities:

> must endeavor to take by themselves the necessary and appropriate measures for controlling the security of personal data, and the necessary measures for the handling of complaints about the handling of personal information and the other necessary measures for ensuring the proper handling of personal

information, and must also endeavor to publicly announce the content of those measures concerned.[74]

The word 'endeavour' does not create an obligation that can lead to a breach of the Act, as it is not a prescribed duty.[75] In the Japanese context, this could be regarded as an example of 'even softer' law, but it is better than the exemptions being complete.

The position of processors (trustees)

Disclosures to processors (called 'trustees' in the PPIA) do not require consent, unlike disclosures to third parties,[76] because there is an exception for trustees.[77] Disclosure to a trustee (processor), requires that the data controller (business operator) must 'supervise' to ensure 'security control' of the data.[78] This is only appears to be a duty to supervise, not the imposition of vicarious liability on the data controller. Vicarious liability for the trustee's actions may arise, however, if the trustee comes within the definition of an agent under Japanese agency law,[79] and this will often be the case.

Whether the processor (trustee) is directly responsible for any breaches of the PPIA by them while they are controlling the data, depends on the definition of 'a business operator handling personal information' which requires that it be 'using a personal information database etc for its business'. If the processor is using the database for 'its business' and not only for the controller's business, then it must comply with the PPIA. Where a data controller has exercised due diligence in choosing a processor, and the law of agency does not impose liability on the controller (e.g. where the processor has exceeded its authority), it may be necessary for a data subject to take action against a processor.

(p.241) 3.3. 'Overreactions' and proposed further exceptions

There have been concerns about 'overreactions' to the legislation, with governments and businesses claiming that some information previously provided to the public for good reasons (or at least by customary practices) cannot now be provided without breaching the PPIA.[80] Which such perceptions are justified, and which are mistaken, is debated. Case claimed that the 'overreactions' resulted in part from 'the generality of the [Act] and its application to all personal information without exception'.[81] He cites a list of distributors of a product which included the name of the key contact at each distributor as an example of the type of information which technically was in breach of the PPIA, and school alumni lists as an example of information customarily circulated in Japan. It seems that 'the response of many, in the face of uncertainty over the scope of their obligations under the Act, has been to adopt an overly cautious and conservative approach'.[82]

The Quality of Life Council concluded 'Most cases of "overreaction" can be resolved if the right principles are correctly disseminated through guidelines', and that the number of such 'overreactions' was slowing.[83] It recommended some additional exceptions to the restrictions on disclosure, including where 'personal information is made public conventionally' (only in relation to government entities), where necessary for the protection of a person's safety, and where necessary in order to cooperate with government entities if an activity is in the public interest or needed for the performance of government services or 'if there is no possibility of infringement of rights or interests and there is a reasonable reason'.[84] These proposals have not yet resulted in legislation.

4. Japan's data protection principles

The Japanese government's privacy reforms announced in December 2013 include proposed reforms to the substantive principles and rights in the PPIA which are significant and may address some of the main criticisms that are made of those aspects of Japan's law in the rest of this chapter.[85] The few details known are mentioned in this chapter where relevant, and summarized in the conclusion to the chapter.

4.1. General considerations

The data protection principles are set out in 17 articles of the PPIA,[86] 'Duties of entities handling personal information etc'. However, they are considered to 'set minimum requirements only [and] the Basic Policy requires that each Ministry establish or revise guidelines depending on actual conditions of each business sector'.[87] As noted previously, by 2008 the guidelines (now 40) differed so much that the Cabinet Office established a standardized guideline, and each ministry then revised its guidelines in light of this template, though they still differ considerably.

(p.242) 'Consent'

'Consent' is not defined in the Acts. It is referred to in arts 16(1) and 23(1) of the PPIA by words such as 'without obtaining the prior consent' which give no indication as to whether consent must be express or may be implied (including by failure to opt-out). The METI Guidelines provide that 'consent' can only be obtained once the data subject has been given a reasonable opportunity to understand to what he/she is consenting.[88] It is desirable for consent to be evidenced by a positive action such as an oral or written statement, or checking a box on a website. However, implied consent might be recognized as valid on a case-by-case basis in view of the circumstances.[89] Minors lack the capacity to consent, but their attorney-in-fact may consent on their behalf.[90] The Financial Services Agency (FSA), *Guidelines for Personal Information Protection in the Financial Field* also state that in principle, consent should be obtained by a written form, not oral.[91]

4.2. 'Finality'—use and disclosure limitations

Statements of purpose

The 'purpose limitation principle' or 'finality principle' is stated most generally in relation to businesses in article 15 of the PPIA:

> (1) When handling personal information, a business operator must specify the purpose of utilization of personal information (hereinafter referred to as the 'purpose of utilization') as far as possible.
> (2) A business operator must not change the purpose of utilization of personal information beyond the scope which is reasonably considered to be duly related to the purpose before the change of utilization.

Clause (2) in effect allows secondary uses (including disclosures) that are 'reasonably considered' to be 'duly related to' the original 'purpose of utilization', which must be specified 'as far as possible'.

Clause (1), in the opinion of the Quality of Life Policy Council, 'asks for detailed specification of the Purpose of Utilization as far as possible instead of abstract or general specification thereof'.[92] The Council notes that 'The Guideline for the Business and Industry Sector gives as a model example "the delivery of products, information on new products, and related after-sales services in the field of XX business"', and that 'it is widely accepted that "XX business" be specified using the term of middle or smaller grouping in the Standard Industrial Classification for Japan'.[93] The METI Guidelines also emphasize that abstract statements of purpose of use are unacceptable.[94]

When public sector bodies 'directly acquire' personal information that is recorded in a document, they must 'clearly indicate the purpose of use to the individual concerned in advance', with a number of exceptions.[95]

(p.243) Use restrictions—private sector

Personal information may not be used beyond the scope necessary for the achievement of the purpose of utilization specified under article 15, without the prior consent of the person concerned.[96] This includes secondary uses that are 'reasonably considered' to be 'duly related to' the original 'purpose of utilization' under article 15(2). Standard exceptions are provided in article 16(3) for uses (i) based on Japanese laws and regulations; (ii) where necessary for protection of life, body or property (and consent is difficult to obtain); (iii) where necessary for public health or children's interests (and consent is difficult to obtain); and (iv) where necessary for cooperation with governments or their representatives carrying out law, and obtaining consent is likely to impede that. Corresponding exemptions from providing notice are provided in article 18(4).

Where the purpose of use is changed to something else 'duly related', the data controller 'must notify the person of the changed purpose of use or publicly announce it'.[97] Individual notice can therefore be avoided by public announcement on websites or otherwise. In addition, various exceptions to any requirements of notice or public announcements are given where interests would be harmed or the purpose of use is considered to be 'clear' in light of the circumstances of acquisition.[98]

For example, an insurance claimant received a telephone call from an acquaintance who was an employee of a life insurance agency but who was not involved in processing insurance claims. This acquaintance had knowledge of details of the claimant's serious disease relating to a claim for insurance benefits derived from his policy, even though the claimant had requested other staff in the insurance agency not to divulge any information about it. NCACJ contented itself with concluding that the acquaintance was not a 'third party' under the Act (so there was no a disclosure involved), but reached no conclusion about whether, in fact, the acquaintance's access was a permitted 'internal use'. It merely said 'the handling of personal information by an employee of a quite separate

division within the company may not be lawful'.[99]

Disclosure restrictions and exceptions to them—private sector

As a general rule, a data controller must not provide personal information to a third party without obtaining the prior consent of the data subject.[100] The same restrictions and exceptions as apply to use of personal information, apply to its disclosure.[101] This would seem to include any disclosures 'reasonably considered' to be 'duly related to' the original 'purpose of utilization' under article 15(2), but it is not clear that reliance is placed on this to expand the scope of permissible disclosures.

The most significant exception to the disclosure restrictions is in article 23(2), which allows businesses to disclose personal information to third parties despite article 23, provided they 'notify' the data subject that they are going to do so, including giving the data subject notice that he or she can 'opt-out' of such disclosure to third parties ('discontinued at the request of the person'). The 'notification' must be 'in a readily accessible condition for the [data subject]' (such as by posting details on a readily accessible website), and must specify that the information will be used to provide it to a third party, the items of information so provided, the means of provision, and that discontinuance may be **(p.244)** requested (i.e. an 'opt-out'). No disclosure of the identity of the third party is required, or their location. No consent to disclosure is then required. Ito and Parker conclude that 'the opt-out exemption is, on the whole, easily satisfied and makes it possible for companies to sell or otherwise transfer personal data to third parties without consent'.[102] This will also include transfers to third parties overseas. Some ministry guidelines such as the 2009 METI Guidelines state that business must not utilize article 23(2) if they have not provided notice that they might do so when collecting the information.[103]

An example is where an Internet auction site required its registered users to display their name and address on the site, claiming this was a legislative requirement and threatening to suspend the membership of those who did not do so. The user claimed he was taking part in auctions as an individual, not a dealer, and that this obligation only applied to dealers, so publishing his address breached the PPIA. NCACJ found no problem with the auction companies' actions because they were not obliged to obtain consent for uses authorized by law, and they had complied with other provisions by giving notice in advance of their intended use.[104]

Additional exceptions are made for outsourcing, mergers of businesses, and joint ventures,[105] and have been summarized as being satisfied when any of the following types of provision of data occurs:[106]

> (1) the disclosee qualifies as a delegatee, with whom the discloser executed a proper agreement satisfying requirements suggested by guidelines;[107]
> (2) the data is provided due to a merger, etc.[108] The 2009 METI Guidelines have established that a contractual agreement constitutes an offer for the legal disclosure of individual data for the purpose of succession of a business; when data security issues (purpose of use, operation method, leakage, etc.) interfere with the business succession process, the safety management measures must be observed in the absence of a contractual agreement (that is, the person does not agree to disclosure of his/her information);[109] or
> (3) the disclosee qualifies as a joint user.[110]

Disclosures to joint users must also be notified to data subjects, by readily accessible means, with details of the scope and purpose of the joint use and who will be responsible for the data, though the level of detail required is uncertain.[111]

Use and disclosure restrictions and exceptions to them—public sector

Public bodies cannot use or disclose retained personal information 'for purposes other than the purpose of use'.[112] There are six exceptions: data subject consent; necessity for executing affairs under the agency's legally authorized jurisdiction, and where reasonable; similarly for disclosures to other government entities; for statistical and research uses; for uses 'obviously beneficial to the individual concerned'; and where other 'special grounds' justify disclosure. These exceptions do not apply if the use or disclosure 'is likely to cause unjust **(p.245)** harm to the rights or interests of the individual concerned or a third party'. Other laws and regulations can also justify use or disclosure. These grounds for other uses are exceptionally broad, more so than in most other jurisdictions.

An administrative organ may not change the purpose of use 'beyond the scope in which it is reasonable to find

that the changed purpose of use is appropriately relevant to the original purpose of use'.[113] The implication is that administrative organizations can change their purposes to include others 'appropriately relevant' where this is 'reasonable'.

4.3. Collection limitations

Private sector

There is no explicit limitation of collection of information to that which is necessary for carrying out the purpose of utilization specified under article 15, but that may possibly be implied by article 16 which limits the use of information to that which is necessary for the achievement of the article 15 purpose. The requirement to give notice of purpose can be avoided by a public announcement of the purpose of collection,[114] but will generally have to be given to individual data subjects in advance of collection of personal data in written agreements, including collection by electronic means.[115]

'A business operator handling personal information shall not acquire personal information by a deception or other wrongful means.'[116] For example, where an employee of a direct marketing company acquired names and addresses by visiting an apartment house, taking letters out of mailboxes so as to copy details of the addressees, then putting the letters back, the NCACJ advised that this was a violation of article 17, and so the individuals could request deletion of their information. A list broking company encouraged students sitting a university entrance exam to provide copies of their class lists, in return for a voucher worth about US$30. NCACJ considered that, although a company is prohibited from disclosing third party personal data, an individual is not so prohibited. NCACJ merely said it was a matter for argument whether acquiring such information from minors might constitute obtaining personal information by fraudulent or dishonest means.[117] The 2009 METI Guidelines set out examples of where information is acquired improperly, which Shimpo explains were 'added to cover situations where the individual information concerned is acquired improperly, even though it was possible to obtain legally, if the acquiring party is aware of the violation of the third party's offer limitation or of the fraudulent procurement ("on the side") where individual information was acquired…illegally or more easily than legal means would permit'.[118]

In the public sector, there is no express restriction on collection by wrongful means in the PPIHAOA, but this would probably be implied by general administrative law requirements. The PPIHIAAA requires 'proper acquisition'.[119] Public sector bodies may only retain personal information 'when the retention is necessary for performing the affairs under its jurisdiction provided by laws and regulations'.[120] This is, in effect, a limit on collection.[121]

(p.246) ### 4.4. Data quality obligations

PPIA article 19 (Maintenance of the Accuracy of Data) provides that 'an entity handling personal information must endeavour to maintain personal data accurate and up to date within the scope necessary for the achievement of the Purpose of Use'. Public sector bodies 'shall endeavour to maintain the retained personal information consistent with the past or present facts within the scope necessary for the achievement of the purpose of use'.[122] The wording is different but the meaning seems to be the same.

4.5. Data security obligations

Article 20 (Security Control Measures) of the PPIA provides that 'an entity handling personal information must take necessary and proper measures for the prevention of leakage, loss, or damage, and for other control of security of the personal data'. The Quality of Life Policy Council discusses various guidelines and benchmarks[123] but gives little concrete indication of any more specific security practices or policies than the general statement in article 20. The frequency and extent of large-scale data leakages in Japan indicates that good security practices are far less than universal. The METI Guidelines on security cover organizational security control measures; personnel-related measures (e.g. non-disclosure agreements, training); physical security control measures; and numerous technical security control measures.[124] Public sector bodies are required to take 'necessary measures for the prevention of leakage, loss or damage and for the proper management of retained personal information'. This obligation also applies when they entrust an individual or business operator with the information.[125]

The PPIA requires businesses to exercise appropriate supervision over employees[126] or contractors or 'trustees'[127] who handle personal data. The Basic Policy states it is important for businesses and contractors to

have a service agreement by which the contractor is required to take security measures. Some members of the Quality of Life Policy Council were of the opinion that the fact of outsourcing personal information should be made known to consumers, whereas others were uncertain of the practical difficulties in naming contractors.[128] The possibility of disclosing the fact of outsourcing but not naming the contractor was not canvassed.

Data breach notification

One of the most important changes in the 2007 METI Guidelines was to require certain responses in case of a data leak or other breach of the PPIA.[129] According to a clarification in the 2009 METI Guidelines '[i]t is permitted to report to the competent minister once a month in case of information leaked through wrongful transmission via facsimiles and mail'.[130] The guidelines refer to taking preparations to provide information to persons affected by a leakage accident, the need to contact the person to prevent secondary damage, and the desirability of making details public as much as possible (while specifying exceptions to where that is necessary).

(p.247) 4.6. 'Openness' concerning practices

The objective of openness of personal data record-keeping practices is therefore achieved by different means in the private and public sectors. PPIA article 24 (Public Announcement of Matters Concerning Retained Personal Data, etc.) applies the OECD's 'openness' principle. Businesses must be prepared to advise any person of the purpose of utilization of all retained data (with some exceptions), and the procedures for accessing it. There is however, no requirement to register details with any government body. In contrast, where an administrative organ intends to retain a personal information file, it must notify the Ministry of Internal Affairs and Communications (MIC) in advance, with details of the name of the file, purposes of use, routine disclosures, and scope of individuals covered by it (among other matters).[131] These details are required to be collated by an administrative organ into a Personal Information File Register, and published.[132] There are numerous exceptions.

4.7. Deletion of data

There is no general obligation on businesses to delete data after it has ceased being of use. However, individuals can request (not require) that retained personal data be deleted.[133] In contrast, public sector bodies may only retain personal information 'when the retention is necessary' (as discussed) and the purpose is specified 'as much as possible' on retention, and 'shall not retain personal information beyond the scope necessary for' the specified purpose.[134] It is therefore implied that deletion is required when the purpose is complete.

A complainant was required by a beauty salon, in order to obtain treatment from them, to include in the service agreement form her name, address, and blood type, and to submit it with an impression of her thumbprint as evidence of identification. Afterwards, she asked the shop to delete her information, but it refused, claiming that the information was necessary for its business. The NCACJ doubted the legality of this but merely advised the complainant that it would first have to request the company's purpose of retention. A direct marketing company refused to accept requests for deletion from its mailing list unless they were accompanied by a copy of the individual's driver's licence and a copy of the individual's resident registration certificate, ostensibly because of a ministerial guideline saying 'one must not delete or cease using an individual's personal data without permission'. The NCACJ recommended that, when a deletion request is made, the company stop requesting such public documents, and only request the membership number and ID that it assigned to registrants. The company agreed to do so. This is a rare example of a NCACJ complaint report including a result.[135]

5. Areas of special concern—coverage in Japan

Japan's laws rarely go beyond the most basic provision of the OECD Guidelines. There are no special provisions in the PPIA, or in the public sector legislation, concerning data matching. Few topics considered significant by the EU are covered.

(p.248) 5.1. Processing of sensitive data

Article 6 PPIA provides, by a circular definition, that the government will take special measures to protect 'personal information whose proper handling is especially strictly required'. This sensitive information therefore remains undefined, and no additional obligations are imposed on data users merely by this provision. Automated decision-making systems could be subject to special regulation under article 6 because of the 'method of use' requiring 'special measures' to protect rights, but this has not occurred.

Legislation regulating businesses in particular fields (e.g. medical care, finance/credit,[136] telecommunications)

has been amended to include stronger confidentiality provisions, particularly the law concerning money-lenders.[137] Ministry guidelines also give special treatment to 'sensitive' data. The METI (2007) and FSA (2007) Guidelines have provisions on special treatment of sensitive information. According to the FSA guidelines, sensitive information means information regarding political views, religion, union activities, race, family origin and registered domicile, health care, sexual activities, and criminal records.

5.2. Use of publicly accessible data (including 'public registers')

None of the legislation deals explicitly with public registers (publicly accessible registers of personal information held by government agencies), and whether the rules concerning use, disclosure, security, deletion, etc. apply to re-use of information from them. It seems that where a business operator uses such information, the PPIA may apply.

The PPIHAOA will exempt information contained in at least some public registers from its scope. 'Retained personal information' is defined in article 2(3) as limited to personal information recorded in 'administrative documents' as defined in article 2(2) of the Act on Access to Information Held by Administrative Organs. Article 2(2) provides *inter alia* that 'Administrative Document' means a document 'held by the administrative organ concerned for organizational use by its employees', but that this excludes '(i) Items published for the purpose of selling to many and unspecified persons, such as official gazettes, white papers, newspapers, magazines, and books'. So a public register where there is a fee for access is clearly exempt from those parts of the PPIHAOA applying to 'retained personal information'. But where there is free access (or a zero yen fee), will it be exempt? Whether a public register would have to comply with the requirements of the PPIHAOA therefore depends upon the interpretation of this definition.

However, the obligations in the PPIHAOA that apply to 'personal information' (as distinct from 'retained personal information') such as the obligation to indicate purpose of collection,[138] or on employees not to disclose without justification,[139] will still apply to information collected for inclusion in a public register. Before the information is published it will be 'retained personal information', and therefore subject to the obligation to not change the purpose of use or disclosure,[140] except in compliance with that section. The purpose of 'including in a public register' may therefore have to exist at the time of collection. An administrative organ cannot use article 9 to impose conditions of use on a recipient of information from a public register, because by that stage the information is not 'retained personal information'.

(p.249) ### 5.3. Direct marketing 'opt-out'

There are no special provisions in the PPIA concerning direct marketing, but the provisions concerning restrict third party disclosures in article 23(2) and (3) apply. This means that a company can, after collection of personal information, put a notice on a website (i.e. 'put those matters in a readily accessible condition for a person') stating that it is changing the purpose of use of the information to include direct marketing, and stating what information will be provided to third parties and 'the means or method of provision', and that the data subject can request this provision be stopped (i.e. can 'opt-out'). There is no requirement, in contrast to other jurisdictions, that the data subject be given a readily accessible means of opting out when they receive direct marketing communications, either on each occasion or the first occasion. There is separate legislation concerning email spam and telemarketing,[141] but there is no Do Not Call list.

6. International data transfers from Japan

Japan does not have any specific data export restrictions. It relies on its proposed engagement in APEC's cross-border recognition system and the PrivacyMark System,[142] as well as the general rules for transfer of personal information to third parties. See the discussion of territorial scope at section 6.1 of this chapter and disclosure limitations at section 4.2 of this chapter for the full implications of these other aspects of Japanese law for data exports.

The position can be summarized as follows. Disclosures to foreign processors (as with other disclosures) require consent,[143] but this can be avoided by the provision of a 'readily accessible' notice allowing data subjects to opt-out of the disclosure.[144] The notice need not even state that the disclosure is in relation to an export to overseas. A qualification of this is that where disclosure is to a trustee (agent), the exporter must 'supervise' to ensure 'security control' of the data. This is only a duty to supervise, not the imposition of vicarious liability on the exporter. The Japanese law does not have extraterritorial application to entities that do not have a presence in Japan (except where the foreign recipient is a trustee of the Japanese exporter). If the

foreign recipient has a presence in Japan, it must comply with Japanese data protection law. As a result, if data is validly disclosed under article 23 to a foreign third party (not a trustee) with no presence in Japan, neither the Japanese transferor nor the foreign recipient will be liable.

6.1. Extraterritorial scope

The PPIA does not apply extraterritorially to entities that do not have a presence in Japan.[145] Therefore, a Japanese data controller that overcomes the general prohibition of **(p.250)** personal information transfers to third parties (see section 4.2 of this chapter concerning disclosure restrictions) can transfer personal information to a foreign recipient which is not obligated to abide by the PPIA. However, if a Japanese data controller provides personal information to a foreign entity and the foreign entity handles the personal information in a manner inconsistent with the PPIA, the providing Japanese data controller might be found in violation of the PPIA under some circumstances. The data controller might be found to violate article 22 (supervision of trustees) if its trustee handles the personal information inconsistently with the PPIA. Furthermore, the data controller might be found to violate article 16 (restriction by the purpose of use), article 18 (notice of purpose of use at time of acquisition), and article 20 (security control measures) if its joint user handles the personal information inconsistently with the PPIA.

In contrast to the case where the recipient of personal information is a purely foreign entity, if the recipient of a transfer of personal information has a presence in Japan and otherwise qualifies as a data controller under the definition of data controller (*kojin jouhou toriatsukai jigyousha*) in article 2(3), it must comply with the duties the PPIA places on data controllers with regard to the personal information received.

In summary, if a recipient of personal information uses the received personal information inconsistently with the PPIA, (i) the data controller which provided the information might be subject to administrative or criminal action under the PPIA, (ii) a domestic Japanese recipient that qualifies as a data controller would also be similarly liable under the PPIA, but (iii) a purely foreign recipient would not be liable under the PPIA. Even if the recipient of the personal information is not subject to the PPIA, if it mishandled the personal information, it is arguable that it might be liable to the data controller under contract law and to the data controller and the aggrieved data subjects under tort law.

An exception to the territorial limitations of the Japanese legislation is that the offences for disclosing or collecting personal information under the PPIHAOA, articles 53–55 can be committed outside Japan.[146]

7. Rights of data subjects in Japan

The data subject's rights are to notification on acquisition of personal information; to access and correction; and only in some very specific cases to object to processing (not including direct marketing).

7.1. Informing data subjects of processing

Business operators have to give an explanation of reasons to data subjects for the decisions they take in relation to access, correction or cessation of processing.[147] In the private sector, where a business operator acquires personal information directly from the person, or has acquired the information pursuant to a contract or other document from the person, they must 'expressly show the Purpose of Utilization in advance'.[148] However, when they otherwise acquire the information from a third party, they must promptly notify the person of the purpose of utilization.[149] Where the business operator changes the purpose of utilization it has the choice of notifying the person of the change, or publicly announcing it.[150] Public announcement is only an option if the new purpose of use is reasonably related **(p.251)** to the old purpose of use, in accordance with article 15. There are exceptions to these three provisions similar to the exceptions to use and disclosure without consent, and in addition where such notification is likely to harm the legitimate interests of the business, or where the purpose is clear in the circumstances of acquisition.[151] Individuals can also request notification of the purpose of utilization of information held about them,[152] and similar exceptions apply.

Notification of disclosure—outsourcing

The Quality of Life Policy Council was of the opinion that the fact of outsourcing personal information should be made known to consumers.[153] It also considered that the individuals' right to obtain access to their own data ('retained personal data') does not include details of the party who disclosed that data to the business receiving the request, in contrast with the EU position.[154] Its members were divided over whether this position should be followed in Japan.

7.2. Access and correction

Requests for disclosure of a person's retained personal data must be answered by a business 'without delay', either in full or with some information redated.[155] Charges for access must be reasonable in consideration of the actual cost of providing access.[156] Correction, addition to, or deletion of, personal information is required on request and 'on the basis of results' of investigation by the business operator.[157] There is no provision for 'the complainant's side of the story' to be added to the file where the business operator does not accept the complainant's request.

The PPIHAOA contains very detailed provisions providing a person's right to access his or her personal information held by administrative organs and the procedures to be followed.[158] It also contains very detailed provisions providing a person's right to correct his or her personal information held by administrative organs and the procedures to be followed. The PPIHIAAA has similar provisions.[159]

7.3. Objections to processing, including direct marketing

There is no general right under the PPIA to object to processing of personal information by a business and request it be discontinued or the data erased, but article 27 allows this to be requested in three cases: (i) where it is being used in violation of the article 16 purpose of utilization; (ii) where it has been acquired by deception or other wrongful means;[160] or (iii) where it is being provided to third parties in violation of article 23. The Quality of Life Policy Council was pessimistic about the effectiveness of this part of the legislation: 'Even after the enactment of the PPIA, the number of spam e-mails, random telephone sales calls, direct mails, etc. has not decreased in the slightest.'[161] Spam and telemarketing are regulated by other legislation, but the PPIA does not seem to have deterred use of the lists on which such marketing is based. The 2008 anti-spam legislation affects this in **(p.252)** relation to spam but not other forms of direct marketing. The PPIA does not have explicit provisions providing a right to opt-out of direct marketing, and it does not seem that the objection to processing provisions are an effective substitute.

There are similar provisions in the PPIHAOA whereby a person can request an administrative organ 'for suspension of use, deletion, or suspension of provision', where the administrative organ (i) has not obtained the information lawfully, retains the information in violation of article 3 obligations to delete it, or uses it in violation of its article 8 purposes of use.[162] The Act sets out detailed procedures.[163]

8. Enforcement in Japan

Because there is as yet no general DPA in Japan, enforcement is primarily as a result of supervision by ministries, with very little role for civil actions, and a very questionable role played by trustmarks.

8.1. Public sector—complaints and enforcement actions

In Japan's public sector, there is considerable evidence of enforcement of the security principle, and well-used procedures for citizens to access their own files, but little evidence of other privacy principles being enforced. Those principles may be generally observed in the public sector, but there is little to indicate how exceptions are dealt with.

The enforcement status of the public sector legislation is checked by the government every year, based on article 49 of the PPIHAOA and article 48 of the PPIHIAAA.[164] The 2011–12 report[165] found 498 security breaches by administrative organs, resulting in 130 disciplinary punishments and one criminal penalty, and 2,006 breaches by incorporated administrative agencies, resulting in 49 disciplinary punishments. There are no similar statistics for breaches not related to security.

Criminal penalties

Under the public sector legislation there is no general provision for criminal penalties, but where employees or former employees wrongly disclose or collect personal information under certain circumstances, criminal penalties can result,[166] even when the offence is committed outside Japan.[167] The Act does not prescribe offences which are committed by recipients of such information.

Appeals to the Review Board

The Act authorizing the establishment of the Information Disclosure and Personal Information Protection Review Board set up procedures to ensure that access to administrative files does not cause unjustified disclosure of personal information.[168] Where decisions by **(p.253)** administrative organs concerning access to a person's

own record, correction, or suspension of use, are appealed against, the head of the administrative organ who is expected to decide the appeal must consult the Information Disclosure and Personal Information Protection Review Board.[169] Its 15-person membership is approved by the Diet. It has strong investigative powers. The main function of the Board is to decide whether objections by data subjects to their personal details being disclosed in the course of information access requests by third parties, should be upheld. Such 'reverse-FOI' procedures are typical of freedom of information laws, and are aspects of privacy protection but not a key element of data privacy laws. The result of such consultation must be made known to all relevant parties including the data subjects who have objected to the disclosure of their personal information. Decisions of the Review Board (9,480 cases as of 28 January 2014) are available online.[170] There are no cases regarding the enforcement of privacy principles other than access and correction, such as security breaches or wrongful disclosure, so this is not a general data protection remedy.

Local government

Heads of local government have the same authority as a competent minister in relation to handling complaints (see section 8.3 of this chapter), and can deal with complaints concerning their own local government bodies. However, there is no evidence of such enforcement.

8.2. Private sector—complaints and enforcement action

Japan has a decentralized and extremely confusing system of dealing with data protection complaints against private sector bodies. Statistical information is incomplete, and there is no information of any significance in the form of case studies. The system is almost completely lacking in transparency. Responsible ministries occasionally issue recommendations to companies, but never take enforcement action.

Bodies able to investigate complaints

A complaint about the handling of personal information by a business may be filed with one of four bodies under the PPIA:

(i) *The business entity concerned*—A business operator 'shall endeavour' to 'appropriately and promptly process complaints'.[171]
(ii) *An authorized personal information protection organization* (APIPO)—There have been 39 organizations[172] so designated by relevant ministers under article 37. These are considered below in section 9.1 of this chapter.
(p.254) (iii) *A local government department*—Heads of local government have the same authority as a competent minister in relation to handling complaints (see section 8.3 of this chapter).
(iv) *The National Consumer Affairs Center of Japan*, including through one of the local Consumer Affairs Centres. The Basic Policy[173] requires the NCACJ to offer advice, provide training and distribute manuals, to assist 'grievance organs' such as Consumer Affairs Centres.

There are no specific provisions in the PPIA allowing persons to make complaints to an APIPO, local government department or NCACJ, or to the 'competent minister' (see section 8.3 of this chapter), nor to require that complaints are first made to the business concerned. Despite the lack of procedures or compulsory provisions, Japanese companies are known to have taken voluntary actions in some cases for the protection of personal information and to ensure transparency even though such conduct is not prescribed as a duty by any law. The Expert Committee Report (2011) gave examples of such voluntary actions.[174] Miyashita also cites one example, where Mitsubishi UFJ Securities, in relation to a data leak concerning 50,000 customers, published apologies in five newspapers and paid US$100 to each customer (a total of US$5 million), without a court order requiring this.[175]

NCACJ complaint statistics

The NCACJ prepares and distributes a 'Manual on Complaint Processing for Personal Information' and a 'Summary of Personal Information Protection-related Complaints and Responses'. No English language versions are available, but translations of the summaries have been made for the purposes of this book. Both NCACJ and the Cabinet Office collect examples of complaints, and since 2006 have been exchanging them,[176] but they are not publicly available.

The statistics show that from 2005–11, the last year for which the NCACJ has released the number of complaints,[177] the number of complaints lodged with either local governments or the NCACJ declined steadily

from 14,028 in 2005 to 5,267 in 2011. The information provided varied from year to year, but is rarely very useful in indicating what, if any, beneficial outcomes have resulted from complaints. For example, in the financial year 2009, the Consumer Affairs Agency statistics show that the principal causes of complaint were fraudulent acquisition of personal information (53 per cent), leakage or loss of data (24.8 per cent), and utilization beyond the purposes of use (14.9 per cent). The outcomes of the 8,559 complaints were 'guidance and advice (84.6%)' or 'other types of information provision (10.8%)' in 8,008 cases (95.4 per cent), and 233 (2.7 per cent) successfully mediated, with most of the rest being introductions to other institutions. Other than the relatively small number (about 35) of mediations each year, with unknown outcomes, the outcomes of the 8,559 complaints were only guidance and advice, information **(p.255)** provision and introductions, and do not involve any imposition of sanctions based on the PPIA. It does not seem that any of these complaints feed in to complaints being investigated by a ministry, so it is not obvious that any mandatory sanctions arise from complaints. Nor is any evidence available of compensation payments or other remedies for damage to individuals. How many complaints are lodged with APIPOs is not stated in these reports or elsewhere, but in 2008 it was stated that 680 complaints had been processed by APIPOs, with results unstated.

NCACJ examples of private sector complaints

The only case studies of how complaints are resolved are found on the website of the National Consumer Affairs Centre of Japan.[178] It gives summaries of 18 complaints from 2004–07[179] (of which 13 are relevant to the enforcement of the law). Since 2007 there have been no summaries published, which is of itself reason for concern. The complaint details are given only in Japanese. Unfortunately, the summaries do not include any information about how (or whether) the complaint was resolved. They seem to be only summaries of types of complaints, and the NCACJ opinion about them, not complaint outcomes, and are therefore of very limited use in assessing the effectiveness of the Act. Nevertheless they are the only information available about how the PPIA operates in practice.

An English translation and analysis of the most significant of the 18 reported cases has been published.[180] They all share the characteristic of being interesting but uninformative, and failing to indicate any enforcement action (with one exception where a business accepted the NCACJ's advice). Some of the complaints have been used earlier to illustrate issues that arise under various principles.[181] The NCACJ complaint summaries reveal little about whether this complaint system is effective, and do not constitute evidence of effectiveness. There is no indication that NCACJ ever investigates the factual issues necessary to come to a final conclusion about a complaint, so in many instances the reader is left with no idea whether there actually was a breach. When NCACJ does reach a conclusion in favour of a complainant, there is no indication whether the business concerned acted on that conclusion. In any other country, these summaries would be regarded with derision if presented by a complaint resolution body.

8.3. Actions following private sector complaints

Ministries cannot impose administrative fines. All they can do is make recommendations to businesses, or issue compliance orders (which, in practice, they do not do). Thus there can never be prosecutions for non-compliance.

(p.256) Administrative orders—enforcement actions by ministries

Under the PPIA, the competent minister (see below) 'may have' a business operator 'make a report' on its handling of personal information,[182] and the minister may then 'advise' the business operator.[183] It is not clear whether the report must be about a specific complaint, or how an individual brings matters to the attention of a minister.

When a business has violated any of the data protection provisions,[184] the competent minister may recommend that the business concerned 'cease the violation concerned and take other necessary measures to correct the violation'.[185] If the business fails to follow the recommendation, and the minister finds that 'a serious infringement on the rights and interests of individuals is imminent' it may order the business to take the measures recommended.[186] Urgent orders may be made under some circumstances without the minister waiting to see whether a recommendation will be followed.[187] The normal case is therefore a three-stage process: a request for a report by the business; a recommendation; and an order.

The 'competent minister' is 'the minister etc concerned with jurisdiction over the business of the business operator',[188] except in the case of personal information relating to employment management, where

responsibility is shared with the Minister of Health Labour and Welfare. The Prime Minister can also designate competent ministers. Each competent minister has its own jurisdiction regarding the enforcement of the law for each business sector. Therefore, complaints will be submitted to each competent minister.

In the financial year 2007, ministers collected reports from the businesses they supervised in 83 cases, but did not make recommendations or orders in any case.[189] In the financial year 2006 they collected reports in 60 cases and made recommendations in four.[190] After 2009 such collations of data were published in Japanese, but not translated into English.[191] In contrast, Japan's Financial Services Agency (FSA) has published reports concerning disciplinary action it has taken against various financial services companies, requiring remedial actions following data spills.

Ito and Parker[192] confirm that in the first five years of the PPIA there were only a small number of cases in which enforcement steps had been taken under the Act, giving as an example:

> One of the significant enforcement proceedings to date was brought against a regional bank in 2005, which resulted from the bank's loss of three CD-ROMs containing personal information about approximately 1.3 million of its customers.[193] It led to a serious rebuke by the regional Finance Bureau, and the issuing of warnings to individual bank officials. The FSA has, by far, been the most active of the government ministries. Of a total of 83 reports ordered from personal information handlers between April 2007 and March 2008, 78 were by the FSA (mostly **(p.257)** on data security measures and measures against leakages). However, no recommendations for improvement were issued during this time.

Unless evidence is available that mere requesting of a report always results in spontaneous offers of remedies where appropriate, it does not seem that ministerial supervision is playing a significant role in any system of responsive regulation here. On the contrary, there is at least one example of the ineffectiveness of public criticism where one of the largest rental DVD, CD, game and book stores in Japan has been criticized severely for data processing without permission of data subjects, and sharing data beyond the limits allowed by the PPIA, but has not changed its practices.[194]

Ito and Parker[195] consider that the Act may be somewhat effective *in terrorem*:

> the real effectiveness of the Act is that it creates for businesses a greater risk of damage to reputation. In fact, the lack of enforcement action may be attributed, in part, to the nature of Japanese society, with its complex system of business etiquette, in which reputation still carries a tremendous amount of importance. Reputation is acknowledged to be particularly important to both individuals and companies (including, to a lesser extent, foreign companies), as is rigid compliance with administrative rules. Japanese businesses would argue that data compliance issues, like other compliance issues, are taken more seriously than in other countries and that even an informal threat of enforcement will usually be sufficient to jolt a non-compliant business into action. The nature of enforcement proceedings taken against the regional bank in 2005, including the summoning of its President to appear before the local Finance Bureau, and the issue of warnings to individual bank officials, demonstrate at least some willingness on the part of the authorities to frighten companies, through their officers, into compliance with the Act.

The total number of submissions to the competent minister based on the PPIA, regarding the improper use of personal data made by entities handling personal information in 2012, was eight (compared to 16 in 2011 and 15 in the 2010 fiscal year). The adjustment of claims concerning the handling of personal information is based on articles 9 and 13 of the PPIA.

The outcomes of the competent ministers enforcing the correct handling of personal information by entities for Fiscal Years 2005 to 2012 were as follows: seven recommendations under article 34(1); the collection of 315 reports; two sets of advice were given. Since it appears there have been no orders made under article 34(2), there cannot have been any prosecutions for offences. Details of these recommendations and the circumstances in which they occurred are, in general, unknown. An enforcement recommendation is known to have been made by two ministries in relation to Google's integrated privacy policy, but it is a vague and mild recommendation of no known effect.[196]

Criminal sanctions

A breach of one of the information privacy principles is not enough in itself to attract criminal penalties under any

of the Acts. Under the PPIA there must also be a breach of a **(p.258)** ministerial order, but as noted above, no such orders have been made. A violation of a ministerial order under article 34 can result in fines up to US$3,000 and up to six months in prison, if the data controller is an individual.[197]

8.4. Individual remedies—court actions

The PPIA does not explicitly provide for individuals to obtain damages in a court for breach of its provisions, but it had been considered an open question whether it does impliedly provide such a cause of action.[198] In what has been described as 'one of the most important court cases to interpret' the PPIA,[199] the Tokyo District Court held that the PPIA did not provide a data subject with a cause of action against a data controller who withheld the data subject's personal information (decision of 27 June 2007). The defendant operated two ophthalmology clinics in Tokyo, and each of the two plaintiffs, patients of one of the clinics demanded that the defendant disclose their medical records to them in accordance with article 25-1 of [the PPIA]. As summarized by Fuse and Kosinski:[200]

> The plaintiffs requested the court to interpret [the PPIA] as providing a private cause of action against the defendant for court-ordered disclosure of the data at issue and monetary compensation. In response, the defendant asserted that the legislature did not intend the PPIA to provide a private cause of action because the text of [the PPIA] provides for extra-judicial conciliation methods (Article 42) and gives a clear grant of authority to the ministries to enforce the [PPIA] (Article 34-1).

The court adopted the defendant's view. Critics of the decision argue that there is evidence from the legislative history of the PPIA, though not from the text of the PPIA itself, that the legislature intended to create a civil right of action, and that that District Court did not take this into account.[201] If this decision is followed by subsequent courts, complainants will have to rely on the very limited administrative remedies under the PPIA, or extra-judicial mediation (discussed below) and will have no direct access to the courts to uphold their rights under the PPIA, at least unless those rights can be equated to something already protected under other laws. It is possible to sue the Japanese national government or local government for negligent application of the law.[202] However, the issue is not settled, particularly as courts in Japan's civil law system courts are not strictly bound to follow earlier decisions.[203]

In other cases, plaintiffs in cases of non-consensual disclosures have successfully taken actions under the tort provision of article 709 of the Civil Code to uphold rights similar to those found in the PPIA, without attempting to base their case on a positive right arising directly from the PPIA. The plaintiffs in one case apparently considered that mere **(p.259)** refusal to allow them to access their record would not constitute a breach of their tortious right of privacy.[204]

In another 2007 case commenced before the PPIA came into force, the Tokyo High Court upheld on 28 August 2007 a District Court decision holding a beauty salon chain vicariously liable for the negligence of a subcontractor. The contractor had let customers' personal information escape onto the Internet where it was distributed by P2P software. Kosinski[205] explains that the significance of the case is that 'the court looked to OECD privacy guidelines and Japanese ministry regulations in effect at the time to determine the applicable standard of care. If this incident were to occur today, the court would instead likely look to the [Act] to determine the standard of care'. Although the damages awarded were objectively very small, averaging only US$265 to 13 of 14 plaintiffs, plus US $45 costs, this was nevertheless record damages for a data leak case. In a previous case connected with Yahoo!, the Osaka District Court awarded a small amount of compensation (US$55 per person) to a group of plaintiffs, against Softbank BB Corp for its violation of its duty of care in preventing improper access to, and leakage of, large amounts of personal data, because of inadequate security measures.[206]

These cases illustrate that, where actions which would breach some of the privacy principles in the PPIA (e.g. intentional or negligent disclosures), plaintiffs may have some remedy under the Civil Code or Japan's 'privacy tort',[207] or other legislation, but for other breaches (e.g. refusal of access or correction, failure to give notice, excessive collection) no tort or other remedies are available. It is doubtful whether these miscellaneous remedies could be an adequate substitute for direct access to the courts to enforce rights under the PPIA. As a result, it is not clear under what circumstances plaintiffs can obtain remedies in the courts for breaches of the PPIA, either under the Act itself, or under the Civil Code.

8.5. Systemic enforcement measures

There is no system of notification or registration by businesses under the PPIA. However, ministries may require information to be provided by the entities that come under their administration, and sometimes do so. The system of notifications to the MIC by administrative organs has been discussed earlier. There is no general system of permits for certain categories of personal data to be collected or used.

Under the new ID Number Act, 'specific personal information protection assessments', which may be similar to privacy impact assessments (PIAs), may be required. The post-2014 reform proposals also include standardization of procedures for requiring PIAs.

9. Self-regulation and co-regulation in the Japanese system

There are two main aspects of co-regulation in the Japanese system. There is no evidence of the effectiveness of the statutorily prescribed industry bodies that are supposed **(p.260)** to receive complaints (APIPOs). Evidence of effectiveness of the PrivacyMark System, a joint public–private trustmark, is more equivocal, with some evidence of complaint handling, but it never revokes trustmarks once they are issued, so its principal sanction remains unused.

9.1. Self-regulation by private dispute resolution bodies (APIPOs)

The role of an 'authorized personal information protection organization' (APIPO) is set out in PPIA, part 4, art. 2 (Promotion of the Protection of Personal Information by Private Institutions). The Basic Policy says that it expects they will play 'an extremely important role' in Japanese data protection, particularly to assist businesses to voluntarily resolve complaints but this is not so.

The competent ministry in a sector may authorize as an APIPO a business that involves itself in the handling of complaints about the personal information practices of other businesses (called 'targets').[208] There are some very vague standards with which the applicant must comply.[209] Each business 'target' must become a member of the dispute resolution body, and this must be made public.[210] APIPOs can receive complaints directly from individuals, and target entities are required to cooperate in investigations, and not reject the APIPO's requests 'without justifiable reason'.[211] Each APIPO is supposed to publish its own guidelines.[212] The minister can require reports from an APIPO[213] or order it to improve its procedures,[214] or even revoke its authorization.[215] There was one case of a minister requiring a report in 2007.[216]

The APIPOs have no independent powers. They are not arbitrators in disputes or even specifically empowered to be mediators. They are presumably supposed to be neutral as between their members and complainants, but even this is not clear.

Although there have been 39 organizations designated as APIPOs by relevant ministers under article 37, the number of complaints lodged with them was not disclosed by the Quality of Life Policy Council. Although the Council adheres to the Basic Policy line that these private dispute resolution bodies are important, it seems to make elliptical criticisms of at least some of them. It states that 'less active authorized personal information protection organizations are expected to proactively process complaints and provide information to target entities in the future', and furthermore:[217]

> From now on, it will be important to fully publicize the roles of authorized personal information protection organizations to the public and entities and to make efforts to help improve confidence in these organizations. In addition, it will be necessary for these organizations to proactively engage in personal information leakage cases in order to further enhance their functions.

No evidence of their effectiveness is presented by the Council, and it seems that no evidence is available. No enforcement mechanism can have credibility without some evidence of its effectiveness.

(p.261) 9.2. Trustmarks

Japan's PrivacyMark, which has been operating since 1998, is explained by its operators[218] as follows:

> The accreditation of PrivacyMark System requires third-party organizations to objectively evaluate the compliance of private enterprises with all relevant laws and regulations, including JIS Q 15001, and is an effective tool that allows private enterprises to demonstrate that they are in compliance with the law and that they have voluntarily established a personal information protection management system with a high

level of protection.

The Japan Information Processing Development Cooperation (JIPDEC),[219] a joint public-private agency established by METI and MIC, is responsible for managing the PrivacyMark System. It has a PrivacyMark System Committee which it says 'is organized with scholars, learned individuals, representatives from business organizations, representatives of consumers and legal professionals'.[220] JIPDEC has three main functions: (i) establishment and revision of standards and regulations involving the PrivacyMark System; (ii) designating and revoking of the Conformity Assessment Bodies (which accredit individual businesses as PrivacyMark users); and (iii) revoking of PrivacyMark Accreditation. So this is a decentralized system in which numerous trade associations and the like are supposed to be able to certify that their own members comply with Japan's legislation, Cabinet Orders, Basic Policy, Guidelines, etc.

It costs a business somewhere in the range of US$3,000 to US$12,000 to obtain a PrivacyMark, renewable every two years at 75 per cent of the initial fee.[221] As of 20 January 2014 13,404 Japanese companies are stated to use the PrivacyMark System.[222] It is intended that both consumers and organizations such as local government bodies will rely on this system in deciding that businesses they are proposing to deal with are reliable in relation to data protection. In order to participate in the bidding process to obtain contracts regarding information processing services with local government entities in Japan, companies must have a PrivacyMark. This is sometimes considered as an entry qualification to the preliminary screening of prospective bidders. In relation to companies proposing to bid for local government contracts, there is therefore a de facto element of compulsion concerning the PrivacyMark, which helps explain its high take-up rate. Consumer reliance may be very low.[223]

There are 28 Conformity Assessment Bodies, explained as follows:

> Conformity Assessment Bodies should be trade associations and other organizations with rich store of knowledge in personal information protection and ability to implement PrivacyMark system. (Limited to non-profit organizations and trade associations established by Japanese law and/or other non-profit organizations admitted by the JIPDEC.)[224]

(p.262) Accreditation involves having an appointed manager for personal data, annual training, annual audit, a permanent contact point for consumers, 'appropriate security measures', and measures for protecting information given to contractors etc.[225]

There are three main methods by which the PrivacyMark System is enforced: (i) individual complaints investigated by Consumer Consultants; (ii) self-reporting; and (iii) investigations by Conformity Assessment Bodies.

The procedure for consumers to make complaints about breaches of the handling of personal information[226] is provided by the 'Complaint processing guideline'.[227] Any consumer who finds violations of the PrivacyMark requirements by any P-mark entity may inform the PrivacyMark Consumer Contact by email or by phone. This requirement is stipulated in the JIS Q 15001 and in the Rules for the Establishments and Operations of PrivacyMark System, including how to use (display) the PrivacyMark. These complaints are processed by consultants licensed as Consumer Consultants, who investigate by telephone. If violations are confirmed they may meet with staff of the entity to make it comply with the rules, and then the results are reported to the consumer. The result of received complaints, activities, and their resolution processed by JIPDEC are published on the Internet.[228] Based on this report, JIPDEC issues a report every year regarding advice to consumers and companies with respect to the misuse, security breach, and privacy-related issues based on each year's complaints trend. However, only four of 28 'Privacy Mark Issuing Organisations' (PMIO) have also released details of the complaints which they have handled, and of security breach cases, but the rest have not.[229]

Second, there is supposed to be a procedure by which accredited businesses self-report any 'accidents' concerning personal data to JIPDEC in accordance with the 'Evaluation Criteria for PrivacyMark Disqualification'.[230] This would be like voluntary data breach notification, but there is no clear evidence of its occurrence.

Third, the PrivacyMark Rules have provisions for Conformity Assessment Bodies to conduct fact-finding studies about a business's 'protection of personal information and use of the PrivacyMark', and for the issuing of

warnings, recommendations, and suspensions or withdrawals of accreditation.[231] Details of such studies and their results are published on the PrivacyMark site, so the accredited companies may face diminished social reputation if this becomes well known. Similarly, JIPDEC can conduct a 'fact-finding study' by any of the 18 Conformity Assessment Bodies, and request it to take improvement measures, or risk withdrawal of accreditation.[232] However, there does not seem to be any information to show that this has occurred.

Enforcement by the threat of withdrawal of the mark is regarded by some Japanese experts as a credible sanction in the context of Japanese business operations, although such **(p.263)** withdrawal is not regarded as having any credibility in some other countries.[233] JIPDEC does issue some information about the result of handling claims but there is no information available regarding the number of revoked or suspended companies. Details of investigation of alleged non-compliant cases are not provided. However, it is known that no company has had its mark revoked in recent years, despite questionable instances.[234] If the the principal sanction of a trustmark system is compromised by its non-use, and there is no available evidence of how decisions are made, it is questionable whether the whole system is credible, particularly when it has elements of compulsion underlying its 'success'.

10. Conclusions—Japan's weak and obscure laws with prospects for reform

This chapter has demonstrated the weaknesses of both the principles in Japan's public and private sector privacy laws and their lack of enforcement, both of which are compounded by lack of transparency. The Japanese government has now promised reforms.

10.1. Very limited principles

It has been difficult to illustrate the real operation of most of the data protection principles in the Acts, because very few useful examples of their application are available. Among their stronger points are public sector coverage, and notice required regarding collection from third parties. However, the principles have been shown to be among the most limited in the data privacy laws in Asia, as seen in their limited private sector scope (the 'small business' exemption); easily manipulated exceptions to use and disclosure limitations; lack of deletion provisions; lack of sensitive information provisions; and lack of restrictions on data exports.

10.2. Differing opinions on enforcement to 2014

This chapter has also analysed the range of enforcement mechanisms provided by Japan's data protection laws, and the available evidence of the extent to which they have been used, and to what effect. Evidence is very often lacking. Such failure to provide transparency of the enforcement system, is, in itself, a deficiency.

There is some divergence of opinion concerning the effectiveness of the enforcement of the PPIA, but from early in the life of the Act, most commentators have been sceptical about its effectiveness. For example, Ponazecki et al. concluded in 2007 that 'there have not been significant administrative fines or penalties or court judgments arising from failures to comply with the Law and the related guidelines'.[235] In their view the main risk for a private company that violates the PPIA is usually the risk of reputational damage rather than the risk of paying large fines or having to defend class action suits. In agreeing with this, Ito and Parker did not have much confidence in the enforcement system:[236]

> **(p.264)** It is less clear for now whether the ministries are likely to take more active steps to enforce compliance with the Act. The deterrent effect is not proven and the ongoing incidents of data leaks and other breaches are proof that more needs to be done by businesses to ensure compliance….It is also difficult to imagine a business ever facing fines, or the directors the threat of imprisonment, under the Act, except in the case of hopelessly reckless failure, or aggressive refusal, to comply; businesses are much more likely to co-operate with the relevant ministries to ensure that they comply with any order to implement corrective measures.

While it may be that reputational damage is the 'main risk' of the current system, that does not mean that this risk is effective in guaranteeing compliance, nor that it delivers anything of value to consumers when non-compliance does occur.

In contrast, Miyashita in 2011 argued that:

> The legal rules for enforcement mechanisms are very particular in Japan, and differ from the strong

> enforcement of the law in European countries. However, it is crucially important to understand that a data breach in Japan means the disruption of social trust and the intimate relationship with customers. In Japan, the risk of loss of social trust and business reputation is regarded as much more significant than paying a fine. Thus, businesses generally follow the guidelines issued by government ministries, and some also adopt their own guidelines which go even further.[237]

However, he agreed with my 2009 conclusion that 'there is a lack of evidence that the legislation is effective, which could be remedied somewhat by Ministries gathering and publishing more detailed data on compliance, enforcement, breaches and remedies'.[238]

There has been no significant change in Japan concerning the availability of any such evidence. This chapter has documented the very limited evidence of application of any of the possible types of statutory enforcement in relation to the public sector, and in relation to the private sector, and by the co-regulatory systems. So, to put it politely, the puzzle of the effectiveness of Japanese data privacy law remains. The Japanese system does not provide evidence of its effectiveness. Its enforcement mechanisms are not used to any significant extent, and the mechanisms by which most of the enforcement measures work are obscure. The result is a system that asks observers to take it on trust that it is effective.

10.3. Plans for reform post-2014

Such criticisms regarding the content and enforcement of Japan's data protection law are understood by Japanese policy-makers, but are not the primary drivers of new policy. The Japanese government has decided to amend its laws, in part as a response to the 2013 revision of the OECD privacy guidelines, but possibly also in part as a response to international perceptions of the weaknesses of Japanese law, and the impediments this might create in the future. The law reform committee at the government's IT Strategic Headquarters[239] discussed reforms for three months[240] including amendments to the current law. The IT Strategic Headquarters decisions announced on **(p.265)** 20 December 2013,[241] with support from the Prime Minister,[242] are intended to be developed into an outline proposal in June 2014, and then a Bill to the Diet in spring 2015. The December 2013 proposals may be paraphrased as follows. First, the aims of the reforms were stated to be based on three pillars: the utilization of personal data in 'the age of big data'; the protection of privacy to meet with the expectations of individuals; and revisions related to globalization. The emphasis is not primarily on privacy protection but on creating an environment where Japanese businesses can utilize personal data, including from people outside Japan, to create new businesses and services.

Second, there will be revisions to privacy principles included in the PPIA concerning such matters as inclusion of a definition of sensitive data; standardization of procedures for obtaining consent; standardization of procedures for implementing PIAs; clarification of anonymized data and its implications for privacy; limitation on data transfer outside Japan; the replacement of the exemption of small and medium-sized enterprises; the right of the individual to ensure the disclosure, erasure, and suspension of the use of personal data; and clarification of the balance between public welfare and individual rights. These proposed reforms to the substantive principles and rights in the PPIA are significant and may address some of the main criticisms that have been made of those aspects of Japan's law.[243]

Third, major reforms are proposed to the procedural and enforcement aspects of Japan's law. The most important is the establishment of an independent supervisory authority (DPA or Privacy Commissioner), which will largely supplant the existing SPIPC (the 'My number' Commission) and (possibly) the ministerial-based enforcement system. Administrative sanctions and criminal penalties might be enforced by this DPA, but whether they will have any substance is unclear. There is no suggestion that the DPA may be able to award compensation for breaches, or that consumers will be able to take court actions for compensation. The application of the DPA enforcement powers within the public sector is also to be addressed, but it is not clear what powers the DPA will have. This supervisory authority will be established as an independent authority, called an 'article 3' body,[244] and as a personal information protection commission. It is hoped by Japan that the DPA will meet the required international accreditation standard as a privacy enforcement authority, such as for membership of the International Conference of Data Protection and Privacy Commissioners. Given the history of privacy protection in Japan, it is a matter of 'wait and see' whether this DPA will really resemble those established in other countries.

The Japanese government considers that these reforms will be underpinned by the 2013 revisions to the OECD

Guidelines, so they may also involve other matters that reflect the changes to those guidelines. However, the reforms appear to go beyond the revisions to the OECD Guidelines, and may, depending on their detailed implementation, constitute a fresh start for Japan's law. Like Hong Kong, Taiwan, and South Korea, Japan's 'second generation' data protection law may be stronger than the first generation law, but dangers lie in the 'big data' plans. The major reforms proposed may provide much more effective means of enforcement, but are only likely to succeed if they also make that enforcement more transparent.

Notes:

([1]) A. Kerr, ch. 5, 'Bureaucracy—Power and Privilege' in *Dogs and Demons—The Fall of Modern Japan* (Penguin 2001).

([2]) Kerr, *Dogs and Demons*.

([3]) For Japan's post-war history see Francis Pike, *Empires at War: A Short History of Modern Asia Since World War II* (I B Tauris, 2010), chs. 1, 4, 9, 27, and 55 and pp. 708–9. For a longer recent historical span, see Andrew Gordon, *A Modern History of Japan: From Tokugawa Times to the Present* (2nd Edn., Oxford University Press, 2009).

([4]) As of 1 January 2014.

([5]) Masabi Chiba, ch. 3 'Japan' in Poh-Ling Tan (Ed.), *Asian Legal Systems—Law, Society and Pluralism in East Asia* (Butterworths, 1997). For another succinct account of Japan's legal system, see Kent Anderson and Trevor Ryan, ch. 4 'Japan: The Importance and Evolution of Legal Institutions at the Turn of the Century' in E. Anne Black and Gary F. Bell (Eds.), *Law and Legal Institutions of Asia* (Cambridge University Press, 2011). For more detailed studies, see Hiroshi Oda, *Japanese Law* (3rd Edn., Oxford University Press, 2009) and Daniel H. Foote (Ed.), *Law in Japan: A Turning Point* (University of Washington Press, 2007).

([6]) See Act on Promotion of Use of Alternative Dispute Resolution (Act No. 151 of 1 December 2004), and the Consumer Contract Act (Act No. 61 of 12 May 2000), amendments regarding Qualified Consumer Organizations.

([7]) Chiba, ch. 3 in Tan (Ed.), *Asian Legal Systems.*

([8]) There are also 438 Summary Courts, and 50 District Courts in each prefecture, plus 50 Family Courts.

([9]) Andrew Adams, Kiyoshi Murata, and Yohko Orito, 'The Japanese Sense of Information Privacy' (2009) 24(4) *AI & Society.*

([10]) Anderson and Ryan, ch. 4 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, p. 134.

([11]) *Case of narcotics control act violation, fraud, and attempt of aforementioned actions—1997* (A) No.636 [1999] JPSC 57 (16 December 1999) at <http://www.asianlii.org/jp/cases/JPSC/1999/57.html>.

([12]) *Judgment concerning the relationship between the act of an administrative organ to collect, manage or use identification information of inhabitants by way of the Basic Resident Register Network, and Article 13 of the Constitution* 2007 (O) No. 403, 2007 (Ju) No. 454; Minshu Vol. 62, No. 3.

([13]) See 1965 (A) No. 1187, judgment of the Grand Bench of the Supreme Court of 24 December 1969, Keishu Vol. 23, No. 12, p. 1625.

([14]) Tokyo District Court Case #1882 (wa) 1961 known as the 'After the Banquet Incident' (*Utage no Ato Jiken*).

([15]) C. Lawson, 'Japan's New Privacy Act in Context' (2006) 29(2) University of New South Wales Law Journal, <http://www.austlii.edu.au/au/journals/UNSWLJ/2006/17.pdf>, p. 93.

([16]) *Case to be brought for obstruction of performance of official duties and bodily injury*—1965 (A) No. 1187 [1969] JPSC 6; Keishu Vol. 23, No. 12, at 1625 ('*Kyoto Zengakuren Case*').

([17]) *Ruling concerning impression of fingerprints* [1995] JPSC 31; Keishu 49-100842.

([18]) *Judgment upon the case concerning whether information on names, addresses, etc., of students who*

applied for participation in a lecture meeting held by a university can be protected by law [2003] JPSC 36; Minshu Vol. 57, No. 8 at 973.

([19]) Oda, *Japanese Law*, pp. 88–9.

([20]) Lawson, 'Japan's New Privacy Act in Context', p. 97.

([21]) Jukinet, 'About Jukinet' (Jukinet, 2012—no longer available).

([22]) Lawson, 'Japan's New Privacy Act in Context', p. 97.

([23]) Lawson, 'Japan's New Privacy Act in Context', p. 98. The committee was chaired by Prof Masao Horibe.

([24]) This committee was chaired by Prof Sonobe.

([25]) Andrew Adams, Kiyoshi Murata, and Yohko Orito, 'The Development of Japanese Data Protection' (2010) 2(2) *Policy and Internet*, pp. 95–126.

([26]) Adams, Murata, and Orito, 'The Development of Japanese Data Protection'.

([27]) Including assisting in drawing up lists of victims, and providing them with grants.

([28]) Graham Greenleaf, Kiyoshi Murata, and Andrew Adams, '"My Number" Unlikely to Thaw Japan's Frozen Data Privacy Laws' (2012) 120 *Privacy Laws & Business International Report*, pp. 22–5 <http://ssrn.com/abstract=2207903>.

([29]) Greenleaf, Murata, and Adams, 'My Number'.

([30]) Japan Times, 'Risks of Using "My Number"' (Japan Times newspaper, 25 March 2013) <http://www.japantimes.co.jp/opinion/2013/03/25/commentary/risks-of-using-my-number/#.Usc9lPb9ogI>.

([31]) Asahi Shimbun, 'Editorial: ID Number System Should Be a Tool to Build a Fair Society' (Asahi Shimbun newspaper, 26 May 2013) <https://ajw.asahi.com/article/views/editorial/AJ201305270077>.

([32]) Act on the Protection of Personal Information 2003 (PPIA (Japan)) <http://www.japaneselawtranslation.go.jp/law/detail/?id=130&vm=04&re=02>.

([33]) Act on the Protection of Personal Information Held by Administrative Organs 2003 (PPIHAO (Japan)) <http://www.asianlii.org/jp/legis/laws/aotpopihbaoan58o2003772/>. Also, an English version of this law is available from 'Japanese Law Translation' <http://www.japaneselawtranslation.go.jp/law/detail_main?re=&vm=2&id=131>.

([34]) Chiba, ch. 3 in Tan (Ed.), *Asian Legal Systems*, p. 594.

([35]) No English translation of this Act is available.

([36]) Cabinet Order for the enforcement Act on the Protection of Personal Information (Cabinet Order 506, 2003) <http://www.caa.go.jp/seikatsu/kojin/foreign/cabinet-order.pdf>.

([37]) Basic Policy on the Protection of Personal Information 2 April 2004 (Cabinet Decision 25 April 2008) <http://www.caa.go.jp/seikatsu/kojin/foreign/basic-policy-tentver.pdf>.

([38]) There are in fact 42, but only 40 publicly acknowledged by the Consumer Agency. See list at <http://www.caa.go.jp/seikatsu/kojin/gaidorainkentou.html> (Japanese only).

([39]) T. Kato, 'Outline of Japan's Protection of Personal Information Act and Its Enforcement', Office of Personal Information Protection, Cabinet Office, Japan (PPTs), Privacy Laws & Business Conference, 14 October 2008, Strasbourg.

([40]) e.g. General industry, Financial industry, Consumer credit, Medical records, Genome R&D, Employee data, Head hunting, Telecommunications, TV Broadcasting/Cable, Education/Students, Welfare recipients, Transportation, Agriculture, Criminal suspects (Case, 2005). A list of 33 current in 2006 is available in Japan APEC

IAP (2006).

([41]) T. Kato, 'Outline of Japan's Protection of Personal Information Act and Its Enforcement'.

([42]) F. Shimpo, 'Japan: A New Guideline for the Economic and Industrial Sectors Pertaining to the Act on Protection of Personal Information' (2009) 102 *Privacy Laws & Business International Newsletter*, p. 20.

([43]) Decision of the Cabinet Office regarding the 'Guideline for the standardisation to all business fields and standards' (not available in English).

([44]) O. Ito and N. Parker, 'Data Protection Law in Japan: A European Perspective', *BNA World Data Protection Report*, December 2008.

([45]) Ministry of Economy, Trade and Industry (METI), *Guidelines Targeting Economic and Industrial Sectors Pertaining to the Act on the Protection of Personal Information*, March 2007, <http://www.meti.go.jp/policy/it_policy/privacy/0708english.pdf>.

([46]) E. Kosinski, 'Japan Amends Its Official Privacy Rules to Include Data Breaches' (2007) 90 *Privacy Laws & Business International Newsletter*, p. 8; Kosinski, 'Japan's High Court Confirms Record Damages for Data Leak' (2007) 90 *Privacy Laws & Business International Newsletter*, p. 1.

([47]) The revised METI Guidelines, September 2009. Not available in English.

([48]) Shimpo, 'Japan: A New Guideline'.

([49]) The earliest such regulations in Japan were the 'regulations concerning personal data protection management on computers', introduced in Tokushima City on 28 June 1973, followed by the privacy protection regulations adopted by Kunitachi City of the Tokyo Metropolitan area in 1975.

([50]) In 1980, there were more than 3,000 local bodies throughout Japan, but due to municipality amalgamations, that number dropped to 1,742.

([51]) Hiroshi Miyashita, 'Japan Appoints New Independent Commission for the Supervision of ID Numbers' (2014) 127 *Privacy Laws & Business International Report*, p. 10.

([52]) Japan, Quality of Life Policy Council, *Summary of Opinions on the Protection of Personal Information*, 29 June 2007, <http://www.caa.go.jp/seikatsu/shingikai/kojin/20th/torimatome.pdf>.

([53]) Quality of Life Policy Council Summary, p. 31.

([54]) Under the Basic Law for the Protection of Consumers of 2004, the Cabinet adopted the 'Basic Plan for Consumer Protection' for 2005–09 and subsequently for 2010–14, and the Consumer Affairs Agency and the Consumer Commission were established in 2009.

([55]) Japan Personal Information Protection Expert Committee Report, 'Primary concern about the Personal Information Protection Act and its Implementation' (2011).

([56]) Under art. 3 of the National Government Organization Act the SPIPC is entitled to exercise its powers independently of the Cabinet Office. Under the ID Number Act there are requirements of independence, as well as appointment by the Diet, and guarantees against dismissal. The chair of the SPIPC is Professor Masao Horibe.

([57]) Supplementary Provisions to the ID Number Act: see Miyashita, 'Japan Appoints New Independent Commission for the Supervision of ID Numbers'.

([58]) In Japan, organizations whose powers are based on art. 3 of the National Government Organization Act are entitled to exercise those powers independently of the Cabinet Office.

([59]) PPIA (Japan), art. 2(1).

([60]) PPIA (Japan), art. 2(4).

([61]) PPIA (Japan), art. 2(5).

([62]) PPIHAOA, arts. 2(2), 2(4), and 2(3) respectively.

([63]) Fumio Shimpo and Graham Greenleaf, 'Japan's Privacy Complaints Reveal Little' (2011) 109 *Privacy Laws & Business International Report* <http://ssrn.com/abstract=2194890>.

([64]) PPIA (Japan), art. 2(3).

([65]) PPIHAOA (Japan), art. 2(1).

([66]) PPIA (Japan), art. 2(2).

([67]) Cabinet Order, 2003, art. 1.

([68]) PPIA (Japan), art. 2(3)–(5).

([69]) Quality of Life Policy Council report (2007).

([70]) Quality of Life Policy Council report, p. 11.

([71]) Quality of Life Policy Council report, p. 23.

([72]) Order of 1 May 2008: information provided by Professor Shimpo.

([73]) PPIA (Japan), art. 50.

([74]) PPIA (Japan), art. 50(3).

([75]) J. Harland, 'Japan's New Privacy Legislation: Are You Ready?' (2004) 20(3) *Computer Law & Security Report*, pp. 200–2.

([76]) PPIA (Japan), art. 23. However, this obligation can be avoided by the provision of a 'readily accessible' notice allowing data subjects to opt out of the disclosure (processing) (see art. 23(2)).

([77]) PPIA (Japan), art. 23(4)(1).

([78]) PPIA (Japan), art. 22.

([79]) For a summary, see Oda, *Japanese Law*, pp. 131–5.

([80]) This is common elsewhere: in Australia such excuses are called 'BOTPAs' ('because of the Privacy Act').

([81]) David Case, 'How Japan's New Personal Information Law Is Having an Impact on Business' (presentation at Privacy Laws & Business Conference, Cambridge, July 2005). See also David Case, 'Japan's Privacy Law to Be Revised' (2007) 86 *Privacy Laws & Business International Newsletter*, p. 12.

([82]) Ito and Parker, 'Data Protection Law in Japan'.

([83]) Quality of Life Policy Council report, p. 4.

([84]) Quality of Life Policy Council report, p. 6.

([85]) See Greenleaf, 'Country Studies—B5 Japan' in D. Korff (Ed.), *Comparative Study on Different Approaches to New Privacy Challenges.*

([86]) PPIA (Japan), arts. 15–31 of ch. 4.

([87]) Quality of Life Policy Council report, p. 12.

([88]) METI 2007 Guidelines, pt. 2-1-10.

([89]) Ministry of Economy, Trade and *Industry METI Privacy Guidelines Q&A* (METI, March 2007) <http://www.meti.go.jp/policy/it_policy/privacy/070330guidelineq&a.pdf>.

([90]) METI 2007 Guidelines, pt. 2-1-10.

([91]) Financial Services Agency, *Guidelines for Personal Information Protection in the Financial Field* (FSA, Japan, 2007), art. 4 <http://www.fsa.go.jp/frtc/kenkyu/event/20070424_02.pdf>.

([92]) Quality of Life Policy Council report, p. 24.

([93]) Quality of Life Policy Council report, p. 25.

([94]) METI 2007 Guidelines, pt. 2-2-1(1).

([95]) PPIHAO Act (Japan), art. 4; PPIHIAAA (Japan), art. 4.

([96]) PPIA (Japan), art. 16.

([97]) PPIA (Japan), art. 18(3).

([98]) PPIA (Japan), art. 18(4).

([99]) Shimpo and Greenleaf, 'Japan's Privacy Complaints Reveal Little'.

([100]) PPIA (Japan), art. 22.

([101]) PPIA (Japan), art. 23.

([102]) Ito and Parker, 'Data Protection Law in Japan'.

([103]) METI 2007 Guidelines, pt. 2-2-4(2).

([104]) Shimpo and Greenleaf, 'Japan's Privacy Complaints Reveal Little'.

([105]) PPIA (Japan), art. 23(4).

([106]) Summary provided to the author by White and Case.

([107]) PPIA (Japan), arts. 22, 23(4)(1); METI 2007 Guidelines, pt. 2-2-3-4.

([108]) PPIA (Japan), art. 23(4)(2).

([109]) Shimpo, 'Amendment of Japanese Guideline'.

([110]) PPIA (Japan), art. 23(4)(2).

([111]) Ito and Parker, 'Data Protection Law in Japan'.

([112]) PPIHAOA (Japan), art. 8; PPIHIAAA (Japan), art. 8.

([113]) PPIHAOA (Japan), art. 3(3).

([114]) PPIA (Japan), art. 18(1).

([115]) PPIA (Japan), art. 18(2).

([116]) PPIA (Japan), art. 17.

([117]) Shimpo and Greenleaf, 'Japan's Privacy Complaints Reveal Little'.

([118]) Shimpo, 'Amendment of the Japanese Guideline'.

([119]) PPIHIAAA (Japan), art. 5.

([120]) PPIHAOA (Japan), art. 3; PPIHIAAA (Japan), art. 3.

([121]) APEC IAP—*Information Privacy Individual Action Plan—Japan (2006).*

([122]) PPIHAOA (Japan), art. 5; PPIHIAAA (Japan), art. 6.

([123]) Quality of Life Policy Council Report, pts 17–19.

([124]) Ito and Parker, 'Data Protection Law in Japan'.

([125]) PPIHAOA (Japan), art. 6; PPIHIAAA (Japan), art. 7.

([126]) PPIA (Japan), art. 21.

([127]) PPIA (Japan), art. 22.

([128]) Quality of Life Policy Council Report, pt. 21.

([129]) Kosinski, 'Japan Amends Its Official Privacy Rules'; METI 2007 Guidelines, pt. 2-2-3-2.

([130]) Shimpo, 'Amendment of the Japanese Guideline'.

([131]) PPAHAO (Japan), art. 10.

([132]) PPAHAO (Japan), art. 11.

([133]) PPIA (Japan), art. 27(1).

([134]) PPIHAOA (Japan), art. 3; PPIHIAAA (Japan), art. 3.

([135]) Shimpo and Greenleaf, 'Japan's Privacy Complaints Reveal Little'.

([136]) There are no special provisions in the PPIA concerning credit reporting, but there are sectoral Ministry guidelines concerning consumer credit.

([137]) Quality of Life Policy Council Report, pt. 10.

([138]) PPIHAOA (Japan), art. 4.

([139]) PPIHAOA (Japan), art. 7.

([140]) PPIHAOA (Japan), art. 8.

([141]) Japan introduced early anti-spam legislation in 2002 (The Law on Regulation of Transmission of Specified Electronic Mail, known as the Anti-Spam Law) but it was opt-out (Law No. 26 of 17 April 2002, as amended by Law No. 87 of 26 July 2005). However, in 2008 Japan amended the legislation, switching to an opt-in regime effective from 1 December 2008 (Japan, MIC, 2009). The law is administered by the Ministry of Internal Affairs and Communication (MIC). The law prohibits common types of fraud and deception, and now has very few exemptions. Its main weakness is that it appears that opt-in can be implied by a person providing their email address, with no other expression of consent, and MIC has not yet provided clarifying guidance on this. It is also unclear if it covers SMS (mobile phone text messages). These comments are based on information provided by Chris Connolly.

([142]) H. Miyashita, 'The Japanese Act on International Issues' (Office of Personal Information Protection, Cabinet Office, Japan; presentation at Privacy Laws & Business Conference, 14 October 2008).

([143]) PPIA (Japan), art. 23.

([144]) PPIA (Japan), art. 23(2).

([145]) White & Case LLP have provided the information of which this section is a paraphrase.

([146]) PPIHAOA (Japan), art. 56.

([147]) PPIA (Japan), art. 28.

([148]) PPIA (Japan), art. 18(2).

([149]) PPIA (Japan), art. 18(1).

([150]) PPIA (Japan), art. 18(3).

([151]) PPIA (Japan), art. 18(4).

([152]) PPIA (Japan), art. 24(2).

([153]) Quality of Life Policy Council Report, pt. 21.

([154]) Quality of Life Policy Council Report, pt. 25.

([155]) PPIA (Japan), art. 25.

([156]) PPIA (Japan), art. 30.

([157]) PPIA (Japan), art. 26.

([158]) PPIHAOA (Japan), arts. 14–26.

([159]) PPIHIAAA (Japan), arts. 12 and 27 respectively.

([160]) PPIA (Japan), art. 17.

([161]) Quality of Life Policy Council Report, pt. 17.

([162]) PPIHAOA (Japan), art. 36.

([163]) PPIHAOA (Japan), arts 37–46.

([164]) MIC Administrative Management Bureau (AMB) issued the report regarding the implementation of PPIHAO (in Japanese) <http://www.soumu.go.jp/menu_news/s-news/01gyokan06_02000004.html>.

([165]) It covers all 41 administrative organs and all 205 incorporated administrative agencies, from 1 April 2011 to 31 March 2012.

([166]) PPIHAOA (Japan), arts. 53–5.

([167]) PPIHAOA (Japan), art. 56.

([168]) 'When a person who has requested the disclosure of an administrative document and corporate document and personal information appeals against the disclosure decision under the Administrative Complaint Investigation Law, the Information Disclosure and Personal Information Protection Review Board carries out a review and submits a report in response to a query from the head of the government body in question', Cabinet Office website note at <http://www.cao.go.jp/en/disclosure.html>.

([169]) PPIHAOA (Japan), art. 42.

([170]) Information Disclosure and Personal Information Protection Review Board decisions (Cabinet Office) <http://koukai-hogo-db.soumu.go.jp/>. There are also some related judgments of courts but they show little about enforcement.

([171]) PPIA (Japan), art. 31.

([172]) The list of accredited authorized personal information protection organizations (APIPO) is available online <http://www.caa.go.jp/seikatsu/kojin/ninteidantai.html> (as of 1 October 2013).

([173]) Japan, *Basic Policy on the Protection of Personal Information* (Japanese government, 2 April 2004, revised 25 April 2008).

([174]) They were classified as: (1) voluntary stop to using personal information held; (2) outsourcing transparency; (3) clarification for the purpose of use in details; (4) elucidate acquisition resources; (5) publishing a privacy policy.

([175]) Hiroshi Miyashita, 'The Evolving Concept of Data Privacy in Japanese Law' (2011) 1(1) *International Data Privacy Law*, pp. 229–37, fn. 35.

([176]) Quality of Life Policy Council report, pt. 29.

([177]) The direct consultation service by the NCACJ was based on 'the Basic Policy of the Review of Clerical Work and Business of Independent Administrative Agency' (Cabinet Order 7 December 2010).

([178]) Parts of this section were previously published as Shimpo and Greenleaf, 'Japan's Privacy Complaints Reveal Little'. Translations and paraphrases of complaints from the Japanese texts are by Fumio Shimpo.

([179]) National Consumer Affairs Center of Japan (NCACJ) <http://www.kokusen.go.jp/jirei/j-top_kojinjoho.html>.

([180]) Translations and paraphrases of complaints from the Japanese texts are by Fumio Shimpo.

([181]) Some of the other issues in the 18 reports are: disclosure of a registration postcard registered under another person's name; requirement of a comprehensive consent that compels agreement to utilize personal information; deletion of individual information after cooling off notification; unsolicited telemarketing; and telemarketing involving a threatening telephone call by a real estate company.

([182]) PPIA (Japan), art. 32.

([183]) PPIA (Japan), art. 33.

([184]) PPIA (Japan), arts. 16–27 except arts. 19 and 30(2).

([185]) PPIA (Japan), art. 34(1).

([186]) PPIA (Japan), art. 34(2).

([187]) PPIA (Japan), art. 34(3).

([188]) PPIA (Japan), art. 36.

([189]) Japan, Cabinet Office, *Summary Report on the Enforcement Status of Act on the Protection of Personal Information in FY 2007 (Tentative Translation, Excerpt)*, September 2008.

([190]) Japan, Cabinet Office, *Summary Report on the Implementation Status of Act on the Protection of Personal Information in FY 2006 (Tentative Translation)*, September 2007.

([191]) Japan, Consumer Agency, *Summary Report on the Enforcement Status of Act on the Protection of Personal Information in FY 2012* (only in Japanese), September 2013, <http://www.caa.go.jp/seikatsu/kojin/24-sekou_3.pdf>.

([192]) Ito and Parker, 'Data Protection Law in Japan'.

([193]) 'Michinoku Ordered to Secure Data' (*The Japan Times*, 23 May 2005).

([194]) Masatomo Suzuki, 'The Consumer Protection with Respect to Point Services' (2013) 12 NCACJ pp. 8–10, July 2013. The company insists that their personal data sharing falls within the scope of cases in which personal data is used jointly between specific individuals or entities under art. 23(4) item 3 of the PPIA.

([195]) Ito and Parker, 'Data Protection Law in Japan'.

([196]) The document issued to Google by the Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry said that, in relation to their new policy and its 'serious, potential consequences for Japanese users' that 'it is important to comply with the law and offer a comprehensible explanation to these users'. 'It must offer services appropriately and provide necessary, additional explanations and complaints procedures for users to access appropriate correspondence arrangements regarding these services and the handling of personal information.' No specific steps were required.

([197]) PPIA (Japan), arts. 56, 57.

([198]) Tokyo High Court case, 25 January 2007, Tokyo High Court case, 8 July 2008, Tokyo District Court case, 29 August 2005, Osaka District Court case, 20 February 2007, Tokyo High Court case, 16 July 2009, Tokyo District Court case, 22 April 2010.

([199]) K. Fuse and E. Kosinski, 'Individual Cause of Action Denied in Japanese Privacy Case' (2008) *Privacy Laws & Business International Newsletter*, no. 94, p. 11.

([200]) Fuse and Kosinski, 'Individual Cause of Action Denied in Japanese Privacy Case'.

([201]) Fuse and Kosinski, 'Individual Cause of Action Denied in Japanese Privacy Case'.

([202]) Information provided by White & Case LLP.

([203]) Yoichiro Itakura, 'A Study on the Claim for Damages by the Basis of the Violation of the Act on the Protection of Personal Information' (2012–11) 11 *Information Network Law Review*, pp. 1–12, argues that there is a possibility of compensation for privacy damages based on the PPIA, but there are no cases as yet directly accepting such a cause of action sufficient to create a judicial precedent.

([204]) Fuse and Kosinski, 'Individual Cause of Action Denied in Japanese Privacy Case'.

([205]) Kosinski, 'Japan Amends Its Official Privacy Rules to Include Data Breaches', p. 8.

([206]) J. Ponazecki and S. Horikawa, 'Japanese Court Orders Payment for 6,000 Yen to Each Plaintiff in Connection with the Yahoo!BB Personal Data Leak' (2006) 7(6) *Privacy Information and Law Report*.

([207]) Japanese law has recognized a right of privacy, a privacy tort in effect, since at least the early 1960s: Lawson, 'Japan's New Privacy Act in Context', p. 97.

([208]) PPIA (Japan), art. 37.

([209]) PPIA (Japan), art. 39.

([210]) PPIA (Japan), art. 41.

([211]) PPIA (Japan), art. 42.

([212]) PPIA (Japan), art. 43.

([213]) PPIA (Japan), art. 46.

([214]) PPIA (Japan), art. 47.

([215]) PPIA (Japan), art. 48.

([216]) Japan, Cabinet Office, *Summary Report on the Enforcement Status of Act on the Protection of Personal Information in FY 2007* (Tentative Translation, Excerpt), September 2008.

([217]) Quality of Life Policy Council Report.

([218]) JIPDEC—Japan Information Processing Development Corporation 'PrivacyMark System', 14 February 2013 (PPTs), on the PrivacyMark website.

([219]) Now called the Japan Institute for Promotion of Digital Economy and Community.

([220]) JIPDEC, 'Japan PrivacyMark System', 'Implementation Structure' page.

([221]) JIPDEC, 'Japan PrivacyMark System'.

([222]) Miyashita, 'The Japanese Act on International Issues'.

([223]) Studies show that young individual consumers' awareness of the PrivacyMark is very low, but apparently growing. Questionnaire surveys conducted in 2008 and in 2013 showed that 1.9% and 7.1% of respondents clearly understood what the PrivacyMark represented, respectively. See Kiyoshi Murata, Y. Orito, and Y. Fukuta (2014), 'Japanese Youngsters' Social Attitude towards Online Privacy' (2014) *Journal of Law, Information and Science* (forthcoming); Y. Orito, K. Murata, and Y. Fukuta, 'Do Online Privacy Policies and Seals Affect Corporate Trustworthiness and Reputation?' (2013) 19 *International Review of Information Ethics*, pp. 52–65.

([224]) JIPDEC, 'Japan PrivacyMark System', 'Implementation Structure' page.

([225]) JIPDEC, PrivacyMark Rules, art. 10.

([226]) JIPDEC, 'The Contact List for P-Mark related complaints', <http://privacymark.jp/contact/index.html>. 'The Contact form for complaints'.

([227]) JIPDEC, 'The Complaint processing guideline', <http://privacymark.jp/reference/pdf/pmark_guide101018/PMK730.pdf> (in Japanese).

([228]) JIPDEC, 'The result of received complaints and its solution', <http://privacymark.jp/news/2012/0823/index.html>.

([229]) JIPDEC, The Handling Complaints and Security Breaches Report (JIPDEC, 2012) <http://privacymark.jp/news/2013/0712/>. The Japan Information Technology Services Industry Association (JISA) issues an annual abstract of a report for security breach incidents and complaints handling <http://www.jisa.or.jp/service/privacy/tabid/763/Default.aspx.>, and the Japan Data Communications Association (JADAC) issues any results of security breach handling incidents <http://www.dekyo.or.jp/>. The Japan Federation of Printing Industries issues also the same kind of report <http://www.jfpi.or.jp/p-mark/index.html>. There are 28 PMIOs but only these four organizations have released their reports.

([230]) JIPDEC, 'Japan PrivacyMark System', 'Reporting Accidents' page; PrivacyMark Rules, art. 20(4).

([231]) JIPDEC, PrivacyMark Rules, arts. 20–22.

([232]) JIPDEC, PrivacyMark Rules, arts. 31–34.

([233]) For example, in the USA with the operation of the TRUSTe mark, see Chris Connolly 'Trustmark Schemes Struggle to Protect Privacy' (Galexia, 2008) <http://www.galexia.com/public/research/assets/trustmarks_struggle_20080926/trustmarks_struggle_public.html>

([234]) For example, in February 2007, Dai Nippon Printing Co. Ltd. (DNP) officially announced the leakage of more than eight million pieces of personal data it was responsible for protecting. However, JIPDEC did not revoke or suspend DNP's PrivacyMark. Such revocation or suspension would have interfered with daily routines of many companies and local governments which delegated personal data handling to DNP.

([235]) J. Ponazecki, D. Levison, and T. So, 'Japan—Personal information privacy update', BNA International *World Data Protection Report*, December 2007.

([236]) Ito and Parker, 'Data Protection Law in Japan'.

([237]) Miyashita, 'The Evolving Concept of Data Privacy in Japanese Law', p. 233.

([238]) Miyashita, 'The evolving Concept of Data Privacy in Japanese Law', p. 232, quoting Greenleaf, 'Country Studies—B5 Japan' in D. Korff (Ed.), *Comparative Study on Different Approaches to New Privacy Challenges.*

([239]) The Strategic Headquarters for The Promotion of An Advanced Information and Telecommunications Network Society (Cabinet Office, Japan).

([240]) Discussions commenced on 2 September 2013 with a final meeting on 10 December.

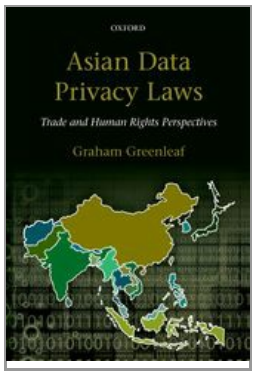
([241]) 'The Plan to Review the Legal System for the Utilisation of Personal Data' (IT Strategic Headquarters, 20 December 2013), alternatively translated as 'Policy on Reviewing Personal Data Utilisation Systems'.

([242]) Prime Minister Abe said in his opening address to this meeting of the IT Strategic Headquarters: 'Today, I would like to have a discussion on creating new rules for promoting the use of "personal data." It is imperative that the active use of data is promoted while making considerations for the protection of privacy. The Government will proactively engage in the rule-making process.' (The Prime Minister in Action, 20 December 2013) <http://www.kantei.go.jp/foreign/96_abe/actions/201312/20it_e.html>.

([243]) For example, as made in this chapter and previously in Greenleaf, 'Country Studies—B5 Japan' in D. Korff (Ed.), *Comparative Study on Different Approaches to New Privacy Challenges*.

([244]) In Japan, organizations whose powers are based on art. 3 of the National Government Organization Act are entitled to exercise those powers independently of the Cabinet Office.

University Press Scholarship Online
Oxford Scholarship Online



Asian Data Privacy Laws: Trade & Human Rights Perspectives
Graham Greenleaf

Print publication date: 2014
Print ISBN-13: 9780199679669
Published to Oxford Scholarship Online: December 2014
DOI: 10.1093/acprof:oso/9780199679669.001.0001

Macau SAR—The ‘Euro Model’

Graham Greenleaf

DOI:10.1093/acprof:oso/9780199679669.003.0009

[–] Abstract and Keywords

Macau’s Personal Data Protection Act of 2005, the focus of this chapter, is one of the strongest data protection laws in Asia on paper, and is also being seriously but moderately enforced. The Macau Special Administrative Region (SAR) of the People’s Republic of China (PRC) is one of the smallest but also one of the most economically successful regions of China. The Act is very similar to Portugal’s legislation in most respects, and is the most European-influenced data privacy law in Asia. Macau’s legislation has now been in force for the best part of decade, making it one of the older Acts in Asia. It has a separate data protection authority. Macau’s legislation adopts the higher standard of ‘European’ principles. It is exceptionally transparent, though not perfect, in its documentation of how enforcement of the legislation functions.

Keywords: data protection, privacy, Asia, Macau, China, data protection authority

1. Introduction to the Macau SAR

The Macau Special Administrative Region (SAR) of the People's Republic of China (PRC) is one of the smallest but also one of most economically successful regions of China, with industries including entertainment and gambling, textiles, and household goods manufacture. It is small in everything but wealth, with a population of under 600,000 and an area of **(p.268)** less than 30 square kilometres, but with per capita income over US$80,000. Portugal administered Macau from the sixteenth century until the transfer of sovereignty to the PRC in December 1999.

Macau's Personal Data Protection Act 2005 (PDPA (Macau)) is one of the strongest data protection laws in Asia on paper, and is also being seriously but moderately enforced. The Act is a very similar to Portugal's legislation in most respects, although also said to be influenced by Hong Kong's Ordinance. As a result it is closer to the EU Privacy Directive of 1995 than any other data protection legislation in Asia. Macau's position as a region of the PRC makes this doubly interesting.

1.1. History and politics

For nearly 450 years from 1555, the Portuguese occupied the territory we now know as Macau, with at least the implicit agreement of the rulers of China.[1] What was originally an informal lease of land did not become a formal treaty between China and Portugal until the nineteenth century.[2] Lisbon maintained cooperative relationships with Beijing throughout most of the colonial period. After the 1974 democratic revolution in Portugal, its new government offered to hand Macau back to China, but it declined the offer. However it willingly accepted Portugal's 1979 acknowledgement of PRC sovereignty of a 'Chinese territory under Portuguese administration'.[3] The retrocession (less formally, 'hand-over') of Macau to the PRC proceeded smoothly in 1999, with Portugal not taking any dramatic steps in the years preceding the handover to change the prevailing social and legal system in Macau. In particular, it did not attempt to introduce belated steps toward democratization, as the British did in Hong Kong.[4] Since Macau re-joined mainland China in 1999, its government has been headed by a Chief Executive, appointed by the PRC government upon recommendation of a 300-person electoral committee from Macau. The Chief Executive leads an Executive Council or cabinet. There is a 29-person Legislative Assembly comprising a combination of directly elected, indirectly elected (through 'functional constituencies') and appointed members.

1.2. Legal system

The 1999 constitutional arrangement of the Macau SAR is similar to that established in Hong Kong two years earlier. Macau became the second Special Administrative Region (SAR) of the PRC, with a Basic Law or mini-constitution, based on the 'one country, two systems' approach., This guarantees Macau the continuation of its existing capitalist social system for at least 50 years, and a 'high degree of autonomy' in its governance and legal system. As discussed in the following section, the Basic Law guarantees various civil liberties, including those relevant to privacy, and this was reflected in pre-hand-over reforms to the Civil Code and Penal Code.

The legal system of Macau had developed for centuries prior to the hand-over as part of

Portugal's legal system, and for the last 20 years this included the substantial changes resulting from Portugal's involvement in the European Union. The Macau SAR inherited a **(p.269)** legal system based on the approach of Portugal's civil law system (itself having been influenced by German civil law). Legislation is therefore the primary source of law, and court decisions of much less importance. Chinese and Portuguese are the official languages of the present legal system, however most legislation (including the five major Codes, based on their Portuguese equivalents) were previously drafted in Portuguese.

Macau describes its legal system as 'founded on a strong tradition of adherence to the rule of law and judicial independence'.[5] The Basic Law makes the judiciary independent. The Court of Final Appeal is the highest judicial authority in the Macau, with a Court of Second Instance, and a Court of First Instance below it.[6] There are some specialist tribunals, of which the most relevant is the Administrative Court.

2. Privacy protections in Macau's general law

Prior to the enactment of its data privacy statute, the law of the Macau already had what was described by Gonçalo Cabral, Legal Adviser to the Macau Government following the retrocession, as a 'host of rules that guarantee some degree of protection to the privacy of personal data and information'.[7] As will become clear from this section, it is necessary to read Macau's data privacy law (PDPA) in light of the extensive civil and criminal penalties possible under the general law.

2.1. Protections in the Macau SAR Basic Law and under the ICCPR

Macau's Basic Law[8] provides in article 30 bis that 'Macao residents shall enjoy the right to personal reputation and the privacy of their private and family life'. By article 32, there may not be infringement of 'freedom and privacy of communication' except where 'in accordance with the provisions of the law to meet the needs of public security or of investigation into criminal offences'.

Numerous other provisions refer to rights which could imply also rights of privacy, including that 'human dignity…shall be inviolable', and 'homes and other premises…shall be inviolable' and protected against arbitrary or unlawful search, or intrusion.[9] Such rights also apply to persons other than residents in Macau.[10] Normally a court would apply other legislative provisions (e.g. the Civil Code), instead of the Basic Law provisions alone, but arguments based on Basic Law provisions alone are possible, particularly in cases concerning human rights.

Macau is not a member of the Asia-Pacific Economic Cooperation (APEC), unlike China, Hong Kong, and Taiwan. Like Hong Kong, it was a founding member of the World Trade Organization (WTO) in 1995.[11] Macau SAR is not a party to the International Covenant on Political Rights 1966 (ICCPR), but the provisions of the ICCPR 'as applied to **(p.270)** Macao shall remain in force and shall be implemented through the laws of the Macao Special Administrative Region' according to article 40 of the Basic Law. ICCPR Article 17 concerning privacy is therefore part of Macau's law. The ICCPR did apply to Macau while it was a Portuguese colony.[12] Macau submitted, via the PRC, a report to the UN Human Rights Committee (HRC) in 2011 on its compliance with the ICCPR.[13] The HRC did not

raise any issues concerning privacy protection under Article 17, and nor did various non-governmental organizations that made submissions to the HRC (although they were very critical in other respects).[14]

Macau is not known for intensive surveillance, except in its casinos. The Macao SAR Resident Identity Card is a contact-based chip card which contains on its face the holder's photo, name, date of birth, height, and ID number. A contactless electronic identity card is also available.[15]

2.2. Protections in the Civil Code

In the Macau Civil Code,[16] enacted in 1999 just before the Portuguese handover to China, is the most general provision concerning privacy. Article 74, states (in translation):[17]

> 1. Everyone shall keep confidential the intimacy of private life of others.
> 2. The extent of confidentiality is defined in accordance with the nature of the case and the condition of the persons; namely, the confidentiality shall be bounded by the context which, by his own acts, the person keeps reserved and, for public figures, by the relationship between the facts and the reason of notoriety.

2.3. Protections in the Criminal Code

This is supported by further provisions in article 75 (Confidential letters), article 76 (Family memories and other confidential writings), and article 78 (Right to personal history), 'the exclusive right on the publication and use of the events of one's own personal history'.[18]

Article 79 (Protection of personal data) goes further, and prescribes, as summarized by Cabral:[19]

> (a) The duty, when collecting personal data for computer processing, to do it in strict obedience to the purposes of the collection and to inform the persons concerned about such purposes.
> **(p.271)** (b) The right of every person to know about any data on himself or herself stored in any computer databases and the purposes of the collection, as well as the right to demand the rectification or update of such data, except when laws require secrecy of criminal procedures.
> (c) The creation of an authority in charge of monitoring the collection, storing and use of computerized personal data, authorizing access to a third person's personal data contained in any computerized database, and authorizing the interconnection of computerized databases

Breaches of these provisions, or threats to breach them, are torts and can be restrained or indemnified if there is either economic and non-economic loss.[20] The fundamental data privacy principles (from a European perspective), and the main obligations of a data protection authority, were therefore set out in Macau's Civil Code as legal rights seven years before the (post-handover) enactment of the PDPA. No cases are known to have

arisen from these provisions.[21]

2.4. Protections in the Penal Code

Macau’s 1995 Penal Code also includes both general protections, for privacy and specific protections for personal data, in articles 184–93. The general protections in article 186 make it an offence to do any of the following acts:[22]

> (a) the interception, recording, use, transmission, or disclosure of a private telecommunication;
> (b) the taking, recording, use, or disclosure of another’s picture or ‘intimate places or objects’;
> (c) eavesdropping;
> (d) the disclosure of facts related with another’s private life or health condition.

Article 187 provides that an offence is committed by ‘whoever creates, keeps or uses a computerized base of data on political or philosophical ideology, religion, race or private life of individuals which allows the identification of the data concerning each individual’.[23] ‘Sensitive’ data is therefore protected by Macau’s criminal law. Penalties (jail sentences or fines) may be tripled if crimes are committed via the media, or with intention of reward or to cause damage.[24]

Prosecutions under articles 184–93 are quite common, as shown in Table 9.1.[25] Prosecutions occur under these sections rather than under the PDPA where these offences are regarded as more serious than a PDPA breach. There are numerous other provisions in Macau law protective of privacy and confidential relations.[26]

2.5. Other statutory provisions

There are provisions in other Acts relevant to privacy which can result in torts, offences, administrative penalties, or disciplinary action. Cabral gives examples of limits on media **(p.272)**

Table 9.1 Criminal prosecutions in privacy-related matters

Crimes against private life

Types of crimes	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009
Violation of a person’s home	35	52	62	99	84	90	68	62	47	58
Disclosure of private life	3	8	11	8	3	22	57	89	95	91
Other crimes	2	1	0	2	3	2	4	0	5	8
Total	40	61	73	109	90	114	129	151	147	157

publication in relation to sexual offences, blocking of access to administrative files to protect the privacy of others, detailed laws on criminal records, disallowance of evidence obtained by intrusions into privacy, and limits on access to civil registries.[27]

3. Macau's Personal Data Protection Act 2005

The Personal Data Protection Act was enacted in 2005, making it one of the earlier data privacy laws in Asia.[28] It is administered by the Office for Personal Data Protection (OPDP).[29]

3.1. History of the data privacy law

The formation of a data protection authority was first discussed by legal officials as early as 1998, possibly influenced by developments in the Portuguese legislation at that time.[30] The president of the Legislative Assembly ordered a study by its legal experts, which concluded that privacy and data privacy are required to be protected in the legal system of Macau and that a specific data protection Act should be formulated. In 2005 eight legislators proposed legislation which was almost a copy of Portugal's law, though they claimed that they also used Hong Kong's ordinance as a reference. The main difference is in the formation of supervising public authority, because it is considered that this function is legally reserved to the government by the Basic Law. The proposal was endorsed by the Legislative Assembly and sent to a Standing Committee. After consultations with, and submissions from, the government and the public, press discussion, and visits to the Hong Kong Commissioner's office, the Committee presented a legal Opinion on the proposal, including proposed amendments. The Law was passed by the Assembly in August 2005 and came into force in February 2006.[31]

The Office for Personal Data Protection

Macau's Chief Executive ordered the formation of a supervising authority, the OPDP, in March 2007, 'operating independently under the supervision of the Chief Executive',[32] and **(p.273)** designated a coordinator.[33] The OPDP can exercise all the legal power attributed to the supervising authority by the Act. As is common legal practice in Macau, the nature of the OPDP is as a 'project' until a law governing the organization of the Office is passed. It is intended that this law will establish an independent authority. After six years, no law formally establishing the OPDP has been passed, one of a number of legislative delays which are a matter of public criticism in Macau. There are also no regulations setting out procedures for compliance with the Act. In 2012 the OPDP became a member of the Asia-Pacific Privacy Authorities (APPA), and of the Global Privacy Enforcement Network (GPEN), and it has been an observer since 2008 at the International Conference of Data Protection and Privacy Commissioners (ICDPPC), which has membership criteria requiring independence.

The OPDP's initial approach was that since an EU-style data protection law is quite new to Chinese society, careful implementation was needed, with an emphasis on public education, but it considered that within two years most public and private sector entities in Macau were aware of the Act and the penalties for non-compliance.

3.2. Scope of the PDPA

The PDPA is of the broadest scope,[34] covering both the public and private sectors with few exceptions. It applies to all processing of personal data whether by automatic means or as part of manual filing systems. Processing for 'purely personal or household

purposes' is exempted (as is normal), but an exception is made for processing 'with the purposes of systematic communication and dissemination'. Macau is therefore able to deal with individuals who use the Internet to disseminate personal information about others without consent, whereas most jurisdictions cannot do so via data protection laws. The Act also explicitly applies to video surveillance and other forms of processing sound and images. The definition of 'personal data' is a conventional one based on the capacity of data to identify a data subject.

Controllers and processors

There is also a conventional distinction, as found in European laws, between a 'controller' who, alone or jointly, determines the purpose and means of processing, and a 'processor' who processes personal data on behalf of a controller.[35] Any processor (or sub-processor) must not process personal data except on the basis of instructions from the controller, unless required to do so by law.[36] If the carrying out of these instructions breaches the Act, it seems that the controller will be vicariously liable, but possibly not otherwise.

As well as the requirement to adhere to the controller's instructions, the processor has separate liabilities. The requirements for processing in articles 5–8 and the user rights in articles 10–13 (except the right of access) are expressed generally, and not only as obligations of the controller, and so could be interpreted as applying to controllers. While data subjects can only seek compensation (indemnity) for breaches of those provisions from the controller under article 14, the provisions concerning administrative offences apply to 'bodies which fail to comply' with the obligations,[37] and it is therefore possible, but not certain, that they also apply to processors. The same applies to criminal offences. Security **(p.274)** obligations are also imposed on the processor.[38] The provisions of the Civil Code may also apply to processors.

4. Macau's data protection principles

The data protection principles in the Act are based closely on Portugal's data protection law, and therefore reflect most aspects of the EU's Data Protection Directive. They include such elements as de-identification, automated processing restrictions, the right to object to processing, and other provisions that might be expected in an EU-inspired law. The decisions of the OPDP are notable for their greater use of concepts derived from European data protection law than is the case in other Asian jurisdictions. However, the principles applied by the PDPA are not always identical with those in the Directive.

4.1. Legitimate processing principles and a general principle

The PDPA commences with a 'general principle' that 'processing of personal data shall be carried out transparently and in strict respect for privacy and for other fundamental rights, freedoms and guarantees enacted in the Basic Law'. This reference means that that freedom of speech and other fundamental rights must be balanced against the data privacy interests expressly protected in the PDPA, without need for an express exception for the press, literary works, etc. as is found in other data privacy laws and in Article 9 of the EU Directive. However, some express exceptions are also provided. The effect of this

'general principle' is apparent in a complaint report by the OPDP concerning one government agency which referred to another agency a complaint by the data subject about noise and heating coming from a restaurant above his residential unit.[39] The complainant was correct that his personal data had been disclosed to the second agency without his consent, which was an apparent breach of the PDPA. However, the OPDP considered that it is required by the Basic Law to take into account the International Covenant on Civil and Political Rights, Article 6(1) of which that the right to life must be protected by law. The agency transferred the data 'to protect the lives of [the data subject] and his children' and 'the right to life has priority' over privacy. Such reasoning gives the OPDP a very flexible way to balance other interests against privacy interests.

The criteria in Article 6 for making data processing legitimate are the basic requirement of 'unambiguous consent of the data subject', or any of the same five exceptions as in Article 7 of the EU Directive. For example, a government agency was fined for MOP8,000 (US$1,000) for recording telephone complaint calls without proper consent. It had set up the telephone recording system to assist handling telephone complaints, and to evaluate staff performance. The system failed to provide the automatic voice reminder function to inform callers that their conversations would be recorded. The agency's staff then failed to give a verbal notification before recording a complainant's call, and without obtaining his consent. This revealed a systematic failure to obtain proper consents from the data subject, and the agency was held to therefore lack legitimacy for processing the complainant's data.[40] Article 5 adds all of the 'data quality' requirements found in Article 6 of the EU Directive.

(p.275) Sensitive data

'Sensitive data' has essentially the same meaning as in the EU Directive, but with 'genetic data' explicitly included.[41] Its processing is prohibited, except where allowed by article 7(2)–(4) or article 8, which are, in general, equivalent to provisions in the EU Directive.

An example is where a Readers' Charity Fund established by the Macao Daily News disclosed through the newspaper the personal data of the Fund's beneficiaries, including name, gender, age, place of residence, and the diseases and difficulties they suffered. The OPDP considered that this disclosure was within the fund's legitimate purposes, and 'was not over-disclosure' because it allowed the public to supervise the use of the fund. Although the applicants knew that unless their personal information was disclosed via the media they would not be eligible for the subsidy from the fund, the fund was nevertheless in breach of article 6 of the law because it was not entitled to rely on the applicants' failures to object to such disclosure, and should have obtained their express consent to disclosure in a way that it could prove.[42]

In another significant decision, the OPDP intervened to cause the suspension of the use of mobile traffic surveillance cameras by the Traffic Services Bureau and the Public Security Police because it lacked legitimacy, because the use might involve the collection and processing of sensitive data outside the sphere of public roads.[43]

Google was fined MOP30,000 (US$3,750) for breaching the PDPA because its Street

View mapping service collected images in the streets of Macau, which are narrow with many alleys crisscrossing each other. This was considered to be the collection of sensitive data that may reveal an individual's private life, etc. without the necessary authorization from the OPDP. Google also breached the privacy law by illegally collecting Wi-Fi and payload data from open Wi-Fi networks and transferring personal information obtained from Macau's Wi-Fi data to the USA. Google has paid the fine imposed for the three offences.[44]

Macau, like Hong Kong, has a separate law concerning 'rehabilitation of offenders'.[45] Among other provisions, if a sentence of imprisonment is not longer than five years, the applicant's civil rights will be automatically restored in five years upon the fulfilment of all penalties, and the criminal record will be removed, provided that there are no further offences.

4.2. Collection principles

The PDPA has the same requirement that personal data is only collected (defined as a form of 'processing') where 'necessary' for other particular types of processing, and must 'not [be] excessive' in relation to the purposes of collection.[46] It therefore appears to be the stricter requirement that data must only be collected where necessary, similar to the EU Directive, described as the 'minimality' requirement,[47] and not the weaker OECD requirement that there be 'some limits' on collection.

(p.276) Collection issues have been a frequent cause of complaint. A construction company could legitimately take photos to document progress on a site that might include images of workers on the site, but it was necessary for the companies involved to respect the 'information rights' of the workers to be told beforehand what was the purpose of the collection of their images in photographs, and the limits on the use of the information. In another example, an institution required visitors to hand over one of their ID documents in exchange for their access pass to the institution, to be exchanged on return of the pass. This was held to be a breach of the principle of 'reasonability' (or proportionality) in article 5, and constituted over-collection of personal data. The institution could invalidate a pass at any time without jeopardizing its security, and did not need to hold ID documents as security.

CCTV in public places legislation

Macau has legislation governing the use of CCTV and similar systems for video or sound recording in public places (including commercial and government-controlled spaces) by police forces using them for security purposes (the 'Legal Regime of Video Surveillance in Public Spaces').[48] Only a brief account is provided here. In most cases capture of sound is prohibited, but police may apply for an exemption. The law limits the use of CCTV to a list of specified purposes including the broad purposes 'safety of public or private property'. It provides that surveillance must be carried out in compliance with the PDPA's requirements in relation to legitimacy of subsequent processing, special protections for sensitive data, and other protections such as security and rights of access. Some areas are 'off limits' for CCTV even if they are public spaces, such as those

used for religious purposes. Many technical aspects come into consideration under the requirement of proportionality, including viewing angles, use of fixed or mobile cameras, possibilities of enlargement and zooms, etc.[49] In the private sector, businesses are required to comply with the PDPA and notify the OPDP regarding their data processing of CCTV. Over 600 applications had been granted by the end of 2013. A simplified notification procedure applicable to some businesses has been introduced.[50]

4.3. Use and disclosure principles

Further processing is prohibited which is 'incompatible' with the purposes of collection,[51] as in the EU Directive, subject to the exceptions for legitimate processing, without unambiguous consent.

One exception is where personal data may be processed without the consent of the data subject 'for pursuing the legitimate interests of the controller or the third party to whom the data are disclosed, except where such interests should be overridden by the interests for fundamental rights, freedoms and guarantees of the data subject'.[52] An investigation of complaints that various shops had posted on their business premises suspect shoplifters' images derived from surveillance systems showed that some had even labelled them **(p.277)** 'thieves' or 'shoplifters'.[53] The OPDP demanded that the shops involved immediately stop posting suspect shoplifters' images, and destroy the related image data, and many did so (but not all, later investigations showed). The OPDP's reasoning was that, although it is legal for institutions to install and run surveillance systems in their premises for security and other purposes of protection of legal rights, the image data derived from surveillance systems for security purposes, including suspect shoplifters' image data, may not be processed or used for something other than these purposes or there is a risk of breaching article 5. This can justify the installation of surveillance systems, but not the public posting of the images of suspected shoplifters, or labelling them as such. If the video data indicates shoplifting, it should be referred to the police.

Excessive or inadvertent disclosures (further processing) are a common source of complaint, as in these examples:

- A retail business was fined MOP10,000 (US$1,250) for publicizing photos and videos of suspects alleged to have stolen items from their shops, despite the Opinion on this subject. It had installed surveillance systems to safeguard its property or other legitimate interests. However the publication was held to be a violation of the principle of proportionality.[54]
- A telephone company was fined MOP4,000 (US$500) for mistakenly sending a customer's bills to another unrelated person's email address over a 10-month period, for failing to take adequate measures to keep its customers' data in its database accurate and up to date, as well as not taking appropriate security measures to protect its customers' personal data.[55]
- A self-employed decorating contractor was fined MOP4,000 (US$500) for disclosure of his debtor and the debtor's wife's personal information. He held

a press conference and disclosed the debtor's residential address in full. This was held to be a violation of the principle of proportionality. However, in relation to the debtor's complaint against two newspapers because they reported his residential address in full, the OPDP held that freedom of press was protected by the Publication Law, and he could only lodge his complaint to a court by civil litigation.[56]

• Following complaints that some employment agencies were posting details of job seekers' personal details in their windows, the OPDP inspected the windows of all employment agencies in Macau, confirming that in some instances very detailed information was posted. According to the Guidelines on Employment Agencies Handling Customer Personal Data issued by the OPDP, in order to adhere to the principles of adequacy and non-discrimination, and ensure the safety of the data, the following data may not be disclosed to the public: ID number or travel document number, nationality, origin, birthplace, birth date, contact details, certificate of criminal record, and other sensitive data (i.e. political beliefs, political society or trade union membership, religion, privacy, racial and ethnic origin, and data concerning health or sex life). The agencies then ceased disclosing such data.[57]

(p.278) • A teaching institution disclosed student names and contact phone numbers in their class groups on a public notice board. The OPDP considered this to be a breach of the security of the students' personal information, because the disclosure was disproportionate. Teachers could be informed of a list of student contact details directly, and if it was necessary to provide other students with a list of those in a class, this could be done by simply listing names or ID numbers without contact details.[58]

4.4. Direct marketing principle

Data subjects must be informed before any direct marketing or 'commercial research' use is made of their person data for or by third parties, and given a right to opt out (right to object). They may also object to such uses at any time,[59] consistent with the provisions in the EU Directive. Persistent telemarketing calls after a customer demanded that calls be stopped have resulted in the OPDP ordering cessation of such calls. A local bank was fined MOP4,000 (US$500) for sending its former client an SMS (mobile phone text message) for direct marketing, ignoring the client's request to stop doing so made under his Right of Objection.[60]

4.5. Rights of the data subject

The rights of the data subject in the PDPA are derived very closely from those in the EU Directive.

Right to information and notice

Where information is collected from data subjects, they must be informed (unless they already have this information) of matters including the purposes of processing, recipients, consequences of not providing the information, and rights of access and correction. This

information should be included in 'documents supporting the collection'.[61] Where the information is collected from other sources, the notice must be provided when the personal data is recorded, or no later than when it is first disclosed.[62] An unusual provision is that data subjects should be warned if data is 'collected on open networks' (unless already aware).[63]

Exceptions to the requirements to give notice may arise from other laws, security grounds, criminal investigations, statistical processing, historical or scientific research, or where collection is required by law. In some such cases, the OPDP may need to be notified instead.[64] Collection for journalistic, artistic or literary purposes is also exempted.[65]

Access, correction, and blocking rights

Article 11 gives data subjects comprehensive access and correction rights (equivalent to EU Directive, Article 12). However, it goes beyond the EU requirements in some respects. Data subjects are entitled to be told the reasoning involved in any automatic processing, even if it does not result in automated decision-making. Also, third parties must not only be notified **(p.279)** by the controller of any 'rectification, erasure or blocking' of data, third parties are also explicitly required to 'rectify, erase or block' the data in their own systems. There is also, as in the EU, a right to object 'on compelling legitimate grounds' to a continuation of processing, and to have it cease where justified.[66]

Exceptions are provided where third parties are to exercise the access and correction rights on behalf of a data subject.[67] In matters concerning security or crime, a 'competent authority' does so. The OPDP does so in cases involving journalistic, artistic, or literary records. The data subject's nominated doctor does so for health information.

Right not to be subject to automated individual decisions

Macau is the only Asian jurisdiction to have yet implemented the provision in the EU Data Protection Directive prohibiting systems which make decisions about a data subject or significantly affecting him 'based solely on automated processing of data intended to evaluate certain personal aspects relating to him, in particular his performance at work, creditworthiness, reliability or conduct'. Exceptions are provided where laws or contracts provide safeguards for the data subject's interests, 'particularly arrangements allowing him to put his point of view'.[68]

4.6. Security principle

The PDPA imposes the same obligation on controllers as in the EU Data Protection Directive, i.e. to 'implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing'.[69] The controller must ensure that any processors also carry out these obligations and are bound to do so (discussed further in section 5.3 of this chapter). In addition, a lengthy list of specific security obligations is prescribed (involving controls of entry to premises, data

media, input, use, access, transmission, logging, and data transmission).[70] The OPDP may waive some of these measures.

A staff member of an agency complained that when he was off work due to illness his medical certificate, including sensitive personal data, was displayed next to the re-arranged work roster. The OPDP found that the agency had inadequate security procedures to protect 'data media' against being read by unauthorized persons. It was fined MOP4,000 (US$500) for the wrongful processing (disclosure) and a further MOP4,000 for the inadequate security provisions.[71]

5. International data transfers from Macau

Macau's law gives a reasonably high level of protection to data subjects in relation to international transfers of personal data, equivalent to that found in the laws of European Union states.

(p.280) 5.1. Extraterritorial application

The Act does not explicitly state its territorial scope in relation to data processing, but is likely to be similar to what is explicitly provided for in relation to video surveillance equipment,[72] namely to apply to any processing outside Macau by a controller based or domiciled in Macau, or any processing by a foreign controller which makes use of equipment located in Macau (equivalent to the EU Directive's Article 4(1)(c)). An overseas controller who, through using a processor based in Macau, makes use of equipment located in Macau, is also likely to be liable under the PDPA, but it may be difficult in practice for a data subject to take action against them. Nevertheless, Google was fined even though it is not a company domiciled or based in Macau.

5.2. Transfers outside Macau

Transfers of personal data to any destination 'outside the MSAR' (Macau SAR), including elsewhere in China, are prohibited unless 'the legal system in the destination to which they are transferred ensures an adequate level of protection' and subject to compliance with the Act. An 'adequate level of protection' is defined in the same terms as the EU Directive, and it is for the OPDP to determine whether a legal system provides such an adequate level of protection.[73] Transfers can therefore only be made under article 19 if the destination jurisdiction, or the particular transfers, already appear on a 'whitelist' maintained by the OPDP or if the OPDP makes a decision in a particular case. Article 20 ('Derogations') then provides a list of exceptions to article 19, very similar to Article 26 of the EU Directive, including where the OPDP issues an authorization because of 'adequate safeguards' being provided.[74]

As yet, the OPDP has not issued any public 'whitelist' decisions stating that particular countries ensure 'adequate protection' in accordance with article 19. They advise controllers to seek an Opinion from the OPDP (see section 6.3 of this chapter, on Opinions). It has issued Opinions on article 19 that some specific transfers involving banking in Hong Kong, Taiwan, and China would have adequate protection. The cases are limited to particular situations as authorizations under article 20, and do not have general

application. The OPDP considers that entities in Macau are now aware now they cannot just simply send data outside Macau without notification to the OPDP. In 2008 there were 27 notifications of transfers outside the Macau SAR, only three of which were from government agencies,[75] and the number has risen to 73 (2012) and 75 (2013).[76] Such information is not available from any other Asian jurisdiction.

Breaches of the data export restrictions have resulted in investigations and fines, particularly in relation to transfers of data to the USA, but also to the Chinese mainland. An employee of a plastic surgery business, when undergoing an operation herself, was assured that the photos taken during the procedure were only for 'before and after' comparisons, but later found them on brochures printed on the mainland to advertise the business in Macau. The business could not explain how this happened. The OPDP found this to be both a breach of the 'special security measures' of article 16, and of the requirements to obtain authorization for transfers outside Macau, and imposed fines for a **(p.281)** total of MOP$8,000 (US$1,000), as well as an injunction under article 43(1) against further use of client photographs for marketing without explicit consent.[77]

In a second case, C was conducting investigations for company A about whether X had breached his obligations to company A in relation to which legal proceedings were underway outside Macau. In Macau, C obtained data from company B about persons with whom X had associated while at company B's hotel in Macau, and then transferred this sensitive personal data outside Macau with company B's knowledge. The OPDP held that this was not legitimate processing by company B of sensitive data, and that none of the exceptions relating to sensitive personal data covered such transfers outside Macau. Company B's knowledge that the data would be transferred outside Macau was equivalent to it doing so, and it had failed to apply for any authorization to do so. It was fined MOP$20,000 (US$2500) for the two infractions.[78]

A third case concerned a company that transferred to the USA all the data contained on the hard disk of the computer of its former CEO, in order to prepare for possible actions it was considering taking against him. The data was 'unselected or unfiltered', and included personal data of persons who had nothing to do with the lawsuit. The OPDP found that there was no current legal action commenced, and that the company, as a locally registered company, could have commenced action against its CEO in Macau, so there was no necessity to transfer the data to a private entity in another country. It should have obtained authorization to do so. It was fined MOP$40,000 (US$5000), half for processing the data without any legitimate basis, and half for breaching the data export requirements.[79]

Google was also in breach of the data export requirements because of its transfer of illegally collected Wi-Fi data to the USA, and was fined MOP$10,000 (US$1,250) on that count.[80]

5.3. Controller and processor obligations in overseas transfers

If data is legitimately transferred overseas under articles 19 or 20, then if the transfer is to an overseas processor acting on behalf of a Macau controller, the controller 'must

ensure compliance' by the processor with all of 'the technical security measures and organisational measures governing the processing'.[81] This must also be embodied in a contract between controller and processor (or similar binding legal act).[82] The effect is that the data subject can sue the controller for any failures by the processor, and there is also a contract for the benefit of the data subject under which the data subject should (in theory) be able to sue to overseas processor. There is no doctrine of privity of contract in Macau which would prevent this.

5.4. Data imports—is there an 'outsourcing exemption'?

If personal data is imported into Macau for processing, it is uncertain whether the processor in Macau will be required to comply with the PDPA in most respects when processing the data. For the reasons previously explained (see section 3.2 of this chapter), it **(p.282)** is likely that a processor in Macau must apply Macau's law to the processing of data originating overseas, but the penalties for not doing so are uncertain: there may in effect be an 'outsourcing exemption'.

6. Reactive enforcement measures in Macau's law

In relation to reactive, or complaint driven, enforcement, Macau's law has one of the most comprehensive 'enforcement pyramids' of the data protection laws in the Asia-Pacific. A wide range of enforcement measures are provided in the PDPA, as well as the provisions in the Civil Code and Penal Code, which can be exercised without prejudice to the right to submit a complaint to the OPDP.[83]

6.1. Complaints and compliance orders

Individuals can complain to the OPDP, but can also have general recourse to other legal and administrative remedies. The OPDP can and does start 'own motion' (suo moto) investigations, and it can issue administrative fines as a result of such investigations. Since failure to comply with statutory obligations within time limits set by the OPDP is a criminal offence,[84] it seems that the OPDP can issue what in other jurisdictions are called 'compliance orders'. The OPDP or a court is also able to order 'temporary or permanent prohibition of processing, blocking, erasure or total or partial destruction of data', when an administrative or criminal offence is found.[85]

The OPDP intervened to cause the suspension of the use of mobile traffic surveillance cameras by the Traffic Services Bureau and the Public Security Police because it lacked legitimacy, in that the use might involve the collection and processing of sensitive data outside the sphere of public roads. The reasoning and the results are very European in their approach.

6.2. Administrative penalties and criminal offences

Contravention of any of the obligations of processors,[86] the rights of the data subjects,[87] security requirements,[88] or data export requirements,[89] constitute administrative offences carrying maximum fines of either MOP40,000 (US$5,000) or MOP80,000 (US$10,000).[90] Negligence is sufficient for administrative offences.[91] The OPDP is responsible for determining amounts of fines.[92] The OPDP issued three administrative

fines for contraventions up to May 2011: against a government agency for disproportionate disclosure when providing all of the details of a person's ID card to a mediation party who needed to locate them; against a bank for failing to observe a direct marketing opt-out; and against an individual decorating contractor for disproportionate disclosure of personal data. There have been a further seven in 2012, noted in case summaries in this chapter, a total of 12 such sanctions since 2007.

Articles 37–42 set out a very wide range of criminal offences, which must be prosecuted before a court, and generally carry penalties from between six months' to two years' imprisonment, and fines. The offences may be committed by controllers, processors, or **(p.283)** third parties. Their subject matter includes (without being comprehensive): failures to apply for authorization; providing false information to the OPDP; misappropriation or use of personal data for purposes incompatible with the purpose of collection; promoting or carrying out illegal combinations of personal data; failing to comply with statutory obligations within time limits set by the OPDP; continuing to allow a controller access to 'open data transmission networks' after notification from the OPDP not to do so; obtaining unauthorized access to personal data; unauthorized destruction or other forms of interference with personal data; failure to interrupt or block processing of data when in a position to do so; and violation of duties of secrecy. The breadth of these potential offences is such that many intentional actions that the OPDP could deal with by an administrative penalty, could also be dealt with as offences before a court. It will often be less expensive and more appropriate for all concerned if the former approach is taken. The other reason why there are very few prosecutions for offences under the PDPA is that, where an equivalent offence under the Penal Code is regarded as more serious, prosecutors usually proceed under those provisions, not the PDPA (see section 2.4 of this chapter for such prosecutions).

6.3. Adverse publicity

'Public warning and censure' and 'publication of the judgment' (concerning violations) are specific 'additional penalties', as are prohibitions of processing and erasure of data.[93] Such publication is to be a summary of the decision, published in the largest circulation Chinese and Portuguese dailies, and by 'affixing a notice' for 30 days, at the expense of the controller or other respondent.[94] In civil law jurisdictions such public identification of parties to legal proceedings is exceptional, and are equivalent to the 'name and shame' approach adopted in Hong Kong.

6.4. Appeals

Actions, decisions, and fines imposed by the OPDP for administrative offences are subject to appeal[95] to the Administrative Court, but no appeals have yet occurred. Where there is a violation of fundamental rights of an urgent nature, there can be a direct appeal to the Court of Final Appeal against any court decision.[96]

6.5. Judicial remedies—compensation payments

Persons who suffer damage as a result of breaches of the Act are entitled to compensation (indemnity) paid by the controller, unless he proves he is not responsible

for the damage.[97] No such cases have occurred.

7. Systemic enforcement measures in Macau's law

The Macau system requires processors to have more interaction with the data protection authority than occurs under any other data privacy law in Asia. In that sense, it is possibly the most 'bureaucratic' system in Asia at present. Macau puts more emphasis on systemic enforcement measures than most other jurisdictions.

(p.284) 7.1. Notification of processing and categories requiring authorization

The Act has a quasi-registration system, which makes it unusual in the Asia-Pacific. There must be notification under article 21 to the OPDP within eight days of most automated processing of data, or processing of sensitive data, unless an exemption from notification is obtained.[98] There have been 11 categories of exemption authorized since 2007.[99] Some of the exemptions are very broad in terms of activities covered,[100] but they are likely to be quite precise in terms of the data that may be processed, the duration it may be kept, etc., and they do not apply to data interconnections or overseas transfers. The result is that a very large proportion of data processing in Macau does not have to be notified.

Article 22 sets out four categories of processing requiring authorization (or prior checking) by the OPDP, without which authorization the processing is illegal. These are: some processing of sensitive data; processing of credit information; data matching ('combinations', discussed in section 7.2 of this chapter); and use for secondary purposes beyond the purpose of collection ('change of purpose'). Article 20 also requires authorizations for some transfers outside Macau. Extension of the retention period for data also requires authorization.[101]

Such notifications and authorizations must be published in a public register and in the OPDP's annual report. The notification is free. Failure to notify the OPDP of processing can result in fines up to MOP100,000 (US$12,500), or double that if the data should have been subject to prior authorization.[102] There have been 244 applications for authorization in the five years 2007–11, and 1,129 notifications.[103] However, by the end of 2013 there had been less than 100 authorizations of any type.[104] It appears that a significant percentage of applications for authorization are not approved. Details of authorization applications not approved are not published, but of 267 approval applications finalized from 2007–13, only 57 (21 per cent) were approved,[105] so this is clearly not a 'rubber stamp' exercise.

During 2008, the second year of its operation, the OPDP applied articles 21 and 22 to all levels of government agencies in the Macau SAR government. This resulted in 402 notifications of personal data processing. By 2013 the notification and authorization regimes were complete for the public sector. It seems that existing public sector practices were examined and given authorizations (where justified) progressively over five years. This has not yet been done for the private sector, but is now being planned and an implementing regulation drafted.[106]

7.2. Authorization of data matching ('combinations of data', or 'interconnection')

The 'combination of personal data' requires OPDP authorization, on application from the controller(s), unless it is provided for in a law or regulation. The criteria 'combinations' **(p.285)** must satisfy to be approved include being necessary for the data controller's legitimate purpose and interests; not reducing the fundamental rights and freedoms of data subjects; have adequate security; and take account of the types of data involved.[107] Hong Kong's law also has provisions dealing with such data matching, but Macau's provisions are unusual.

In 2008, the OPDP reported receiving 151 applications for authorization of personal data combination (interconnection), as a result of the OPDP issuing a circular in late 2007 requiring all government agencies to seek such authorization. In 2012 all 20 authorizations issued were for 'interconnections' between various government agencies. In previous years there were often a mix of applications for interconnections between government entities, and for those between private sector entities, including between different banks (sometimes overseas) and between local braches of companies and overseas head offices. How many are refused is not stated.

7.3. Advisory OPDP functions—Opinions, Guidelines, and Codes

On request from a controller,[108] the OPDP will provide formal Opinions on issues of interpretation of the Act, and these Opinions are published on its website and in its Annual Report. To 2012, 19 such Opinions had been issued, but only two were available in English.[109] The OPDP also publishes Guidelines on significant aspects of the operation and interpretation of the Act. Eleven had been issued to 2013, but only seven are available in English.[110]

The Act encourages professional bodies and other bodies representing other categories of controllers to submit draft codes of conduct for approval, but registration by the OPDP only 'has the effect of a declaration of [a code's] lawfulness but does not have the nature of a legal provision or a statutory regulation'. So registration of a code only indicates that its provisions are consistent with the Act, in the view of the OPDP. There are no codes as yet.

8. Transparency and responsive regulation in Macau

The official languages of Macau are Chinese and Portuguese, but a substantial amount of information is translated by the OPDP into English. Although only the 2008 and 2009 *Annual Reports* of the OPDP are as yet available in English (but are up to date in other languages), summaries of a large number of complaint investigations are available in English, and it seems that all complaint summaries published are eventually translated into English.[111] The complaint summaries are the most valuable information on the enforcement of the Act, and are used to provide examples throughout this chapter. Opinions, Decisions and Authorizations are also translated to English, but not as comprehensively. Substantial information is therefore available for assessment of the OPDP's effectiveness, even without benefit of translation, but the limits of the material available without translation must nevertheless be borne in mind. For the purposes of

this study, **(p.286)**

Table 9.2 Investigations where summaries published, and where sanctions resulted

Year	Investigations*	Summaries†	% Summarized	Sanctions	% Sanctioned
2007	15	6	40	0	0
2008	30	6	20	0	0
2009	29	10	35	1	10
2010	43	15	35	0	0
2011	76	40	56	3	4
2012	118	31	26	7	6
2013	103	45	44	8	8
Total	414	153	40%	19	6%

(*) These figures are for completed investigations, not new investigations opened.

(†) The Portuguese version of the summaries was counted. Publication is to 14 March 2014.

key statistics from the 2010–12 Annual Reports have been translated from the Chinese version.[112]

The available information concerning investigations by the OPDP (whether in response to complaints or ‘own motion’ investigations) is summarized in Table 9.2.

In the first seven years of the operation of the OPDP, 2007–13, it investigated 414 complaints, an average of 69 per year, and the number per year is now over 100. The ratio of complaint summaries to matters completed was 40 per cent. The number of investigations completed each year has more than tripled since 2008, the first full year of operation. These are impressive figures, in terms of transparency, by comparison with any other jurisdictions known. From 2007–12, there was a 6 per cent likelihood that an investigation would result in the imposition of a sanction, rising to nearly 8 per cent in 2013.[113] In all cases to date, the sanctions applied have been administrative fines or requirements to change practices. Other avenues of remedy have not yet been used. The OPDP Annual Reports are informative but give an incomplete picture of outcomes resulting from sanctions imposed. Nevertheless the table shows a sufficiently high level of the transparency for Macau’s data protection system to contribute to ‘responsive regulation’ (see Chapter 3, and Asian comparisons in Chapter 18). While far from perfect, Macau has one of the highest levels of transparency of all the Asian privacy jurisdictions.

9. Conclusions—a successful and responsive ‘transplant’

Macau’s operation of a European-style data privacy law in a prosperous, predominantly Chinese society, gives the PRC the opportunity to consider how such a law might work in China as a whole, and other Asian countries a similar opportunity for comparison.

However, there is little evidence to suggest that this model will be followed elsewhere. Being based so closely on the EU Directive, Macau's legislation adopts the higher standard of 'European' principles. However, as legislation which has been in operation for nearly a decade it lacks some elements now found in other Asian laws such as data breach notification requirements, 'no disadvantage' provisions or an 'anonymity' minimum collection provision (see Chapter 17, section 6.3).

Macau's data privacy principles have been modelled closely on those in the EU's Data Protection Directive (via Portugal's legislation), but they have been customized carefully to **(p.287)** fit the administrative environment and other circumstances of Macau. Although the subject matter of complaints and the penalties in the majority of cases are 'small scale', this is not unusual for data privacy legislation, and there are notable exceptions such as the Google Street View and the Security Bureau findings.

Macau's legislation has now been in force for the best part of a decade, making it one of the older Acts in Asia. It is exceptionally transparent, though not perfect, in its documentation of how enforcement of the legislation functions, even going so far as to make considerable information available in English, as well as the two official languages, Chinese and Portuguese. One improvement still necessary is to provide more information about remedial outcomes resulting from the Act, although Macau already publishes a high proportion of complaint summaries to complaints resolved, and so this is already substantially achieved.

Although not all types of sanctions available from the PDPA are yet in active use, a good 'enforcement pyramid' is available, and the considerable number of complaint summaries available demonstrates that administrative fines are often used by the OPDP. Prosecutions also often occur under other legislation. Civil actions for compensation are not yet common. The combination of fines, prosecutions, and publicity appears to work well in such a small jurisdiction. This does seem like a successful 'transplant' of a European model, one that has then been adapted in its administration to local conditions.

Notes:

([1]) Austin Coates, *A Macao Narrative* (Oxford University Press, 1978), p. 27.

([2]) Kevin K.S. Tso, 'Fundamental Political and Constitutional Norms: Hong Kong and Macau Compared' (2012) 13(1) *Australian Journal of Asian Law*, p. 4 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2159544>.

([3]) Tso, 'Hong Kong and Macau Compared', pp. 4–5.

([4]) Tso, 'Hong Kong and Macau Compared', p. 5.

([5]) 'The Legal and Judiciary System' (Government of Macau, July 2013) <http://www.gcs.gov.mo/files/factsheet/Law_EN.doc>.

([6]) As in Hong Kong, the Court of Final Appeal must refer to the PRC National People's

Congress Standing Committee issues arising in cases which involve interpretation of aspects of the Basic Law concerning affairs which are the responsibility of the PRC Government, or the relationship between central PRC and SAR authorities. This has not yet occurred.

([7]) Gonçalo Cabral, 'The Legal Protection of Personal Data in Macau' (Asian Data Privacy Forum, Hong Kong, 27 March 2001) <https://www.pcpd.org.hk/english/infocentre/files/Macau.doc>. The following account has been assisted by his analysis, but departs from it on some points.

([8]) Basic Law of the Macao Special Administrative Region of the People's Republic of China <http://www.umac.mo/basiclaw/english/main.html>.

([9]) Basic Law, arts. 30 and 31, respectively.

([10]) Basic Law, art. 43.

([11]) Tso, 'Hong Kong and Macau Compared', p. 7.

([12]) It became a matter of dispute before the UN Human Rights Committee as to whether the Optional Protocol also applied to Macau up to the 1999 handover, but a majority held that it did not: *Kuok Koi v Portugal* (Human Rights Committee, communication 925/2000); discussed in Sarah Joseph and Melissa Castan, *The International Covenant on Civil and Political Rights: Cases, Materials and Commentary* (Oxford University Press, 2013), pp. 93–6.

([13]) *Initial report submitted by the Macao Special Administrative Region of the People's Republic of China in light of Article 40 of the International Covenant on Civil and Political Rights* (Human Rights Committee, UN, 12 May 2011) (hereinafter 'Macao report to UN Human Rights Committee').

([14]) *List of issues to be taken up in connection with the consideration of the initial report of Macao, China (CCPR/C/CHN-MAC/1) adopted by the Human Rights Committee at its 105th session, 9–27 July 2012* (UN Human Rights Committee, 5 September 2012); 'Human Rights Issues in Macau 2013' (New Macau Association, December 2013).

([15]) 'Macao SAR Resident Identity Card' (Government of Macao) <http://www.dsi.gov.mo/idcard03_e.jsp>.

([16]) Decree-Law no. 39/99/M or 3 August 1999.

([17]) Jorge A.F. Godinho, 'The Macau Civil Code—A Partial English Translation' (SSRN, 12 September 2013) <http://ssrn.com/abstract=1280595>.

([18]) Cabral, 'The Legal Protection of Personal Data in Macau', pt. III.

([19]) Cabral, 'The Legal Protection of Personal Data in Macau', pt. III; no translation of art.

78 is available.

([20]) Cabral, ‘The Legal Protection of Personal Data in Macau’, pt. III.

([21]) Advice received from Mr Ken Yang, OPDP (email to author, 21 January 2014).

([22]) Cabral, ‘The Legal Protection of Personal Data in Macau’, pt. IV.

([23]) Cabral, ‘The Legal Protection of Personal Data in Macau’, pt. IV.

([24]) Cabral, ‘The Legal Protection of Personal Data in Macau’, pt. IV, referring to art. 193 of the Criminal Code.

([25]) *Macao report to UN Human Rights Committee*, p. 72.

([26]) *Macao report to UN Human Rights Committee*, pp. 74–9.

([27]) Cabral, ‘The Legal Protection of Personal Data in Macau’, pt. V.

([28]) Some of the following is derived from Graham Greenleaf, ‘Macao’s EU-influenced Personal Data Protection Act’ (2008) 96 *Privacy Laws & Business International Newsletter*, pp. 21–2.

([29]) The website of the OPDP is at <http://www.gpdp.gov.mo/> and select ‘English’ to view the Act in English <http://www.gpdp.gov.mo/index.php?m=content&c=index&a=lists&catid=183>.

([30]) The history of the law is documented in a book published by Macao’s Legislative Assembly (in Portuguese and Chinese): see *9º volume—Lei da Protecção dos Dados Pessoais* <http://www.al.gov.mo/colect/col_lei-01/col_po.htm>.

([31]) Ken Yang, ‘Effective Approach in Implementation of Data Protection Law: Macao’s Experiences’ (Powerpoints, OPDP Macao, 3rd Asian Data Privacy Scholars Conference, Hong Kong, July 2013).

([32]) ‘About us’ section <http://www.gpdp.gov.mo/en/>.

([33]) As at the time of writing in 2013, since establishment of the office, the position of OPDP coordinator has been held by Ms Sonia Chan.

([34]) PDPA (Macau), art. 3.

([35]) PDPA (Macau), art. 4, definitions of ‘controller’ and ‘processor’.

([36]) PDPA (Macau), art 17.

([37]) PDPA (Macau), art. 23.

([38]) PDPA (Macau), art. 15(3).

([39]) 'Public Department transferred case to Bureau B without citizen's request' (OPDP, Investigation File:0059/2010/IP, 2012).

([40]) 'Public Department A recorded phone calls without obtaining callers' consent' (OPDP, Investigation File no. 0020/2011/IP).

([41]) PDPA (Macau), art. 7.

([42]) 'The Fund disclosed personal data of beneficiaries' (OPDP, Investigation File no. 0007/2008/IP).

([43]) 'Mobile Video Traffic Monitoring System' (OPDP, Investigation File no. 0008/2010/IP).

([44]) 'Google Street View cars collected data of imaginary [sic] information and Wi-Fi Network in Macao' (OPDP, Investigation File no. 0013/2010/IP).

([45]) Decree No. 27/96/M; see 'Certificate of Criminal Record' on 'Questions and Answers' <http://www.dsi.gov.mo/QAndA_e.jsp>.

([46]) PDPA (Macau), arts. 6 and 5(1)(3).

([47]) Lee Bygrave, *Data Protection Law: Approaching Its Rationale, Scope and Limits* (Kluwer, 2002), pp. 59–60.

([48]) *Legal Regime of Video Surveillance in Public Spaces* (Macau) (no English translation available); See <http://bo.io.gov.mo/bo/i/2012/12/lei02.asp> (in Portuguese) or <http://bo.io.gov.mo/bo/i/2012/12/lei02_cn.asp#2> (in Chinese).

([49]) Guidance is contained in an OPDP Opinion on the Law (n.0005/P/2012/GPDP) (not available in English).

([50]) 'The Processing of Personal Data by Video Surveillance System for Security Purposes' (OPDP, Authorization No. 01/2013).

([51]) PDPA (Macau), art. 5(1)(2).

([52]) PDPA (Macau), art. 6(5).

([53]) OPDP Opinion 2 of 2009.

([54]) 'Shops posted images of suspect shoplifters derived from their surveillance systems' (OPDP, Investigation File no. 0012/2009/IP).

([55]) 'A telecommunication company sending e-bills to unrelated person' (OPDP, Investigation File no. 0007/2011/IP).

([56]) 'The names and home address of a debtor and his wife were disclosed at a press

conference' (OPDP, Investigation File no. 0028/2009/IP).

([57]) 'Employment agencies posted job seekers' personal data' (OPDP, Investigation File no. 0006/2008/IP).

([58]) 'Posting students' personal data' (OPDP, Investigation File no. 0005/2008/IP).

([59]) PDPA (Macau), art. 12(2).

([60]) 'Promotional SMS sent to a former customer by a bank' (OPDP, Case Investigation File no. 0026/2010/IP).

([61]) PDPA (Macau), arts. 10(1) and (2).

([62]) PDPA (Macau), art. 10(3).

([63]) PDPA (Macau), art. 10(4).

([64]) PDPA (Macau), art. 10(4).

([65]) PDPA (Macau), art. 10(5).

([66]) PDPA (Macau), art. 11(1).

([67]) PDPA (Macau), art. 11(2)–(5).

([68]) PDPA (Macau), art. 13.

([69]) PDPA (Macau), art. 15.

([70]) PDPA (Macau), art. 16.

([71]) Case Note 'Displaying medical certificate publicly', 0030/2011/IP (OPDP, 2012).

([72]) PDPA (Macau), art. 3(3).

([73]) PDPA (Macau), art. 19.

([74]) PDPA (Macau), art. 20(2).

([75]) OPDP 2008 Annual Report.

([76]) Data provided by the OPDP to the author.

([77]) 'A company used before and after plastic surgery photos for promotion without the patient's consent' (OPDP, File no. 0041/2010/IP (OPDP, 2012).

([78]) 'Hotel customers' personal data was forwarded to a third party and transferred outside Macao' (OPDP, Investigation File no. 0013/2012/IP).

([79]) ‘Company A transferred to United States the data stored in the computer used by its former CEO’ (OPFile no. 0068/2012/IP).

([80]) ‘Google Street View cars collected data of imaginary information and Wi-Fi Network in Macao’ (OPDP, Investigation File no. 0013/2010/IP).

([81]) PDPA (Macau), art. 15(2).

([82]) PDPA (Macau), arts. 15(3) and (4).

([83]) PDPA (Macau), art. 28.

([84]) PDPA (Macau), art. 37(1)(5).

([85]) PDPA (Macau), art. 43(1).

([86]) PDPA (Macau), arts. 5–9.

([87]) PDPA (Macau), arts. 10–14.

([88]) PDPA (Macau), arts. 15–18.

([89]) PDPA (Macau), arts. 19–20.

([90]) PDPA (Macau), art. 33.

([91]) PDPA (Macau), art. 35(1).

([92]) PDPA (Macau), art. 36.

([93]) PDPA (Macau), art. 43.

([94]) PDPA (Macau), art. 44.

([95]) PDPA (Macau), art. 36(2).

([96]) PDPA (Macau), art. 29.

([97]) PDPA (Macau), art. 14.

([98]) PDPA (Macau), art. 21.

([99]) See ‘Authorizations about the notification obligations’ at <http://www.gpdp.gov.mo/index.php?m=content&c=index&a=lists&catid=208>.

([100]) For example, data processing for election campaigns; by educational institutions relating to students; relating to users of libraries and archives; relating to administration of employees and service providers.

([101]) PDPA (Macau), art. 5(2).

([102]) PDPA (Macau), art. 32.

([103]) Yang, ‘Effective Approach in Implementation of Data Protection Law’; see the Register at <http://www.gpdp.gov.mo/pubinfo/index_pt.php>.

([104]) Calculated from the ‘Authorization’ at <http://www.gpdp.gov.mo/en/>.

([105]) Figures provided by the OPDP to the author.

([106]) Yang, ‘Effective Approach in Implementation of Data Protection Law’.

([107]) PDPA (Macau), art. 9.

([108]) See ‘Services: Application for Opinion’ section at <http://www.gpdp.gov.mo/en/>.

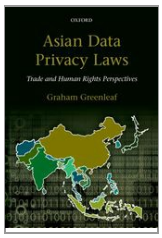
([109]) See ‘Opinions’ section at <http://www.gpdp.gov.mo/en/>.

([110]) See ‘Guidelines’ on the OPDP website. Issues covered include: employee monitoring; monitoring employee attendance using biometrics (fingerprints, hand geometry, facial identification, and others); publication of personal data on the Internet; and merchant processing of cardholder ID.

([111]) For example, the same numbers of complaints were published in 2009 and 2012 in both Portuguese and English, but the number from 2012 is as yet slightly larger for Portuguese than for English.

([112]) Translations by George YiJun Tian, whose assistance is much appreciated.

([113]) These figures were provided by the OPDP to the author.



Asian Data Privacy Laws: Trade & Human Rights Perspectives
Graham Greenleaf

Print publication date: 2014
Print ISBN-13: 9780199679669
Published to Oxford Scholarship Online: December 2014
DOI: 10.1093/acprof:oso/9780199679669.001.0001

Singapore—Uncertain Scope, Strong Powers

Graham Greenleaf

DOI:10.1093/acprof:oso/9780199679669.003.0010

[–] Abstract and Keywords

Singapore's Personal Data Protection Act 2012 is one of the most recent data privacy laws in Asia, fully in force only from mid-2014. Singaporean law does not provide a very supportive context for human rights protections. This chapter explains that the Personal Data Protection Commission (PDPC) will administer a law with a very limited scope, covering only the private sector but with uncertain exceptions. The Act's data protection principles are a minimal version of a 'normal' data privacy law, with a few stronger additions. However, the enforcement provisions provide a serious and multi-faceted 'enforcement pyramid'. Although there are as yet no decisions under the law, the PDPC Guidelines illustrate its expected operation. It is data protection law intended to have a 'pro-business' effect, but it could be enforced strongly within its narrow scope.

Keywords: data protection, privacy, Asia, Singapore, ASEAN, PDPC, data protection authority

(p.290)

1. The Singaporean contexts of privacy protection

Singapore enacted the Personal Data Protection Act[1] (PDPA) on 15 October 2012, and swiftly took steps toward implementation,[2] with ministerial appointment of a Personal Data Protection Commission (PDPC) to administer the PDPA and a Data Protection Advisory Committee to advise the Commission. The PDPA only covers the private sector, and even then with many exceptions and exemptions. The data protection provisions come into effect in July 2014, whereas the 'Do Not Call' provisions (not discussed in this chapter) came into effect in January 2014. References to the PDPA in this chapter are only to the data protection aspects of the Act. In the absence of decisions made under the Act, the PDPC's *Key Concepts Guidelines*[3] and *Selected Topics Guidelines*[4] provide valuable illustrations of the operation of many provisions, although they are not legally binding on the PDPC. At the time of writing, regulations have not yet been made.

1.1. History and political system of Singapore

The significance of the island of Singapore commenced with the agreement obtained by Sir Stamford Raffles in 1919 after complex negotiations involving the Sultan of Johore, allowing the East India Company to establish a trading post on Singapore. The colonial history of Singapore was that of a successful British trading, financial, and services hub and military base, until the brutal Japanese wartime occupation, with no significant industry until after independence.[5] Post-colonial Singapore had a brief period as part of Malaysia from 1963, before it became independent in 1965. Already in power in Singapore after 1959 elections, the People's Action Party (PAP) has retained power through successive elections, uninterrupted until the present. Since independence, Singapore has obtained continually admirable economic growth coupled with a diffusion of prosperity throughout the population, and one of the world highest reputations for both efficiency and lack of corruption in all sectors. Scholars characterize Singapore's regime as the most stable in Southeast Asia[6] but that this stability has also been achieved through factors including limitations on full democracy,[7] in addition to many accomplishments such as very high home ownership. The result is a political system best characterized as semi-democratic or quasi-democratic.

(p.291) 1.2. Legal system of Singapore

Singapore's pre-independence legal history is extremely complex, partly because of Singapore's subordination to a series of larger colonial legal entities (India and the Straits Settlements), and the ad hoc complexities of the separation of Singapore from Malaysia.[8] Singapore's Constitution is a consolidation of a number of documents.[9] It has a unicameral legislature, and Bills are enacted by the usual methods of Westminster-style legislatures. Singapore's court system comprises the Supreme Court (Court of Appeal and High Court) and State Courts. Issues concerning the interpretation of the Constitution may be referred to a special tribunal of three Supreme Court judges by the President.[10] Singapore received the common law and equity of the English legal system during the colonial period. The position of UK statutes was resolved in 1993, to the effect that no English legislation was of any effect in Singapore except that named in the Application of English Law Act 1993 (Singapore),[11] and by the July 1994 Practice Statement of Singapore's Court of Appeal which stated that with the abolition of appeals to the Privy Council, the Court of Appeal was no longer bound by its previous decisions, nor those of the Privy Council.[12]

The Supreme Court has the power to decide the constitutionality of legislation, but on only one occasion has the High Court found legislation to be unconstitutional and this was reversed by the Supreme Court. In addition, Singaporean courts have not been willing to give broad and protective interpretations to individual rights found in the Constitution. They are 'generally trusting of the executive and have often endorsed state imperatives in their decisions regarding fundamental liberties, rather than put the executive on strict proof for any derogations of individual rights or liberties'.[13] Because of these factors, and the limited scope of privacy-related rights in Singapore's Constitution (see section 1.4 of this chapter), the approach of constitutional courts in many other Asian jurisdictions, which have often found legislation interfering with privacy to be unconstitutional (see Chapter 17, section 2.2), is not likely to occur in Singapore.

Although Singapore has in various ways a state-dominated legal system, it is seen as one of the 'key pillars to Singapore's success', with its courts having obtained 'an enviable reputation for efficiency and the quality of their judgments'.[14] These factors are likely to enhance the administration of Singapore's data privacy legislation, and to positively influence the quality and efficiency of decision-making by administrative and quasi-judicial bodies such as will administer the PDPA.

1.3. State surveillance in Singapore

Singapore has an extensive and sophisticated system of surveillance of its population. The PDPA does not apply to the Singapore government or public authorities. The key element in the system is the National Registration Identity Card (NRIC) and corresponding **(p.292)** number. Carriage of the card is not compulsory, but its production will often be required in order to obtain government services, stay in hotels, open bank accounts, etc., and it is very commonly required by the private sector in order to enter premises. Other elements of Singapore's overall surveillance system are SingPass, a user-created password Singaporeans must use to access electronic government services, a national online service holding all patients' records from all hospitals and clinics in Singapore, and an Electronic Road Pricing (ERP) system for monitoring road usage and charging for it.[15]

1.4. The absence of non-statutory privacy protections

Singapore provides very little legal protection to privacy outside the new PDPA. It has no explicit constitutional protections of privacy, and it is not a party to any enforceable international agreements protecting privacy. It is uncertain whether there is tort protection against harassment, but otherwise there is no tort of invasion of privacy. Some protection is provided by breach of confidence law.

No constitutional or treaty privacy protections

Singapore is therefore among those Asian jurisdictions without a strong legal context of protection for human rights within which data protection legislation operates. On the other hand, Singapore has one of the highest reputations of any country for lack of corruption in its public sector, and a high reputation for the operation of the rule of law. While overall comparisons between countries on the basis of such factors are very difficult to make, these are factors which should be borne in mind in any comparative assessment of Singapore's data protection regime with other

countries.

Singapore's Constitution has a number of provisions relating to protection of individual liberties,[16] but none of them refers to privacy or to personal information. This is in contrast with the strong constitutional protections of privacy found in many other jurisdictions in Asia (see Chapter 17). Seventeen Asian countries have ratified the International Covenant on Civil and Political Rights 1966 (ICCPR), but Singapore is one of the six Asian countries which are members of the UN but have not even signed the ICCPR (see Chapter 2, section 4.1). It does not therefore make periodic reports to the UN Human Rights Committee. Although Singapore is not a party to any binding agreement concerning human rights, in 2012,[17] the Association of Southeast Asian Nations (ASEAN) heads of state, including Singapore, adopted the ASEAN Human Rights Declaration,[18] as discussed in Chapter 2, section 2.1.

Limited but uncertain protections in common law or equity

Singapore may have taken the lead in common law countries in Asia in developing a tort of harassment, but the question is not settled. In the 2001 High Court of Singapore **(p.293)** *Malcomson Case*,[19] Lee Seiu Kin JC defined 'harassment' for the purpose of this action, as including (non-exhaustively)

> a course of conduct by a person, whether by words or action, directly or through third parties, sufficiently repetitive in nature as would cause, and which he ought reasonably to know would cause, worry, emotional distress or annoyance to another person.

'Surely in respect of intentional acts that cause harm in the form of emotional distress, the law is able to provide a recourse', he concluded after reviewing the authorities and finding that none prevented development of a tort of harassment in Singapore. He granted a comprehensive injunction restraining the defendant contacting Malcomson or employees of his company, either directly or indirectly, in any way, or sending anything to either or them. However, in a 2013 decision of the same court, Choo Han Teck J was 'not convinced that a cause of action exists presently at common law to found a claim in the tort of harassment',[20] and considered that in Singapore this was a development that could only be taken by the legislature. Singapore has now enacted the Protection from Harassment Act 2014, which covers stalking and online sexual harassment and bullying, and in some cases will apply even where either the accused or the victim is located outside Singapore.[21]

2. The PDPA's scope—limited, with uncertain boundaries

The complex provisions defining the scope of the PDPA reveal key potential weaknesses. This section considers its exclusion of the public sector and various private sector exemptions, both of which are of very broad but have uncertain boundaries, as well as exemptions favouring freedom of speech, which are very narrow.

2.1. The PDPA's origins

Singapore is one of the last economically advanced countries to adopt a comprehensive data privacy law for its private sector. The gestation of the law is traced by Chesterman,[22] commencing with a 'Model Code' of 10 principles, developed by Singapore's National Internet Advisory Committee.[23] It subsequently became the basis for the 'TrustSg' trustmark administered by Singapore's National Trust Council, a system 'not regarded as particularly effective', although some revocations of trustmarks have occurred.[24]

An inter-Ministry committee started to consider data protection legislation in 2005, and proceeded through a series of overseas investigations, consultation papers, and submission rounds. The PDPA which emerged from the process is in most respects the same as the draft Bill announced earlier in 2012 by the then Ministry of Information, Communications **(p.294)** and the Arts,[25] which confirmed many features foreshadowed in a previous discussion paper. However, other features were jettisoned, generally resulting in improved privacy protections. Chesterman sees the primary motivations for the Singapore legislation as economic, rather than civil liberties or consumer protection, concerns which aim to increase the flow of personal data into Singapore by making it become a 'trusted node'.[26] Whether the Act will or should succeed in creating such international trust is arguable. The limitations of the scope of the Act will be the, the main focus of sceptical consideration.

2.2. Personal data—identifiable, 'publicly available', and deceased

A conventional definition of 'personal data'[27] means that the starting point of the PDPA is that it applies to any information which, in practice, can be used by an organization to identify a person. The PDPA applies to any 'organization', which is given a wide definition.[28] Unusually, the PDPA imposes its restrictions on disclosures and security obligations to data concerning persons deceased for 10 years or less.[29] It does not apply to information 'contained in a record that has been in existence for at least 100 years'.[30] Data protection laws in other Asian countries do not provide protection to the deceased, but there is a precedent in Canada.[31] 'Business contact information' as defined in section 2 of the PDPA[32] is exempt, except where specifically mentioned.[33] However, potential abuse of such information is tempered somewhat by Singapore's existing anti-spam law,[34] and by the Do Not Call provisions in the PDPA.

Publicly available information

The data protection principles do not apply to personal data which is 'publicly available',[35] which is defined to mean 'personal data that is generally available to the public'.[36] Books, newspapers, government public registers, and websites accessible to all are 'available to the public'. However, the word 'generally' must carry some meaning. First, it indicates that the information need not be available to the whole public, and there are difficult questions which follow about whether content for which access must be paid is 'generally available' (and with what limits). Similar questions arise regarding content to which only members of certain organizations or facilities have access (e.g., Facebook, or a credit bureau). Social networks create cascading issues of what is 'general' availability because they allow users to create gradually broadening circles of access to varying amounts of personal data, by nomination of 'friends' and otherwise. Secondly, for such a provision to be consistent with the overall purpose of the legislation, 'generally' available content cannot include content solely because it has been made available through a breach of the data protection principles themselves—at least where it is possible to remove it from further public **(p.295)** availability. The definition also excludes from the Act's scope, personal data which can be 'observed by reasonably expected means' at a location or event open to the public. The PDPC considers[37] that this exempts from the Act examples such as CCTV footage in stores or public streets, and overt filming at public events (even if there is an entry fee). On the other hand, part of a public restaurant might be used for what is clearly a private party even though it is visible, and still be covered, as is the interior of a taxi while it is under hire. Although there is nothing unusual with data protection laws grappling with the difficult question of drawing the line to indicate where personal data which has become sufficiently 'public' so that some or all data protection provisions ought not to apply to it, some other jurisdictions in Asia have reached very different positions, including Hong Kong (see Chapter 17, section 3.2 for comparisons). For example, information available from public registries in Singapore will not be subject to the Act, but in Hong Kong the position is more complex.

2.3. Public sector exclusion of uncertain scope

Among the world's 101 jurisdictions with data privacy laws as at 2013,[38] Singapore is in a very small sub-group in applying such laws to the private sector only (Malaysia, Vietnam and India, and the Qatar and Dubai mini-jurisdictions for their International Finance Centres, are the others). An equally small group applies its laws *only* to its public sector, but the other 90 per cent have laws which cover both sectors, at least to a substantial extent. The PDPA does not apply to the public sector (any 'public agency'), nor to any organization processing personal data on behalf of a public agency.[39] Any organization established by a statute can be gazetted to be a 'public agency'.[40] So data subjects will need to know for whom a company is acting when collecting data before they know whether the PDPA protects them—but they will have no right to know if the company is acting for the government, and no recourse under the PDPA if they hand over personal data under a false assumption of protection. This is a rather nasty Catch-22 with which to start an Act that claims to recognize 'the right of individuals to protect their personal data'.[41] It is a unique Singaporean touch, with no parallels in other Asian data privacy laws. The Minister has stated that the public sector 'has its own set of data protection rules that are based broadly on the same data protection principles',[42] but these are not enforceable by individuals and, even in relation to access and correction of their own records, individuals can only make 'requests'. Even worse, as Chesterman notes, because 'those rules are not public…this statement is difficult to evaluate'.[43] Singapore does not have freedom of information legislation, which exacerbates the uncertainty.

2.4. Private sector exclusions—'known unknowns'

As is usual in data privacy laws, the PDPA does not impose any obligation on an individual 'acting in a personal or domestic capacity'.[44]

(p.296) The PDPA has a longer than usual list of exemptions for uses made for an 'evaluative purpose'[45] which will exempt many uses made of personal data in relation to employment,[46] education, insurance, and 'such other similar purposes as may be prescribed by the Minister'. There are also potential exemptions of unlimited scope because regulations can prescribe that the obligations of the PDPA do not apply to 'any other organisations or personal data, or classes of organisations or personal data'.[47] Further increasing the uncertainty of scope, the PDPC may also, with the approval of the Minister, by order published in the *Gazette*, 'exempt any person or organisation or any class of persons or organisations from all or any of the provisions of this Act, subject to such terms or conditions as may be specified in the order'.[48] So the scope of the PDPA is to a very significant extent undefined: the Singapore government can retrospectively narrow its provisions however it wishes.

In addition, any other 'written law' will prevail over the provisions of this data protection law (to the extent of inconsistency), even if the PDPA is the later law,[49] as will any other rights, privileges (including legal privilege), immunities, obligations (except contractual obligations), or limitations arising from any other laws, whether written or not[50] and no matter when arising. This clause makes the PDPA inferior to all other legislation, past or future, as well as to undefined aspects of common law or equity. Among other things, this means that any of Singapore's many existing sectoral provisions with some effect on data protection will prevail over the PDPA, to the extent they are inconsistent with it.[51] Whether this is beneficial to data subjects will depend on whether there are higher or lower standards in the sectoral legislation (a matter beyond the scope of this chapter), but it will also be confusing. While the inferior position of the PDPA undoubtedly cuts down its scope, the exact effect of this provision awaits judicial interpretation.

The limitations of the private sector scope of the PDPA may be offset somewhat by Singapore's existing sectoral and other laws concerning secrecy and disclosure.[52] In 1999, more than a decade ago, there were already 161 such laws listed in an official report,[53] although none involved comprehensive data privacy regimes. Since then, there have been significant new laws in such sectors as banking and telecommunications, and relating to official secrets, statutory bodies and government companies, statistics, electronic transactions, and computer misuse. Kah Leng Ter considers that, given that the Singapore sectoral laws operate in substitution for the PDPA, their effect will be largely negative on data protection, because they usually:[54]

> contain secrecy and disclosure provisions which typically penalise the unauthorised release of personal information and…do not confer private rights of action or direct remedies that are typically available under data protection laws.

(p.297) ### 2.5. Limited exemptions supporting freedom of speech

There are exemptions allowing collection without consent—but no exemption from other principles—for 'news organisations' solely in relation to 'news activities'. Both were undefined in the Bill as introduced into the legislature, but the PDPA as passed defines both[55] in relation to exceptions to the requirement for consent for collection.[56] 'News activities' is given a broad definition, but a 'news organisation' is limited to organizations which operate newspapers (required in Singapore to be licensed under the Newspaper and Printing Presses Act), newswire services, or broadcasting services (licensed under the Broadcasting Act). Chesterman observes that this seems to imply that online publications are excluded from this exemption.[57] If (and only if) such an online site was able to obtain a licence under the Broadcasting Act, would it be a 'news organisation' and be able to come within the 'news activities' exemption? If this was not possible, then such exclusion from the limited protection given by the PDPA seems inconsistent with the proposals by Singapore's Media Development Authority to regulate online news sites so as to place them on 'a more consistent licensing framework as traditional news platforms'.[58] Unlicensed bloggers and other online commentators will now have increased risks of actions against them, under the PDPA, if they collect personal information without consent in ways which do not fall within other exemptions such as those for personal and domestic activities or 'publicly available' information. Singapore has an international reputation for a low level of press freedom, and one that is falling, not improving.[59] It also has an extremely strict law of defamation, in which balancing public interests against private reputational interests does not play a significant role, and nor does a 'public figure' doctrine.[60] The potential effect of the additional burden on freedom of speech in Singapore, because of the narrowness of the exception for collection without consent, is difficult to predict. There are other exceptions in the PDPA that support freedom of speech, namely, the exceptions for publicly available data (see section 2.2 of this chapter), and data collected solely for artistic or literary purposes (exception from collection limitations only).[61]

2.6. Cumulative effect of exemptions

Taken together, these exemptions and mechanisms for exemptions make the scope of the PDPA little more than a 'known unknown'. However, potential abuses might not eventuate, because governments (and authorities with delegated discretions) exercise **(p.298)** restraint. It is not inevitable that the scope of Singapore's PDPA will be further reduced, though it is a significant risk. Nevertheless, the diversity and breadth of the exemptions from its scope, the open-ended nature of many of them, and the subordination of this Act to all other Acts, have few parallels in data protection laws in their cumulative effect. As a result, the PDPA has a narrower scope than any other Asian data protection law.

3. The PDPA's data privacy principles—mainly minimal

The data protection principles in Singapore's PDPA are, on their face, consistent with the minimum principles of data protection established in the

1980s, in relation to access, correction, data quality, and security. They add a deletion/de-identification requirement. However, this observation is subject to the caveat that the exemptions provided are more extensive than is typically the case in comparable legislation, and are subject to further exemptions by regulations or ministerial decisions. The analysis here is structured differently from the nine principles described by the PDPC.[62]

3.1. 'Finality'—collection, use and disclosure principles, and notice

The notion of 'finality'—that collection, use and disclosure of personal information should be determined by the purpose of initial collection, with few and well-defined exceptions—is central to data protection principles including the OECD Guidelines.[63]

In Singapore's PDPA, the principles concerning collection, use (including secondary uses) and disclosure are based on complex intersections of (a) a purpose that 'a reasonable person would consider appropriate in the circumstances';[64] (b) the actual purpose of collection; (c) notice of this purpose (or subsequent change of purpose);[65] and (d) consent by the data user.[66] Seen in this way, the Singapore PDPA seems to be based on notice and consent (plus a reasonable purpose). If this is so, it would give strong protection to data subjects. However, the substance of this apparently protective approach is reduced a great deal by the following:

(a) Individuals are deemed to have consented ('deemed consent') to collection, use, or disclosure by 'voluntarily' providing their personal data to the organization for that purpose, where it is reasonable to do so.[67]
(b) Where there is deemed consent, no notice is required.[68] Therefore notice (in the form required by section 20) cannot be required for the 'reasonableness' element of deemed consent, because that would be circular. The PDPC's examples are consistent with this approach.[69]
(c) Neither the requirement of consent nor the requirement of notice[70] applies wherever the lengthy schedules of exemptions for collection, use, and disclosure (Second **(p.299)** to Fourth Schedules) apply.[71] While these schedules cannot be discussed in detail here, even a list of their subject matters indicates how extensive they are.[72] The three schedules need to be checked carefully to see exactly which types of exemptions apply to each of collection, use or disclosure. Many of these exemptions are of very broad scope, phrased in very general terms, and are in effect largely undefined.
(d) Collection, use or disclosure without consent can also be required or authorized by any other law.[73] No notice will be required under such circumstances, unless the other law so requires.

Singapore's principles are therefore not based so much on consent and notice but are 'exception-based', with the exceptions based on 'deemed consent', lengthy schedules of exceptions, and other legislation. Seen this way, consent and notice play the role of residual provisions where no exception is available. It is difficult to assess in abstract whether the exceptions or the residual requirements will apply more frequently, however, it appears that Singapore's PDPA only embodies the concept of 'finality' to a limited extent.

The PDPC advises data controllers that it is 'good practice' to review its practices to decide where it should obtain actual consent rather than relying on deemed consent, due to the multiple elements required to establish deemed consent.[74]

Where actual (i.e. not deemed) consent is required, the PDPC's opinion is that failure to opt-out 'will not be regarded as consent in all situations' but 'will depend on the actual circumstances and facts of the case'. Their examples envisage that the 'tick here if you do not wish your personal details to be provided to X' type of opt-out does constitute consent, if it is prominently located in the course of when the data subject is voluntarily disclosing personal data, but an approach such as 'return this opt-out form to us or we will disclose your personal data that we already hold' is not consent.[75]

Direct marketing

The PDPA does not include any separate principle concerning direct marketing (an opt-out principle in the EU Directive[76] and some other laws, and now an opt-in requirement in South Korea and Hong Kong). Marketing issues are dealt with by the general principles **(p.300)** concerning use and disclosure discussed in this part. In addition, the PDPA has extensive provisions concerning a Do Not Call Registry,[77] which is not covered in this study.

3.2. Other data protection principles

The PDPA covers all of the other minimum data protection principles—access, correction, data quality, security, and, to some extent, openness and perhaps 'accountability'—plus deletion which is not included in the minimum principles. Nor is transfer limitation, discussed in the following section.

Access and correction

The access principle requires data subjects to be provided with the personal data about them that an organization possesses or controls 'as soon as reasonably possible'.[78] Access to details of uses or disclosures is required, but only for the year preceding the request. There is a lengthy Fifth Schedule setting out where organizations have the option not to provide access, and a conventional list of conditions where access is prohibited (for example, protecting the privacy of others),[79] unless redaction can satisfy the conditions prohibiting disclosure.[80]

Correction of 'errors and omissions' of data in an organization's possession or control is required,[81] unless the organization considers on reasonable grounds that no correction should be made. Corrected data must be sent to organizations that have received it in the past year, unless they do not need the correction for legal or business purposes.[82] There are exemptions in the Sixth Schedule. Corrections requested but not made must be annotated on the person's file.[83] There is no requirement to alter opinions.[84]

Data quality and security

The 'data quality' principle requires organizations to 'make a reasonable effort' to ensure that personal data they hold is 'accurate and complete' if (and only if) it is likely to be used to make decisions about the data subject, or likely to be disclosed by it.[85] The PDPC stresses the very limited nature of this obligation, but also that what is reasonable depends on the decisions to be made using the information.[86]

There are briefly stated requirements requiring organizations to make 'reasonable security arrangements' to protect personal data in its possession or under its control.[87] PDPC guidelines fill out details of the administrative, physical, and technical measures that organizations should consider may be necessary depending on a number of factors indicating potential seriousness of security breaches.[88]

Some 'openness' and 'accountability' required

Although the PDPC refers to an 'openness obligation',[89] the PDPA obligations are not exactly the same as the OECD 'openness' principle. An organization must develop policies **(p.301)** and practices necessary to meet its obligations under the PDPA, and make information about those privacy policies, and its complaint resolution processes, available on request.[90] This obligation to answer requests is not restricted to data subjects, and therefore goes some way to meet the OECD 'openness' principle, but it does not require disclosure of all the aspects of a company's personal data processing practices suggested by the OECD principle.[91] The PDPA does not require publication of privacy policies (nor did the OECD). The PDPA also implements the OECD 'accountability' principle, because it requires that an organization designates a person responsible for compliance (not necessarily an employee), and also requires business contact information be provided.[92] The stronger version of a 'Privacy Officer' with specific qualifications and obligations is not required by the PDPA. Overall, the PDPA requires a moderate amount of openness. Some companies may choose to go further.

Data retention/deletion

An organization must 'cease to retain' or alternatively, de-identify (anonymize), personal data as soon as it is reasonable to assume both that (a) the data is no longer serving its purpose of collection; and (b) its retention is 'no longer necessary for legal or business purposes'.[93] The reference to 'business purposes' should be read as 'business purposes which are legitimate' (encompassing justifications based both on exceptions and notice, and consent). However, it would always be difficult (perhaps impossible) for a complainant/plaintiff to prove that all 'business purposes' had expired, particularly because section 20 notices will not always (or perhaps even often) be required. It is not clear that the onus is on the organization to prove that there is still a legitimate purpose. The absence of a clear onus significantly reduces the value of this requirement, as it could make business compliance with this obligation optional. The PDPC's guidelines do not explicitly address the question of onus of proof, but examples and statements of best practice assume that organizations will document or demonstrate reasons for retention. Where contracts are involved, businesses may retain records for at least six years from the termination of the contract.[94]

The PDPC's guidelines on anonymization[95] contain many valuable suggestions concerning techniques for reducing risk in the processing of personal data. They point out that anonymized data is not personal data, and consequently Parts III to VI of the PDPA will not apply to it. It is also the case that anonymization satisfies the 'cease to retain' requirement of section 25. The PDPC is careful to correctly stress that '[t]o the extent that an organisation can still identify individuals from dataset X, it is still considered personal data to the organisation', whether the identification is from the dataset itself, or requires the use of other data to which the organization is likely to have access.[96] However, confusion and error could be caused by the list of seven 'anonymisation techniques' given by the PDPC, if data controllers wrongly concluded that use of any of these might be sufficient for anonymization in the sense required by the PDPA. They would very rarely be sufficient. Real anonymization is far more difficult to achieve than is possible from use of **(p.302)** one of these techniques,[97] as the PDPC realizes and illustrates with examples.[98] It does discuss 're-identification and its risks', but there it only refers to risks if the organization intends to publish or disclose the data.[99] The PDPC's guidelines are very valuable, provided organizations do not confuse risk reduction with anonymization.

Sensitive data or processing, and ID numbers

The PDPA does not define categories of data as 'sensitive' or provide special protections for particular categories of data. Nor does it single out particular types of processing, such as fully automated processing resulting in decisions made about individuals, or categories of processing requiring some form of 'prior checking'. In these respects the principles in the PDPA differ from, or fall short of, the 'European' or '2nd generation' set of privacy principles. Consistent with this, the PDPA applies to Singapore's ID system (the NRIC number and card), but through the general application of the Act, not through any special principles. The PDPC's guidelines explain how that applies.[100]

3.3. The minimum set of principles, plus some additions

Singapore's PDPA implements in some way all of the basic OECD Guidelines and Council of Europe Convention[101] principles (except the part of 'openness' principle), as well as two of the additional 'European' principles:[102] collection is limited to what is necessary for purpose (though with wide exceptions); and there is provision for deletion of data (also easily circumvented). The PDPA also includes strong and novel elements not yet included in all or most Asian laws: that the fact of disclosures to third parties are to be included in access requests; that third parties who have had such access be notified if corrections are made; and something like a prohibition on the denial of service where a data subject refuses to provide more than the minimum data necessary (as in South Korea). The Singaporean provision prohibits organizations, as a condition of providing a product or service, from requiring an individual to consent to the collection, use, or disclosure of their personal data beyond what is reasonable to provide the product or service.[103]

On the deficit side, the Act does not include the European-influenced principles of additional protection for sensitive personal data[104] found in the majority of Asian laws. Nor does it include the 'European' elements of controls on automated decision-making or the ability to opt-out from direct marketing, both found in some other Asian laws. Other Asian jurisdictions have also moved beyond these 'European' elements and included innovations such as a requirement to provide anonymous transactions where possible; segregation on consent forms of those items that require consent and those that do not; provision of notice to the data subject when personal data is collected from third parties; deletion of data on **(p.303)** request; a right to block the use of data; or a data breach notification requirement. Other Asian laws have also regulated aspects of the use of data by the private sector not addressed by Singapore's PDPA such as specific regulation of use of ID; use of information found in public registers; and special provision on visual surveillance, although it is possible that some of these issues will be addressed in subsidiary legislation in Singapore. A detailed comparison of all Asian data privacy laws is provided in Chapter 17. Some of these possible additional principles were considered at some point in the consultative documents leading up to the PDPA, but others were not. Reasons for rejection are unclear.

The data protection principles in Singapore's PDPA can be described as a minimal version of a 'normal' data privacy law, with a few valuable additions. They are considerably better than the somewhat derisory version promised by the earlier consultation paper.[105] An important caveat is that, while the principles concerning collection, use, and disclosure take as their starting point the purpose of collection, the 'finality' of that purpose is massively reduced by all of the methods described in section 3.1 of this chapter. When coupled with the very considerable limitations in scope of the PDPA (see section 2 of this chapter), it appears to be an Act with 'more holes than cheese'. Whether this turns out to be the case will depend on how it is applied in practice, by the government's exemption practices and by the PDPC.

4. Intermediaries (processors) and international data transfers from Singapore

Where processing is carried out by an 'intermediary' (the Singaporean term), that processor may be located within Singapore or may be an overseas processor. The general position of local intermediaries is first discussed. International flows of personal data require consideration of number of interrelated issues (see Chapter 3, section 3[106]), some of which also affect purely domestic processing of personal data.

4.1. Exemptions for 'data intermediaries', liability for controllers

The PDPA does not impose 'any obligation on a data intermediary in respect of its processing any personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing', except in relation to the obligations concerning data security[107] and data retention.[108] 'Processing' is given a very broad definition (every type of operation on data including its recording when collected), and 'data intermediary' is simply defined as an organization that processes data on behalf of another organization.[109] The term 'data processor' is often used in other jurisdictions in the **(p.304)** same sense that 'data intermediary' is used in Singapore, and the party for whom the processing is done is often called the 'data controller'. A Singaporean organization will 'have the same obligations…in respect of personal data processing on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself'.[110] The organization that has 'data processed on its behalf and for its purposes by a data intermediary' (the data controller) is therefore vicariously liable for any breaches of the PDPA by the data intermediary (data processor) provided they are done for its purposes.[111] There are many more potential complications in determining when an organization is, or is not, a data intermediary.[112] The PDPC indicates that parties who may be 'agents' of another party at law will not have their obligations in relation to data processing determined solely by that relationship,[113] but by whether the PDPA classifies them as an intermediary.[114]

If the data intermediary processes the data in any way which is not 'on behalf of and for the purposes of' the data controller, the position is reversed: the data processor is liable for any such unauthorized processing which breaches the PDPA (because section 4(2) of the PDPA[115] will not apply and the data protection principles refer in neutral terms to an 'organisation') and the data controller is not vicariously liable under section 4(3). From the perspective of the data subject, it will be essential, but may be difficult, to determine whether a data processor was acting within or beyond the scope of its actual authority when it processed data in breach of a data protection principle, otherwise action will be taken against the wrong party. The data controller is not obliged to give notice to the data subject that a third party intermediary will be involved as a data processor.[116] Where an errant data processor acting outside the scope of its authority becomes insolvent or is otherwise difficult to proceed against, the data subject will have no recourse against the data controller under the PDPA. The data subject may reasonably consider that it is unfair that it is expected to proceed against an unknown and possibly impecunious third party, especially if it is a third party outside the jurisdiction.

Examples given by the PDPC[117] indicate the wide range of circumstances that may create a controller-intermediary (processor) relationship: subcontracting market research and the writing of a report; delivery of a parcel to the address of a named person; and one part of a corporate group processing personal data for other parts of the group. The PDPC notes that it is good practice for a data controller 'to undertake an appropriate level of due diligence to ensure itself that a potential data intermediary is capable of complying with the PDPA'.[118] This is clearly wise advice, given that the data controller may have vicarious liability for breaches of the PDPA by the intermediary. Singapore's approach is superior to that of jurisdictions which explicitly require due diligence, but then impose no liability in relation to actual breaches. The controller needs to use its contract with the intermediary to protect its own position in relation to the PDPA, so as to at least ensure it can be indemnified by the intermediary in the event of breaches.

(p.305) 4.2. Extraterritorial scope

There is no specific provision for extraterritorial operation of the PDPA, in contrast to the draft Bill where there was limited extraterritorial operation for processing actions with a 'Singapore link'. In the absence of any express or implied extraterritorial claims in the Act, of which there seem to be none, it can be concluded that the PDPA only applies to actions (collection, use, disclosure, and so on) that take place in Singapore. This interpretation is consistent with the definition of 'organisation', which explicitly states that it applies whether or not a company (or other entity) is formed or recognized under the law of Singapore or has an office or place of business in Singapore.[119] This means that foreign companies which do not have a physical presence in Singapore can still be liable under the PDPA, but only for actions which take place in Singapore such as collection or disclosure of personal information.[120] In contrast, if they do not store data in Singapore, it is difficult to see how they could be liable for lack of security over such foreign-located data. Assertions of extraterritorial application are unusual in data protection laws in Asia, and usually only benefit only the nationals of the countries concerned (see Chapter 17, section 5). Singapore's approach does not seem to claim extraterritorial jurisdiction for the PDPA, because it only claims jurisdiction over activities that take place in Singapore, but it does have an extraterritorial effect because those activities in Singapore may be the results of data processing activities that primarily occur outside Singapore.[121]

4.3. Liability where there is an overseas processor (intermediary)

The provisions that a Singaporean organization will 'have the same obligations…in respect of personal data processing on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself',[122] do not contain any explicit limitation that they will apply only to intermediaries carrying out processing in Singapore. However, the limitation of territorial operation of the PDPA to processing that takes place in Singapore may have the same effect. If the PDPA does not apply to the overseas actions of an intermediary, then there are no 'obligations' for which the Singapore-based controller is vicariously liable. This would apply whether or not the intermediary's actions are within the terms of the processing contract: neither controller nor intermediary would be liable. If this approach is correct, the only protection for the data subject can come from controller-intermediary contracts or binding corporate rules (see section 4.4 of this chapter).

Alternatively, but less likely, Singapore may have imposed a form of vicarious liability on Singaporean data controllers for overseas processing by intermediaries, at least where it is within the terms of the processing contract. If this is found to be the case, then while the data intermediary provisions have deficiencies from the perspective of data subjects, particularly in relation to transparency, their starting point of maintaining some liability of the controller is better than a mere requirement of due diligence. These provisions would be capable of producing remedies for data subjects who have been harmed by overseas data processing. This would be the best result for the data subject.

(p.306) 4.4. Data exports limitations deliver less than they promise

Organizations to which the PDPA applies may not transfer personal data outside Singapore except in accordance with regulations (not yet made) 'to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under this Act'.[123] This was a late development, as the draft Bill did not include a specific provision concerning data exports. The Proposed Regulations[124] suggested by the PDPC (but not yet made) do not include any mechanism by which it can be decided that the law of a particular overseas country is 'comparable' to Singapore's law, so as to allow data exports to that country (i.e. no 'white list' mechanism has been proposed). Instead, the PDPC proposes that all personal data exports should be made 'pursuant to a legally binding instrument that contains the appropriate safeguards in the form of contractual clauses or binding corporate rules', binding both sender and receiver. For *inter*-corporate transfers, contracts are expected to be used, and for *intra*-corporate transfers, binding corporate rules are expected to often be used. It is proposed by

the PDPC that the Regulations will specify those obligations which must be included in the legally binding instrument, and will cover purpose, use, and disclosure; accuracy (except for overseas data intermediaries/processors); protection (security); and retention and (knowledge of) policies. Onward transfer restrictions are not mentioned. No other jurisdiction in Asia has a data export provision that is very similar to Singapore's. The absence of a strict doctrine of privity of contract in Singapore (see section 4.4 of this chapter) could assist this approach, but the PDPC has not proposed that export contracts must be expressly made for the benefits of data subjects.

An undesirable aspect of the PDPA's data export provisions is that an organization can apply to the PDPC to be exempted from any such regulations,[125] (when made) and the PDPC can even give them a secret exemption.[126] Whatever the regulations may say about regulating data exports, data subjects can be kept in the dark by the Commission that is supposed to protect them. Perhaps this provision will never be used, but there will be no way of knowing whether it has been used. It appears to be an unnecessary provision which will reduce confidence in Singapore's law.

4.5. Enforcement of the export contract by the data subject

Unusually for a common law jurisdiction,[127] Singapore has reformed the doctrine of privity of contract so as to allow third parties for whose benefit contracts are made to enforce those contracts.[128] The law provides that a third party (the data subject in this case) may only enforce a term of a contract if it expressly provides that he may, or 'the term purports to confer a benefit on him' except 'if, on a proper construction of the contract, it appears that the parties did not intend the term to be enforceable by the third party'.[129] He or she will also need to be 'expressly identified in the contract…as a member of a class or as **(p.307)** answering a particular description'.[130] If these conditions are satisfied, then the data subject will be able (according to Singapore law) to enforce the data processing contract against the overseas recipient of their personal data, including attempting to seek damages or an injunction in case of breach of contract. This is necessary because the PDPA does not have any extraterritorial operation (as explained earlier) and the data subject cannot enforce the PDPA in relation to actions occurring outside Singapore.

The PDPC's Proposed Regulations are therefore plausible in terms of the section's aim to ensure that 'comparable' protections are provided by the overseas recipient, because it is, in theory, possible that a data subject might be able to sue to enforce the export contract. However, in reality the prospects of enforcement by data subjects (the individuals who suffer harm) are very slight indeed. The PDPC's proposals give no indication that the regulations will contain any of the safeguards needed to make them work to benefit data subjects. They do not require that the data export contract must conform with the requirements of the Contracts (Rights of Third Parties) Act necessary for the data subject to have standing to sue. They do not specify that the 'legally binding instrument' must allow the data subject to take enforcement action in the courts of Singapore.

There are likely to be two further areas of deficiency in relation to protection of data subjects against overseas misuse of their personal data: transparency and enforcement. Data subjects have no way of knowing that their personal information is likely to go, or has gone, to any overseas destination, and no way of knowing what 'legally binding instrument' may or may not exist to give them rights. This lack of transparency in data export arrangements is the norm across Asian jurisdictions (see Chapter 17, section 5). Then, assuming that an appropriate 'legally binding instrument' does exist (and the data subject becomes aware of it), the data subject will only be able to enforce his or her rights under that agreement, namely, by taking action under the contract or binding corporate rules before a court in a foreign country. This is a very poor substitute for being able to lodge a complaint before the PDPC in Singapore.

In summary, with the exception that the PDPA includes a restricted form of vicarious liability for overseas processors, the PDPC is proposing (through a regulation) to allow Singaporean organizations to otherwise wash their hands of any responsibility for exports of personal data from Singapore to anywhere in the world, no matter what the result, provided that the Singaporean organization has followed the correct formalities. It is a bad result for Singapore's citizens and for any foreigners whose personal data end up in Singaporean hands.

4.6. Insufficient regard for data subjects in data exports

Singapore is not alone among Asia-Pacific jurisdictions in its low level of concern for protecting its citizens when their personal data is exported. Recent laws in various Asian and other jurisdictions (see Chapter 17, section 5) place few, if any, restrictions on the export of personal data based on the lack of protection in the jurisdiction of the recipient. Some of these laws compensate by including provisions on extraterritoriality or through limited vicarious liability for acts of processors, but these are not an adequate substitute for either consent based on full disclosure or absolute liability for such breaches as may occur.

(p.308) 4.7. Data imports—an 'outsourcing exemption'

Where a Singaporean company contracts to do data processing for an overseas company, the 'data intermediary' provisions will apply. The Singaporean data processor ('data intermediary' in PDPA terms) will be largely exempt from the operation of its own PDPA (with obligations only in relation to data security and deletion). However, Singapore's PDPA will not apply to the overseas data controller, for actions outside Singapore, because of the lack of extraterritorial operation of the PDPA. Nor is it likely that section 4(3) of the PDPA[131] will impose a vicarious liability on a data controller located overseas for breaches of the data protection principles which occur in the course of the authorized processing. The data subject (whether located overseas or in Singapore) will have to rely upon the law of the exporting county, which may or may not impose liability on the exporter (the foreign data controller) to comply with other data protection principles (such as access and correction) and perhaps vicarious liability for any deficiencies in the extraterritorial data processing. If the exporting country's law provides no protection as such, then there is none.

It therefore seems that there is an 'outsourcing exemption': a lower level of data protection provided under Singapore law where personal data is imported into Singapore for outsourced processing. Exemptions with similar effect are found in some other Asian jurisdictions with data protection laws, but not in others (see section 5, Chapter 17). Perhaps this very limited operation of data protection law to outsourcing will assist in making Singapore a more attractive destination for data processing, consistent with the impetus for Singapore's law being economic development, but its effect on data exports from the EU or other countries with data export restrictions is uncertain (see section 5, Chapter 17).

5. Enforcement in Singapore—multi-faceted potential, with sharp teeth

The data protection aspects of the Singapore PDPA will not be in operation until July 2014 so its provisions all remain untested. One of the stronger features of this new data protection regime is that it has multiple and alternative approaches to enforcement. The seriousness with which businesses operating in Singapore should take the enforcement of the Act by the PDPC is possibly indicated by the PDPC's approach to implementing the Do Not Call Registry part of the PDPA,[132] only a month after it came into force:[133]

> Investigations have been taken in response to 1500 valid complaints from the public on 580 organisations since the DNC provisions took effect on 2 Jan 2014 and the PDPC had commenced taking enforcement action. The organisations are from sectors such as private education, property, banking & finance, retail, insurance and telecommunications. Complaints relating to suspected unlicensed money-lending activities have also been referred to the Police.
>
> At present, PDPC is investigating a recalcitrant organisation, with a view to prosecution, as it has continued to send multiple unsolicited telemarketing messages to numbers listed in the DNC Registry despite being notified by the PDPC.
>
> PDPC has offered to compound the offences against at least two other organisations for between $500 and $1,000, while more than a hundred other organisations had been issued notices of warning in lieu of prosecution. Additional offers of composition and notices of warning will be issued over the next few weeks.

(p.309) 5.1. A data protection authority, but not an independent one

The PDPA provides for the appointment of the PDPC by the Minister, with up to 17 members.[134] There is also an eight-person Advisory Committee[135] with which the PDPC may consult—although it is not bound by the Committee's suggestions.[136] As well as its key function to 'administer and enforce' the PDPA, the PDPC has a variety of advisory, educational, and international cooperation functions.[137] It can also issue Guidelines indicating the manner in which it will interpret the Act, and so far it has issued two sets of Guidelines.[138]

The PDPC is explicitly presented as a government authority ('Singapore's main authority in matters relating to personal data protection'[139]) and not as an independent statutory authority. The Minister may revoke any appointment to the PDPC 'without assigning any reason'[140] and may set the term of any appointment.[141] The PDPC is unusual among the 85 data protection authorities (DPAs) which have been so far been created worldwide[142] because it and its Malaysian counterpart are the only two DPAs that have jurisdiction over the private sector but not the public sector. These two are not a 'watchdog on government', unlike other DPAs. While there are strong and obvious reasons why DPAs which have as part of their function the prevention of abuses by a government must be independent of that same government, these reasons do not apply with the same strength in Singapore and Malaysia. Here we are dealing with the regulation of industry by a government agency and, while there are always arguments for and against the use of independent regulators, the position of Singapore's PDPC as a semi-independent regulatory body is nothing unusual. However, if in future the PDPA is extended to cover the public sector, the PDPC's independence will need review, and all the arguments concerning the meaning of 'independence' in relation to a DPA[143] will need to be taken into account.

5.2. The PDPC's powers to enforce the Act

The PDPC may investigate non-compliance with the PDPA 'upon complaint or of its own motion…to determine whether an organisation is not complying with this Act',[144] with powers as set out in the Ninth Schedule. There is no requirement that the PDPC have reasonable grounds for suspicion of non-compliance before commencing an own-motion **(p.310)** investigation. The PDPC may exercise its powers to give directions as a result of an own-motion investigation, not only as a result of a complaint.[145] The power of own-motion investigation is important and has been used extensively by the DPAs in Hong Kong, Macao, and South Korea.

The PDPC may refuse to investigate a complaint, or suspend or discontinue an investigation, 'if it thinks fit'. An inclusive list of possible reasons for exercise of its discretion are provided, including where a party has commenced legal proceedings in respect of any alleged contravention, where the PDPC has referred the matter to another regulatory authority, and where 'a complaint is frivolous or vexatious or is not made in good faith'.[146] Where such refusal to investigate occurs, the complainant has no right to appeal, as there is no decision to appeal against. Such procedures are easily abused by DPAs. Fortunately, the Singapore PDPA does not have a provision specifically allowing investigation to be discontinued whenever the PDPC considers the respondent has adequately dealt with the matter. The Australian law has such a provision, which disadvantages complainants because it is applied even where the complainant disagrees. The equivalent Singapore provision only refers to where 'the parties…have mutually agreed to settle the matter'.[147] These aspects of the PDPC's powers are not unusual.

More unusual are the explicit provisions that the PDPC may, with the consent of both parties, refer a dispute to mediation,[148] or may direct either party to attempt to resolve a dispute in a way it considers appropriate.[149] South Korea's law makes heavy use of mediation, but through a body created specifically for that purpose: the 'Personal Information Dispute Mediation Committee'.

Decisions, directions, and administrative penalties

The PDPC's powers to enforce the PDPA are extensive compared with most DPAs, but do not include the power to award compensation to complainants. The PDPC may review decisions concerning refusal to provide access to personal data (or undue delay in doing so), payment of fees, or correction of data.[150] Where the PDPC considers that an organization 'is not complying' with any of the privacy principles (in Parts III–VI of the PDPA[151]) it may give directions to ensure compliance, which may include any or all of directions: (a) to stop collecting, using or disclosing personal data in contravention of the PDPA; (b) to destroy personal data collected in contravention; (c) to comply with any directions concerning access and correction; or (d) to pay a financial penalty of such amount not exceeding S$1m.[152] Such directions may be enforced by the PDPC registering the direction in a District Court.

The 'million-dollar penalty' possible under section 29 is an impressive dissuasive sanction. It is very high compared with the maximum fines for contravention of an enforcement notice in Hong Kong, which is about S$16,300 (HK$100,000), and the maximum fine in South Korea of about S$112,000 (100m won). In practice, in Hong Kong the highest fine in 2012 was only S$1,600. While such high levels of sanctions are generally desirable from the perspective of increased likelihood of compliance, they will only be desirable in practice if they are used by the PDPC with an appropriate sense of proportion. A million-dollar fine may be no more than a fleabite to some multinational corporations whose business models **(p.311)** are based on privacy invasion, but could bankrupt a small business or individual if used disproportionately in relation to small-scale breaches.

5.3. Offences

A breach of the principles in the PDPA is not an offence per se, and the high level of potential administrative penalties makes that largely unnecessary. A number of other actions[153]—essentially those showing a dishonest intent—may constitute offences, resulting in maximum fines ranging from S$5,000–S$100,000 for organizations or S$5,000–S$10,000 for individuals. However, where there is wrongful access to, or alteration of, personal data (an offence under section 51 of the PDPA[154]), only the section 51 penalties apply (with a maximum fine of $5,000) and the PDPC cannot make orders under section 29. There is also no requirement that the government must commence a prosecution for an offence before section 29 ceases to apply. It is not clear why actions that are also an offence, as well as a breach of a privacy principle, are only liable to a

lesser penalty to a maximum of S$100,000 (or none at all if there is no prosecution), rather than a potential penalty of up to S$1m for merely failing to comply with a principle. One explanation might be that the section 51 offences are aimed primarily at relatively minor offences affecting a single individual, and if multiple occurrences occur then there will be multiple offences.

5.4. Avenues of reconsideration and appeal

The appeal structure under Singapore's PDPA means that resolution of a dispute, and the legal issues accompanying it, may pass through many hands, and this is one of its strong points. First, aggrieved organizations or individuals have 28 days to apply to the PDPC to reconsider a decision it has made or direction it has given.[155]

Individuals or organizations dissatisfied with PDPC decisions may also appeal to the Data Protection Appeal Panel[156] on any grounds (law, facts, or remedies). Their appeal will be heard by an appeal committee of three or more members drawn from the panel.[157] Appeal committees will have all the powers and duties of the PDPC necessary for their work, plus those of a District Court (including enforcing attendance of witnesses, **(p.312)** examination on oath, and compelling production of documents).[158] They may confirm, vary, or set aside the PDPC direction or decision which is the subject of the appeal; remit the matter to the PDPC; impose, revoke or vary the amount of a financial penalty; or give directions the PDPC could have given.[159] They can also set aside findings of fact while upholding a PDPC decision.[160]

The appeal committees will therefore share many of the characteristics of the administrative tribunals that hear data protection appeals in other jurisdictions. In Hong Kong, appeals are to the Administrative Appeals Board, a general administrative law tribunal, not one specifically for data protection matters. In both South Korea and Macao, appeals to the courts (not to another tribunal) may be made against DPA decisions.

In Singapore there is also a limited right of appeal from an appeal committee to the courts, initially to the High Court, on a point of law, or from a direction as to the amount of financial penalty,[161] but not on questions of fact. The PDPC, the complainant, and the respondent may each appeal.[162] Further rights of appeal to the Court of Appeal are the same as from the High Court in its original civil jurisdiction.[163] The limited grounds of appeal are a minor deficiency in Singapore's PDPA.

Transparency—advantages and dangers

How much of this multi-layered dispute resolution system will be transparent to other potential complainants, or businesses, or their advisers? It is clearly desirable that directions made under the PDPA, and the reasoning supporting them, should be available to the public, although not necessarily in identified form. In some cases it may be in the public interest that respondents be identified. It will less frequently be in the public interest that complainants be identified—it may worsen the privacy invasion—but sometimes they may want public identification so as to vindicate their reputations.

The PDPA is not clear on these points. There is nothing in section 29 of the PDPA[164] indicating that the PDPC can publish decisions it makes (in redacted form where necessary), nor any clear obligation in section 6 to do so. Secrecy obligations cover 'all matters relating to the identity of persons furnishing information to the Commission', except where disclosure is necessary for the PDPC to perform its functions.[165] Appeal committees must notify the PDPC, as well as the parties, of their decisions and reasons,[166] but once again nothing is said about publication. Other Asian jurisdictions make considerable use of 'name and shame' sanctions (see Chapter 18, section 3.3).

On the other hand, if it is necessary for directions of either the PDPC or an appeal committee to be enforced, then the direction must be registered in a District Court, and may therefore become public. Similar issues will arise when appeals, or civil liability claims, are heard by courts. State courts in Singapore are normally open and public, but they can hear matters *in camera* if 'satisfied that it is expedient in the interests of justice, public security or propriety, or for other sufficient reason to do so';[167] similar provisions apply in relation to the Supreme Court.[168] Other jurisdictions which rely on privacy appeals to administrative tribunals and courts (such as New Zealand, Hong Kong, New South Wales, **(p.313)** and Victoria) have dealt with these problems by careful balances between the benefits of open justice and privacy protection of complainants.

5.5. Compensation and other civil liability

Complainants who have suffered 'loss or damage directly as a result of a contravention'[169] of the principles in Parts IV–VI (but not the general obligations of transparency and accountability under Part III) have a right of private action before a court to obtain injunctions or damages.[170] The court may grant such a plaintiff any or all of: '(*a*) relief by way of injunction or declaration; (*b*) damages; or (*c*) such other relief as the court thinks fit'.[171] A complainant cannot initiate such actions if the PDPC has made a decision in relation to the same contravention until any appeal rights have been exhausted,[172] which seems to imply that the complainant need not proceed *ab initio* before the court and instead may have the court take into account the finding of a contravention by the PDPC. However, it is not explicit that this is so, or whether it is necessary for the complainant to prove *ab initio* that there is a contravention. If it is the latter, this is likely to significantly reduce, or perhaps even eliminate, actions under section 32.

There is no provision for the PDPC to intervene in civil actions for damages to provide assistance to complainants (compare Hong Kong—see Chapter 18, section 3.5). Given the costs of initiating litigation in Singapore, and the risks of costs being awarded against the plaintiff, there is therefore no low-cost or low-risk means by which Singaporean data subjects can seek modest amounts of compensation for data protection breaches. At present, South Korea is the only Asian jurisdiction where such compensation is a routine part of data protection enforcement.

5.6. Personal and vicarious liabilities—employees and company officers

Singapore's PDPA raises important issues for businesses trading in Singapore concerning who is liable for breaches and offences, in relation to both liability of employers for acts of their employees and personal liability of corporate officers for offences.

Any act done or conduct engaged in by an employee in the course of his or her employment will also be treated as done or engaged in by the employer, whether or not it was with the employer's knowledge or approval. An employee 'acting in the course of his employment' has no liability for breach of the principles in the PDPA.[173] In relation to offences under the Act, it is a defence for the employer to prove that it took such steps as were practicable to prevent the employee from doing the act or engaging in the misconduct,[174] but this does not affect the employer's civil liability.

Singapore's PDPA also imposes personal liability on company officers for offences that involve the consent, connivance, or neglect of a company officer,[175] an unusual provision in **(p.314)** a data protection law. Similar provisions apply to partnerships[176] to unincorporated associations[177] and to limited liability partnerships.[178] 'Officer' is given a broad definition[179] and members of companies involved in management may also in

some cases be liable.[180] Singapore is not the only Asian jurisdiction where such liability is part of a data protection law. Under South Korea's legislation, company officials may face up to five years in prison for failure to protect customer data, and prosecutions have occurred.

5.7. Other enforcement mechanisms

Singapore's Act is based largely on reactive enforcement, through responses to complaints. However, this is not the only enforcement mechanism, as the PDPC may initiate investigations on its own and has the ability to use its enforcement powers following such own-motion investigations. Otherwise, the PDPA does not provide for any systemic measures to prevent or deter breaches of the privacy principles. In other legislation in Asia, there is limited provision of such systemic measures (see Chapter 18, section 4). Given that such systemic measures have had relatively little impact elsewhere in Asia, their absence from Singapore's legislation is not very unusual.

5.8. Conclusions—barriers to relief but serious risks in non-compliance

The sanctions the PDPC can impose—without going to a court—are very strong, and do not depend upon continuation of breaches. The appeal structure puts this enforcement in many hands, not just those of the public servants at the PDPC. The vicarious liability risks for companies may also be severe, which means that companies doing business in Singapore must pay attention to privacy. If they fail to pay attention to Singapore's standards, the penalties or the compensation resulting from non-compliance may be high.

In theory, individual complainants have a valuable right to direct access to the courts to pursue compensation for breaches, and to other remedial orders through the appeals structures. However, the compensation provisions may, in practice, only produce compensation for the type of complainant who would also be likely to take action under defamation laws, and could afford to do so, because of the risks of publicity exacerbating privacy harms, or bankruptcy through adverse costs orders.

6. Conclusions—balancing the rights of the data subject against business interests in Singapore

The context into which Singapore's PDPA arrives is on the one hand unpromising, because of its very limited constitutional and common law protections for privacy. On the other hand, it is extremely promising, because of the high reputation for lack of corruption, and efficiency, of both the bureaucracy and judiciary of Singapore, and the quality of their judgments.

The PDPA has an exceptionally limited scope, perhaps the narrowest of any Asian law (see section 2 of this chapter). The data protection principles in the PDPA are summarized in section 3.3 of this chapter as a minimal version of a 'normal' data privacy law, with a few valuable additions, and very extensive and uncertain exceptions. The result is one of the **(p.315)** weaker sets of principles in Asian data protection laws (for comparisons, see Chapter 17), but it is clearly the intention of the legislation to minimize its impact on businesses, particularly in relation to costs. One commentator considers that 'it would be worthwhile for local businesses to consider exceeding the minimum data protection requirements' because 'the Act may not come up to par with international data privacy standards'.[181]

Singapore's PDPA does appear to have a serious and multi-faceted 'enforcement pyramid'. Overall comparisons between jurisdictions are complex (see Chapter 18), but in Asia, only Macao and South Korea can compare with Singapore in the variety and strength of enforcement mechanisms that are provided. However, it will take some years after Singapore's PDPA is fully in force before meaningful comparisons of the reality of enforcement are possible.

From the perspective of a Singaporean data subject (consumer or citizen), the PDPA is much better than no data protection legislation at all—more than half the countries in Asia and more than half the countries in the world still have none[182]—although the excessively limited scope and generally minimalist content of the PDPA is regrettable from a data subject perspective. However, a future government in Singapore has an existing law to amend and strengthen. Also, now that a law exists, Singaporean citizens may push for it to be strengthened. Neither will have to start from scratch.

From a business perspective, deficiencies from a data subject perspective could be considered as virtues, in that they deliver what has been described as a 'pro-business approach'[183] where the likelihood of non-compliance is much reduced by the limited scope of and major exceptions to, the PDPA which make breaches easy to avoid or difficult to detect. This must be balanced against the fact that the PDPC has diverse, flexible, and potentially punitive powers (including the 'million-dollar penalty'). A business that blatantly fails to comply with Singapore's data protection rules might find itself in considerable difficulty. The early months of the Do Not Call Register show the PDPC taking a very activist approach to enforcement. Despite these potentially strong but still theoretical enforcement methods, it remains questionable whether an Act with otherwise relatively weak protections for data subjects will be to the long-term advantage of Singaporean businesses. It cannot be assumed that a 'pro-business' approach will succeed in creating consumer confidence in Singaporean e-commerce, because it may not satisfy international requirements for comparably protective laws in the years ahead.

Notes:

([1]) Personal Data Protection Act 2012 (Act 26 of 2012) (Singapore).

([2]) Following enactment, Singapore's Ministry of Communications and Information brought the PDPA into effect on 2 January 2013, but gave businesses 18 months to comply before the data protection aspects of the Act become enforceable in July 2014, but only 12 months for the Do Not Call provisions.

([3]) PDPC, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (PDPC, 24 September 2013) ('*Key Concepts Guidelines*').

([4]) PDPC, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (PDPC, 24 September 2013) ('*Selected Topics Guidelines*')

([5]) For a brief general history, see Peter Church, ch. 9 'Singapore' in *A Short History of South-East Asia* (5th Edn., Wiley, 2009); for post-war history, see Francis Pike, *Empires at War: A Short History of Modern Asia Since World War II* (I B Tauris, 2010), chs. 18 and 57, and pp. 715–16.

([6]) It is argued that this is primarily because '[s]ince the late 1960s, elites in the PAP and bureaucracy have maintained their deep cohesion', and that to a large extent this has functioned as a meritocracy (with internal competition for positions) rather than by less desirable methods. See William Case, ch. 3 'Singapore: A Stable Semi-democracy' in *Politics in Southeast Asia: Democracy or Less* (Curzon, 2002), pp. 85–9.

([7]) These limitations include tightly controlled information flows, limits on media ownership, and because, although the formalities of electoral

equality are carefully observed, opposition parties are 'systematically impaired before election day arrives' through discouragement against joining opposition parties, strategic use of lawsuits, carefully organized constituencies, and even threats to deny public housing maintenance to constituencies that failed to vote PAP. See Case, *Politics in Southeast Asia*, pp. 90–5.

([8]) The complex legal history is explained in Kevin Y.L. Tan, ch. 10 'Singapore: A Statist Legal Laboratory' in E. Ann Black and Gary F. Bell (Eds.), *Law and Legal Institutions of Asia* (Cambridge, 2010). See also Walter Woon, ch. 8 'Singapore' in Poh-ling Tan (Ed.), *Asian Legal Systems* (Butterworths, 1997).

([9]) It is based on its State Constitution of 1963, plus provisions added through the Republic of Singapore Independence Act. It was last consolidated as a reprint in 2010: see <http://statutes.agc.gov.sg>.

([10]) Tan, ch. 10 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, p. 352.

([11]) *Application of English Law Act 1993* (Singapore): see Tan, ch. 10 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, p. 348.

([12]) Tan, ch. 10 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, p. 338.

([13]) Tan, ch. 10 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, p. 354.

([14]) Tan, ch. 10 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, p. 355.

([15]) EPIC, 'Republic of Singapore' in *Privacy and Human Rights* (EPIC, 2006). <http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Republic-24.html>.

([16]) Constitution of the Republic of Singapore (1985), pt. IV.

([17]) It is, like all other UN member states, subject to the Universal Periodic Review of the Human Rights Council of the UN, see <http://www.ohchr.org/en/hrbodies/upr/pages/uprmain.aspx>.

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

([19]) *Malcomson Bertram & Anr v Naresh Mehta* [2001] SGHC 308; [2001] 4 SLR 454 at 470H to 474A <http://lwb.lawnet.com.sg/legal/lgl/rss/landmark/%5B2001%5D_SGHC_308.html>.

([20]) *AXA Insurance Singapore Pte Ltd v Chandran s/o Natesan* [2013] SGHC 158.

([21]) Ministry of Law 'Factsheet on the Protection from Harassment Act 2014' (Ministry of Law, 1 March 2014) <www.mlaw.gov.sg/content/dam/minlaw/corp/News/Factsheet%20on%20proposed%20Protection%20from%20Harassment%20Act%202014.pdf>.

([22]) Simon Chesterman, ch. 1 'From Privacy to Data Protection' in Simon Chesterman (Ed.), *Data Protection Law in Singapore: Privacy and Sovereignty in an Interconnected World* (Academy Publishing, 2014), pp. 14–22.

([23]) See also Graham Greenleaf, 'Singapore Takes the Softest Privacy Options' (2002) 8 *Privacy Law & Policy Reporter*, pp. 169–73.

([24]) Chesterman, ch. 1 in Chesterman (Ed.), *Data Protection Law in Singapore*, p. 16, citing Chris Connolly 'Privacy White Lists—Don't be Fooled' (Galexia, 2009) <http://www.galexia.com/public/research/assets/privacy_white_lists_2009/>.

([25]) Graham Greenleaf, '"New" Data Privacy Laws: Malaysia, the Philippines and Singapore' (2012) 116 *Privacy Laws & Business International Report*, p. 22.

([26]) Chesterman, ch. 1 in Chesterman (Ed.), *Data Protection Law in Singapore*, pp. 19 and 22.

([27]) PDPA (Singapore), s. 2.

([28]) The definition of 'organization' applies the PDPA (Singapore) to individuals and all types of associations of persons, whether or not formed under the law of Singapore, or residing or with an office in Singapore: PDPA (Singapore), s. 2.

([29]) PDPA (Singapore), s. 4(4).

([30]) PDPA (Singapore), s. 4(4)(b).

([31]) See Chesterman, ch. 1 in Chesterman (Ed.), *Data Protection Law in Singapore*, p. 24.

([32]) PDPA (Singapore).

([33]) PDPA (Singapore), s. 4(5).

([34]) Spam Control Act (Singapore).

([35]) PDPA (Singapore), Second Sched., para. 1(*c*); Third Sched., para. 1(*c*); Fourth Sched., para. 1(*d*).

([36]) PDPA (Singapore), s. 2.

([37]) PDPC, *Key Concepts Guidelines*, pp. 49–53.

([38]) Graham Greenleaf, 'Scheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories', *Journal of Law & Information Science* (forthcoming 2014).

([39]) PDPA (Singapore), s. 4(1)(*c*).

([40]) PDPA (Singapore), s. 2(2).

([41]) PDPA (Singapore), s. 3.

([42]) Dr Yaacob Ibrahim, Minister for Information, Communications and the Arts, 'Second Reading Speech on the Personal Data Protection Bill 2012', 15 October 2012, para. 10.

([43]) Chesterman, ch. 1 in Chesterman (Ed.), *Data Protection Law in Singapore*, p. xiii.

([44]) PDPA (Singapore), s. 4(1)(*a*).

([45]) See definition of 'evaluative purpose' in PDPA (Singapore), s. 2.

([46]) See Yee Fen Lim, ch. 8 'Data Protection in the Employment Setting' in Chesterman (Ed.), *Data Protection Law in Singapore*.

([47]) PDPA (Singapore), s. 4(1)(d).

([48]) PDPA (Singapore), s. 62.

([49]) PDPA (Singapore), s. 4(6)(b).

([50]) PDPA (Singapore), s. 4(6)(a).

([51]) 'In the event of any conflict, the sectoral regulations will prevail': Kah Leng Ter, 'Singapore's Personal Data Protection Legislation: Business Perspectives' (2013) 29 CLSR 264, p. 265.

([52]) Such sectoral laws are not covered in this book. Countries vary in whether the sectoral laws are in addition to, or in substitution for, the comprehensive laws.

([53]) National Internet Advisory Committee Legal Subcommittee, *Report on a Model Data Protection Code for the Private Sector* (February 2002) Annex. 2.

([54]) Ter, 'Singapore's Personal Data Protection Legislation', p. 265.

([55]) PDPA (Singapore), Second Sched., para 2.

([56]) There are no specific exemptions for news organizations in relation to use and disclosure of personal data without consent, but an exemption may not be necessary if the purpose of collection is 'news activities', because there is no change of purpose of use or disclosure. Any breaches because of lack of consent will already have taken place at the time of collection. This differs from the draft Bill: see Ministry of Information, Communications and the Arts, *Public Consultation Issued by Ministry of Information, Communications and the Arts: Proposed Personal Data Protection Bill* (19 March 2012).

([57]) See Chesterman, ch. 1 'From Privacy to Data Protection' in Chesterman (Ed.), *Data Protection Law in Singapore*.

([58]) 'Fact Sheet—Online News Sites to Be Placed on a More Consistent Licensing Framework as Traditional News Platforms', *Singapore Media Development Authority* (2013) <http://www.mda.gov.sg/AboutMDA/NewsReleasesSpeechesAndAnnouncements/Pages/NewsDetail.aspx?news=4>.

([59]) The 2013 Reporters Without Borders and Freedom House rankings are summarized by Shah Salimat, 'Singapore Falls to Record-low Place in Press Freedom Ranking', *Yahoo! News* (4 May 2013) <http://sg.news.yahoo.com/singapore-falls-to-record-low-place-in-press-freedom-ranking-035131531.html>.

([60]) Tsun Hang Tey, *Legal Consensus* (Centre for Comparative and Public Law, University of Hong Kong, 2011) pp. 30–4.

([61]) PDPA (Singapore), s. 17(1) and Second Sched., cl. 1(g).

([62]) See PDPC, *Key Concepts Guidelines*, pp. 31–2.

([63]) Organisation for Economic Co-operation and Development Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (OECD Doc. C(80)58/FINAL) (23 September 1980).

([64]) PDPA (Singapore), s. 18(a).

([65]) PDPA (Singapore), s. 20.

([66]) PDPA (Singapore), s. 13(a).

([67]) PDPA (Singapore), s. 15.

([68]) PDPA (Singapore), s. 20(3)(*a*).

([69]) Although the PDPC states that for deemed consent to apply 'the onus would be on the organisation involved to ensure that the individual was aware of the purpose for which for which his personal data would be collected, used or disclosed', it does not specifically say that such awareness must come through s. 20 notice. The examples given do not involve such notice. See PDPC, *Key Concepts Guidelines*, pp. 39–41.

([70]) An exception is where s. 20(4) requires that notification of purpose and a relevant contact be given to an individual when an organization is

collecting, using or disclosing personal data for the purpose of managing or terminating an employment relationship.

([71]) PDPA (Singapore), ss. 17 and 20(3)(*b*).

([72]) Considerably simplified and, often with qualifications omitted, the exemptions may be summarized as: where necessary in the interests of the individual, whose consent cannot be obtained in a timely manner and where consent could be expected; emergencies threatening the life, health, or safety of the data subject or another person (in relation to use and disclosure); disclosures for the purpose of contacting the next of kin or friend of any injured, ill, or deceased person; 'publicly available' personal data (as defined in s. 2 of the PDPA) where 'necessary in the national interest'; where necessary for 'any investigation or proceedings' (and consent to collection would be likely to compromise this); where necessary for evaluative purposes; solely for artistic or literary purposes (collection only); by a news organization solely for news activity; for debt recovery; in relation to provision of legal services; for credit reporting; disclosures by educational institutions about students to government bodies; disclosures by healthcare authorities to government agencies for policy reviews; disclosures to law enforcement agencies with written self-certification by a senior officer that this is necessary for law enforcement; for the administration of trusts; for provision of domestic and personal services; documents produced for employment, business or professional purposes; for the purposes of managing or terminating employment; in relation to business asset transactions; data disclosed by public agencies; research purposes, including historical research (in relation to use and disclosure); and disclosures for archival or historical purposes.

([73]) PDPA (Singapore), s. 13(b).

([74]) PDPC, *Key Concepts Guidelines*, p. 41.

([75]) PDPC, *Key Concepts Guidelines*, p. 35.

([76]) Directive 95/46/EC of the European Parliament and of the Council (24 October 1995) (protection of individuals with regard to the processing of personal data and on the free movement of such data) [1995] O.J. L. 281/31 ('European Data Protection Directive').

([77]) PDPA (Singapore), pt. IX.

([78]) PDPA (Singapore), s. 21.

([79]) PDPA (Singapore), s. 21(3).

([80]) PDPA (Singapore), s. 21(5).

([81]) PDPA (Singapore), s. 22.

([82]) PDPA (Singapore), s. 22(2)(*b*).

([83]) PDPA (Singapore), s. 22(5).

([84]) PDPA (Singapore), s. 22(6).

([85]) PDPA (Singapore), s. 23.

([86]) PDPC, *Key Concepts Guidelines*, pp. 64–7.

([87]) PDPA (Singapore), s. 24.

([88]) PDPC, *Key Concepts Guidelines*, pp. 68–70.

([89]) PDPC, *Key Concepts Guidelines*, pp. 76–7.

([90]) PDPA (Singapore), s. 12.

([91]) OECD Guidelines: '12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.'

([92]) PDPA (Singapore), s. 11.

([93]) PDPA (Singapore), s. 25.

([94]) Limitations Act (Singapore); see PDPC, *Key Concepts Guidelines*, pp. 71–2.

([95]) PDPC, *Selected Topics Guidelines*, pp. 10–22.

([96]) PDPC, *Selected Topics Guidelines*, p. 11.

([97]) Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 *UCLA Law Review*, p. 1701 <http://ssrn.com/abstract=1450006>.

([98]) PDPC, *Selected Topics Guidelines*, p. 13.

([99]) PDPC, *Selected Topics Guidelines*, p. 13.

([100]) PDPC, *Selected Topics Guidelines*, pp. 36–7.

([101]) Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Regarding

Supervisory Authorities and Transborder Data Flows (8 November 2001) <http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm>.

([102]) Graham Greenleaf, 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108' (2012) 2(2) *International Data Privacy Law* 68, at pp. 72–4.

([103]) PDPA (Singapore), s. 14(2)(*a*).

([104]) Extra protection for sensitive data was foreshadowed in a consultation paper, but did not eventuate. See Ministry of Information, Communications and the Arts, *Public Consultation Issued by Ministry of Information, Communications and the Arts: Proposed Personal Data Protection Bill* (19 March 2012).

([105]) A consultation paper proposed an 'opt-in' by industry sectors for its more onerous principles, and an 'opt-out' for industry sectors (with permission from the Personal Data Protection Commission) from some of the basic principles. See Ministry of Information, Communications and the Arts, *Public Consultation Issued by Ministry of Information, Communications and the Arts: Proposed Personal Data Protection Bill* (19 March 2012).

([106]) There are five issues where a local data controller (in Singapore) exports personal data: (i) Does the law of the controller's jurisdiction assert extra-territorial operation? (ii) Under what conditions are transfers (data exports) to a foreign jurisdiction allowed? (iii) Are there special rules for controller-to-processor transfers? (iv) Can the data subject enforce a contract against the recipient of exported data? (v) Is the controller liable for breaches by a foreign processor? (vicarious liability).

([107]) PDPA (Singapore), s. 24.

([108]) PDPA (Singapore), ss. 25 and 4(2).

([109]) PDPA (Singapore), s. 2(1). See also Daniel Seng, ch. 4 'Data Intermediaries and Data Breaches' in Chesterman (Ed.), *Data Protection Law in Singapore*.

([110]) PDPA (Singapore), s. 4(3).

([111]) PDPA (Singapore), s. 4(3).

([112]) For a detailed account, see Seng, ch. 4 in Chesterman (Ed.), *Data Protection Law in Singapore*.

([113]) The PDPA does not alter the law of agency as such, and in situations such as where a processor utilizes personal data in ways going beyond their role as a data intermediary, the law of agency may be very relevant. It may also be complicated by the subordinate role of the PDPA to other legal obligations, if inconsistent (see section 2.4 of this chapter).

([114]) PDPC, *Key Concepts Guidelines*, p. 27.

([115]) PDPA (Singapore).

([116]) PDPA (Singapore), s. 20.

([117]) PDPC, *Key Concepts Guidelines*, p. 25.

([118]) PDPC, *Key Concepts Guidelines*, p. 24.

([119]) PDPA (Singapore), s. 2.

([120]) For a similar approach, see Dan Svantesson, *Extraterritoriality in Data Privacy Law* (Ex Tuto Publishing, 2013), pp. 116–17.

([121]) See Svantesson, *Extraterritoriality in Data Privacy Law*, p. 85 for such an 'activity-based' approach to extraterritorial jurisdiction.

([122]) PDPA (Singapore), s. 4(3).

([123]) PDPA (Singapore), s. 26(1).

([124]) Personal Data Protection Commission, *Proposed Regulations on Personal Data Protection in Singapore* (5 February 2013), pt. III.

([125]) PDPA (Singapore), s. 26(2).

([126]) PDPA (Singapore), s. 26(3)(*b*).

([127]) Of Asian jurisdictions with data privacy laws, India still does not have a general exemption to doctrines of privity of contract for third party benefit contracts, and Hong Kong is currently considering law reform proposals to introduce recognition of a third party benefit exception.

([128]) Contracts (Rights of Third Parties) Act 2001 (Singapore). This was preceded by the Law Reform and Revision Division, Attorney-General's Chambers, Singapore, *Report on the Proposed Contracts (Rights of Third Parties) Bill 2001* (LRRD No. 2,/2001, 11 October 2001).

([129]) Contracts (Rights of Third Parties) Act (Singapore), ss. 2(1)(*b*) and 2(2).

([130]) Contracts (Rights of Third Parties) Act (Singapore), s. 2(3).

([131]) PDPA (Singapore).

([132]) PDPA (Singapore), Part IX. The Do Not Call Registry is not covered in this chapter.

([133]) PDPC Press Release: 'PDPC takes action against organizations for breaching Do Not Call Registry Requirements under the Act' (PDPC, 14

February 2014).

([134]) PDPA (Singapore), s. 5. The PDPC is chaired by Mr Leong Keng Thai, Deputy Chief Executive and Director-General (Telecoms and Post), Infocomm Development Authority of Singapore ('IDA'), and is comprised of five other senior officers of the IDA in addition to himself.

([135]) Chaired by Ms Liew Woon Yin, a consultant and former director of Intellectual Property for the Singapore government. Other members are from business, academia, and the consumers' association.

([136]) PDPA (Singapore), s. 7.

([137]) The PDPC will represent Singapore internationally in relation to data protection matters, and may co-operate with other organizations (including foreign and inter-governmental organizations) in data protection matters: PDPA (Singapore), s. 6. Such co-operation may extend to the sharing of information, but in the case of foreign data protection bodies, there are provisions requiring and authorizing appropriate confidentiality agreements: PDPA (Singapore), s. 10. It also has power to issue advisory guidelines: PDPA (Singapore), s. 49. The PDPC may delegate the exercise of its powers and functions to other public officers: PDPA (Singapore), s. 8, and the Minister may also appoint an administration body to manage the PDPC's budget and give it administrative support: PDPA (Singapore), s. 9.

([138]) PDPA (Singapore), s. 49. See PDPC, *Selected Topics Guidelines*; PDPC, *Key Concepts Guidelines*.

([139]) 'What We Do' on the PDPC website at <http://www.pdpc.gov.sg/about-us/what-we-do>.

([140]) PDPA (Singapore), First Sched., para. 3.

([141]) PDPA (Singapore), First Sched., para. 4.

([142]) Graham Greenleaf, 'Scheherazade and the 101 Data Privacy Laws'.

([143]) Graham Greenleaf, 'Independence and Structure of Data Protection Authorities: International Standards' (2012) 28(1) CLSR 3.

([144]) PDPA (Singapore), s. 50.

([145]) PDPA (Singapore), s. 29.

([146]) PDPA (Singapore), s. 50(3).

([147]) PDPA (Singapore), s. 50(3)(*b*).

([148]) PDPA (Singapore), s. 27(1).

([149]) PDPA (Singapore), s. 27(2).

([150]) PDPA (Singapore), s. 28.

([151]) PDPA (Singapore).

([152]) PDPA (Singapore), s. 29.

([153]) PDPA (Singapore), s. 51. The fines can be summarized as: (a) attempting to access or change another person's personal data without their authority (S$5,000 fine); (b) doing various acts in order to evade a request from the PDPC, in relation to either personal data or information about its collection, use or disclosure (S$50,000/S$5,000 fine); (c) obstructing or impeding the PDPC or its officers (S$100,000/S$10,000 fine); and (d) knowingly or recklessly making a false statement to, or knowingly misleading or attempting to mislead the PDPC (S$100,000/S$10,000 fine).

([154]) PDPA (Singapore).

([155]) PDPA (Singapore), s. 31. Unless the Personal Data Protection Commission decides otherwise, such a request will not cause any direction or decision to be suspended, except an order for payment of a penalty: PDPA (Singapore), s. 31. Such a request results in any appeal to the Appeal Panel to be deemed to be withdrawn: PDPA (Singapore), s. 34.

([156]) PDPA (Singapore), s. 34. The minister appoints the appeal panel and its chairman: (PDPA (Singapore), s. 33), and may appoint up to 30 members to the panel, for such period as he or she determines, and revoke appointments without giving reasons (para. 1 of the Seventh Schedule to the PDPA). Members are to be appointed 'on the basis of their ability and experience in industry, commerce or administration or their professional qualifications or their suitability otherwise for appointment', so it is quite possible that there may be a range of appointees from outside government.

([157]) In relation to each appeal, the chairman of the appeal panel is to nominate three or more members of the appeal panel to constitute a Data Protection Appeal Committee (PDPA (Singapore), s. 33(4)). Decisions are by majority of those present, or in the event of a tie, by the casting vote of the chair (para. 3(2) of the Seventh Schedule to the PDPA).

([158]) PDPA (Singapore), Seventh Sched., para 4.

([159]) PDPA (Singapore), s. 34(4).

([160]) PDPA (Singapore), s. 34(6).

([161]) PDPA (Singapore), s. 35.

([162]) PDPA (Singapore), s. 35(2).

([163]) PDPA (Singapore), s. 35(4).

([164]) PDPA (Singapore).

([165]) PDPA (Singapore), s. 59.

([166]) PDPA (Singapore), Seventh Sched., para. 4(8).

([167]) Subordinate Courts Act (Singapore) (Cap 321, 2007 Rev Ed), s. 7(2).

([168]) Supreme Court of Judicature Act (Singapore) (Cap 322, 2007 Rev Ed), s. 8(2).

([169]) A breach of a data protection principle is therefore not actionable per se; loss or damage must result. This is a rare instance of the Asia-Pacific Economic Cooperation 'Preventing Harm' privacy principle being included in legislation. No maximum amount of damages is specified and there is no explicit provision concerning non-pecuniary loss. Such an action for damages was not mentioned in the previous consultation paper. The amount of damages claimed will determine which court has jurisdiction, and rights of appeal will follow from that.

([170]) PDPA (Singapore), s. 32(1).

([171]) PDPA (Singapore), s. 32(3).

([172]) PDPA (Singapore), s. 32(2).

([173]) PDPA (Singapore), s. 4(1)(*b*).

([174]) PDPA (Singapore), s. 53.

([175]) PDPA (Singapore), s. 52(1): 'Where an offence under this Act committed by a body corporate is proved—(*a*) to have been committed with the consent or connivance of an officer; or (*b*) to be attributable to any neglect on his part, the officer as well as the body corporate shall be guilty of the offence and shall be liable to be proceeded against and punished accordingly.'

([176]) PDPA (Singapore), s. 52(3).

([177]) PDPA (Singapore), s. 52(4).

([178]) PDPA (Singapore), s. 52(5).

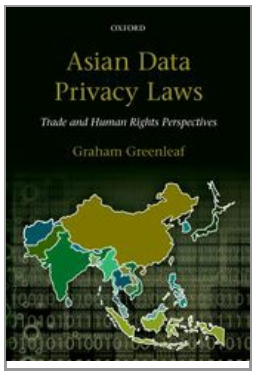
([179]) PDPA (Singapore), s. 52(5).

([180]) PDPA (Singapore), s. 53(2).

([181]) Ter, 'Singapore's Personal Data Protection Legislation', p. 272.

([182]) Greenleaf, 'Scheherazade and the 101 Data Privacy Laws'.

([183]) Ter, 'Singapore's Personal Data Protection Legislation', p. 272.



Asian Data Privacy Laws: Trade & Human Rights Perspectives
Graham Greenleaf

Print publication date: 2014
Print ISBN-13: 9780199679669
Published to Oxford Scholarship Online: December 2014
DOI: 10.1093/acprof:oso/9780199679669.001.0001

Malaysia—ASEAN's First Data Privacy Law in Force

Graham Greenleaf

DOI:10.1093/acprof:oso/9780199679669.003.0011

[–] Abstract and Keywords

Malaysia's Personal Data Protection Act of 2010 was brought into force in November 2013, when a Personal Data Protection Commissioner was appointed. Data users then had three months to comply with the Act and its Regulations, making it the first data privacy Act in the ASEAN (South-East Asia) region to be fully in force. This chapter evaluates the Act in the absence of any enforcement as yet. The Act has very limited scope, and a defective and limited method of enforcement. The main 'democratic deficit' in the law is the omission of the public sector. Unless there are vigorous prosecutions of offences, complainants will be left powerless because they are unable to take civil action. However, the principles contained in the Act are generally reasonable and often include stronger 'European' elements. Despite its deficiencies, this data privacy legislation will be a significant step forward for Malaysians.

Keywords: data protection, privacy, Asia, Malaysia, ASEAN, PDPC, data protection authority

(p.318)

1. The unpromising contexts of Malaysian privacy law

Periodically, since 1998, Malaysian ministers monotonously announced their intentions to introduce comprehensive data protection legislation. In 2010, the government finally did introduce a Bill,[1] and quickly enacted the Personal Data Protection Act 2010 (PDPA), but there the story stalled. A new Personal Data Protection Department under the Information Communication and Culture Ministry was created to oversee the implementation of the Act in 2011. It was not until 15 November 2013 that the Act was brought into force and Abu Hassan Ismail (Director-General of the Department) was appointed as Personal Data Protection Commissioner as well. A number of Regulations came into force on the same day.[2] Data users then had three months, until 15 February 2014, to comply with Act and Regulations, making it the first data privacy Act in the Association of Southeast Asian Nations (ASEAN) region to be fully in force. Nothing further of significance has happened since. Before examining the Act, its context will be considered.

1.1. Political history of Malaysia

The formation of Malaysia was a complex historical evolution.[3] From about 1400, the Sultanate of Melaka (Malacca) was a great trading and cultural centre, dominating much of the Malay peninsula, and adopting Islam. In 1511 the Portuguese conquered Melaka but not the rest of the peninsula, such as the kingdoms of Brunei or Johor. In 1641 the Dutch, in alliance with Johor, ousted the Portuguese. From the cession of the island of Penang in 1786 to the (British) East India company, the British gradually expanded their dominance of the Malay peninsula throughout the nineteenth century, until in 1896 four 'protectorates' that had been established in individual Malay states became the Federated Malay States (FMS) with a federal capital at Kualu Lumpur. Five other 'unfederated' Malay states continued as protectorates, and Sabah and Sarawak in Borneo remained independent. During the next half-century of colonialism, the influx of Indian plantation labourers, and Chinese immigrants in the commercial sector, created the future ethnic basis of Malaysia. Japanese military occupation from 1941–45 was followed by a resumption of British colonial rule, with the intention that a federation of all the Malay states plus Penang and Melaka would be formed. As a result of the suppression of the communist rebellion (the 'Emergency') a very centralized federation emerged. Malaysia was formed in 1963. It originally included Singapore, but in 1965 it was agreed that Singapore should separate. Violence during the 1969 elections resulted in a state of

emergency being declared and a military/police government for two years until parliamentary rule was re-established in 1971.

Now an independent nation, Malaysia continues to have a complex history.[4] A coalition led by the United Malays National Organisation (UMNO), has ruled Malaysia ever since independence: Malaysia has never had a change of government. Since 1971 it has retained **(p.319)** the formal appearance of a democracy, but its elections have been far from 'free and fair',[5] although this was improved in the most recent election in 2013. Prime Minister Mahathir ran a highly centralized authoritarian regime from 1981, and one which was increasingly oriented towards moderate Islam. His government misused the legal system to harass and jail his political opponents, particularly his former deputy, Anwar Ibrahim. The government of the Prime Minister since 2008, Najib Razak, continues the same repressive tactics of the misuse of sodomy and sedition laws into 2014. The context in which the new data privacy law in Malaysia arrives is a multi-racial society (but probably the most Islamic society that has a data privacy law), a quasi-democratic polity, and one in which the legal system continues to be misused for political ends.

1.2. Legal system of Malaysia

Malaysia is a federation of states with a parliamentary system of government, headed by a constitutional monarch (the Yang di-Pertuan Agong, elected in five-year rotations from the hereditary rulers of nine states). It has separation of powers between parliament, executive, and judiciary, and a government headed by a Prime Minister. This occurs at both federal and state levels. The bicameral federal parliament has an upper house which is in part appointed, and in part elected from state parliaments. The division of legislative powers between the federal and state governments is provided in the federal Constitution, with most, but not all, powers in relation to privacy issues located at the federal level.[6]

The judiciary comprises the Federal Court (the highest court), the Court of Appeal and two High Courts (one for Peninsular Malaysia, one for Borneo and Sarawak), plus various subordinate courts, including the Sessions Court, which has jurisdiction over offences under the PDPA. In 1985 appeals to the UK Privy Council were abolished. The judiciary is empowered to interpret the Constitution and to determine whether legislation is unconstitutional. Judges are appointed by the monarch, on the advice of the government.[7] The Constitution provides that 'Islam is the religion of the Federation; but other religions may be practised in peace and harmony in any part of the Federation'.[8] There is a Syariah Court of the Federal Territories.

The application of English common law and equity in Malaysia is governed by the Civil Law Act 1956, section 3(1) and other provisions which provide that courts in Malaysia will apply the common law and rules of equity of England as they applied prior to 1956 (and in some parts of Malaysia, prior to 1951 or 1949). Consequently, developments in United Kingdom law subsequent to those dates do not have binding effect on Malaysian courts, although they may be persuasive.[9]

Tey considers that 'the rule of law has been considerably weakened by several events concerning the judiciary'. He presents a detailed account of 'the executive's taming of the **(p.320)** Malaysian courts', including the manipulation by the executive of mechanisms for removal of members of the judiciary (resulting in the removal of the highest judicial officer and two others by a dubious tribunal), constitutional amendments to reduce judicial powers, judicial misbehaviours ('rot from within'), and the legal persecution of political opponents.[10] All of this contributed to an assessment of Malaysia's legal system in 2000 as one of the five worst in Asia, a perception compounded by the backlog of 700,000 cases at that time.[11] The possibility of misuse of the PDPA needs to be guarded against, given Malaysia's legal history.

1.3. State surveillance in Malaysia

The Malaysian state has in the past operated a rather heavy-handed, though not pervasive, set of surveillance measures, but there has been some liberalization in recent years. Much of Malaysia's most controversial surveillance was carried out under the Internal Security Act (ISA), enacted in the 1960s at the time of the Communist insurgency.[12] The Act was repealed in 2009 and replaced in 2013 by legislation which continues to contain some repressive features.[13] Malaysia phased in MyKad from 1999 and became 'one of the first countries in the world to use a chip-based identification card that is also a multipurpose smart card'. It 'has seven functions other than identification: driver's licence, passport information, health information, e-cash function (referred to as electronic purse, or e-purse), toll payment (or Touch 'n Go), automated teller machine, and public key infrastructure'.[14] It contains a photo and thumbprint, and is compulsory for all newborn children. Its use is compulsory for almost all government purposes, and for many private sector uses. Nevertheless, as of 2013 over a million Malaysians had failed to renew their MyKads, and 64,000 had failed to apply for them.[15] MyKad use by the public sector is outside the scope of the PDPA, and will only be relevant in relation to 'commercial transactions' in the private sector (see section 3.2 of this chapter).

2. Privacy protections outside the data privacy law of Malaysia

Other than in the PDPA, privacy protections in Malaysia are not significant, except for a law of very limited benefit in the credit reporting sector.

2.1. Constitutional and treaty protections

Malaysia's federal Constitution does not include any explicit reference to privacy in its list of 'fundamental liberties',[16] nor any protections which are likely to provide an implied right **(p.321)** of privacy, with the possible exception of the requirement that '[n]o person shall be deprived of his…personal liberty save in accordance with law'.[17] As Munir and Yasin note,[18] Malaysia's Federal Court has stated, although only in dicta, that it is 'patently clear from a review of the authorities that "personal liberty" in Article 5(1) includes within its compass other rights such as the right to privacy',[19] referring to Indian case law on similar provisions in its Constitution. It is therefore still possible that some protection of privacy could develop through Malaysia's Constitution.

Malaysia has not signed the International Covenant on Civil and Political Rights 1966

(ICCPR), so it has no treaty obligations concerning privacy. It is a member of the Asia-Pacific Economic Cooperation (APEC), and so is supposed to adhere to the APEC Privacy Framework, but is not a party to the APEC Cross-border Privacy Rules (CBPR). As an ASEAN member it is a signatory to the ASEAN Human Rights Declaration (see Chapter 2). Malaysia therefore has no binding international commitments concerning privacy.

2.2. Common law and equity

Malaysian courts, in a series of cases,[20] have rejected claims based on a common law tort of invasion of privacy, culminating in the Court of Appeal upholding a finding that 'the law of this country, as it stands presently, does not make an invasion of privacy an actionable wrongdoing'.[21]

The development in the United Kingdom of the law of breach of confidence to protect individual privacy is a post-1956 development, and Malaysian courts have not yet held conclusively whether or not similar developments will take place in the now-separate common law and equity of Malaysia. The recent cases concerning a common law tort have not considered the question of breach of confidence.

2.3. Credit Reporting Agencies Act

Credit reporting agencies (CRAs) are exempted from the PDPA. The Credit Reporting Agencies Act 2010 (CRAA) was enacted contemporaneously with the PDPA, apparently in response to difficulties experienced by a credit reporting company called Credit Tip Off Services.[22] Detailed consideration of such sectoral laws is beyond the scope of this book; however, the CRAA has been analysed by Munir and Yasin,[23] who conclude that the structure based on a separate Act is not ideal and that '[i]deally, like in Australia or New Zealand, the provisions on CRAs should be either incorporated into or derived from the PDPA'. They identify deficiencies such as the lack of definition of what information may be provided to CRAs, and a complete lack of restriction on who can obtain reports from CRAs.[24] It would seem that this Act is a retrograde step for privacy protection in Malaysia, and strikes a 'poor balance' between the interests of consumers and commerce, as Munir and Yasin put it.[25]

(p.322) ### 2.4. Public sector—state freedom of information laws

The states of Selangor and Penang, both with governments led by the federal opposition party (Pakatan Rakyat) both enacted freedom of information laws in 2011.[26] These laws therefore provide the first legal rights for Malaysians in those states to have access to their own records held by government bodies, including government-linked corporations and local governments in Selangor. There are no such rights at the federal level.

3. Limits on the scope of the PDPA

The PDPA has a largely conventional definition of 'personal data', but limits its application to automated transactions, plus only some manual transactions. The scope is limited to personal data in commercial transactions, and excludes government. The PDPA can only be said to cover part of the private sector, and then subject to many exceptions, particularly where any state-related activities are concerned. Within its scope it will be

valuable, but the narrow scope of the Act must always be kept in mind.

3.1. Meaning of 'personal data'

The definition of 'personal data' in the PDPA has a conventional starting point in that it is based on any information which identifies a person: information 'that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user'.[27] It explicitly includes sensitive personal data (defined separately), and expressions of opinion about the data subject.

However, the definition also requires that the information satisfy one of three conditions, which can be summarized as: (a) it is being processed by automatic means; (b) it is recorded with the intention that it be so processed; or (c) it is recorded as part of a 'relevant filing system' (or with the intent it should be part of one).[28] A 'relevant filing system' is defined as a set of information structured either by reference to individuals or their characteristics so that 'information relating to a particular individual is readily accessible'.[29] The result is that almost all collection of personal data for inclusion in automated or manual record-keeping systems will be included, and only some incidental recording of identifying data in manual systems in ways which cannot effectively be subsequently retrieved will be excluded. Some marginal cases may be contentious. Any processing of identifying data by automated means, even if it cannot be subsequently retrieved, will be included.

3.2. Limitation to commercial transactions

The Act applies only to 'any personal data in respect of commercial transactions'.[30] The definition of personal data also restricts it to 'information in respect of commercial transactions'.[31] 'Commercial transactions' are defined broadly to mean 'any transaction of a commercial nature, whether contractual or not' and that this 'includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, **(p.323)** banking and insurance'.[32] The Information Communication and Culture Ministry has estimated that 25,000 institutions would come under the Act.

The PDPA includes the usual exemption for 'personal, family and household affairs'[33] but the limitation to 'commercial transactions' will also exclude the non-commercial affairs of churches, educational institutions, and non-profit organizations. It should also exclude information about conduct in government affairs. There is no 'small business exemption', unlike in Australia or Japan. Credit reporting business carried out by a credit reporting agency is exempt and is subject to separate legislation (see section 2.3 of this chapter).

3.3. Exclusion of the public sector and 'regulatory functions'

The largest omission from the scope of the PDPA is that it 'shall not apply to the Federal and State Governments'.[34] The exact boundaries of this exclusion are not clear from the PDPA or interpretation legislation.[35] Munir and Yasin question whether even departments under ministries are included,[36] but this would seem to be an unusual exclusion from the meaning of 'government'. It is more likely that government-owned

trading companies would fall outside the meaning of 'governments', as would companies carrying out government business under contract, and such bodies would have to comply with the PDPA, provided that what they were doing could be classified as 'commercial activities'.

There is a very broad exemption under section 45(2)(e) from most of the principles for any processing by commercial organizations 'for the purpose of discharging regulatory functions' where application of the Act would be likely to prejudice those functions.[37] This may be used to exempt some government-owned companies, and other companies, from some aspects of the Act.

The correct approach is to first determine whether an entity is to be regarded as a 'government' entity, in which case the PDPA will not apply even if it is carrying out commercial activities. If it is not a 'government' entity, then the question of 'commercial activities' comes into play, and then the possible exemption under section 45(2)(e).

Malaysia does not have other significant protections for personal information in the public sector which limit state abuses of privacy, such as the 'right to information' Acts found in some other Asian states. Singapore's Act also excludes the public sector, but in different terms (see Chapter 10).

3.4. A limited media exception

Processing for the purpose of publishing 'journalistic, literary or artistic material' is exempted (except from the security principle), but only where the data user reasonably believes that (a) the publication would be in the public interest (taking into account the 'special importance of public interest in freedom of expression'), and (b) compliance with a particular principle or provision is 'incompatible with the journalistic, literary or artistic purposes'.[38] This is not a blanket 'media exemption' but a carefully written partial exemption, and one which it will be complex for the media, Commissioner and courts to apply. It is important that this Act should not unduly restrict freedom of expression in Malaysia.

(p.324) 3.5. Other exemptions, including ministerial orders

There are other broad exemptions in section 45 for processing of personal data for specified purposes: for prevention of physical or mental harm; for statistical and research uses that do not produce identified outputs; and in connection with court processes. These are not blanket exemptions from all principles, and typically do not provide exemptions from the security, data integrity, and retention principles. In addition, there are lengthy lists of exemptions from specific principles, particularly the disclosure principle. Finally, the minister may, upon the recommendation of the Commissioner, exempt a data user or class of data users from any of the principles or other provisions of the Act.[39]

3.6. Obligations only on data users, not data processors

Obligations under the PDPA are imposed only on 'data users', defined as 'a person who

either alone or jointly or in common with other persons processes any personal data or has control over or authorizes the processing of any personal data'.[40] The definition expressly excludes a 'data processor' from its scope, defined as a 'person, other than an employee of the data user, who processes the personal data solely on behalf of the data user, and does not process the personal data for any of his own purposes'.[41] If a data processor starts to process the data for his or her own purposes (for example, by using or disclosing it, or storing it after it was supposed to be deleted), then the processor becomes a data user at that point, with the liability imposed by the Act.

3.7. Conclusions concerning the scope of the Act

The cumulative effect of all of these different types of limitations is that Malaysia's PDPA has an exceptionally narrow scope, which can be summarized as the systematic use of personal data arising from commercial transactions in some other commercial transactions (not involving the government), subject to numerous exceptions both stated in the Act and subject to potential expansion by the minister. However, some uncertain aspects of the apparent exclusions of the government from the Act, and the meaning of 'commercial transactions', create latitude for potentially surprising interpretations of the scope of the Act by the Commissioner and the courts.

Rectification of anomalies in the Act

The minister can rectify anomalies by using his powers to issue a gazette notice under section 144 to modify the Act in whatever way seems 'necessary or expedient for the purposes of removing any difficulties or preventing anomalies in consequence of the coming into operation of this Act'.

4. Seven principles in the PDPA, plus data subject rights

The PDPA's seven personal data protection principles in sections 5–12 (named general; notice and choice; disclosure; security; retention; data integrity; and access) are more **(p.325)** strongly influenced by the EU Data Protection Directive than by the OECD Guidelines or APEC Framework. The EU-style starting point is that processing of personal data (including collection) requires consent.[42] There are also what are, in effect, additional principles in Part II Division 4 'Rights of Data Subject', where the EU Directive's influence is seen even more clearly: the right of data subjects to withdraw consent to processing; a further right to prevent processing likely to cause damage or distress, which is independent of questions of consent; and the right to prevent processing for the purposes of direct marketing.[43] Many other exceptions to the principles are provided throughout the Act. The Regulations also now add more detail to the obligations and rights in the PDPA.

4.1. The 'general principle'—processing with consent

The general principle in section 6 is that data users must not process personal data unless the data subject has given consent to the processing. 'Processing' is a term of the broadest possible meaning, covering everything from collection, storage, use, and disclosure, to destruction of personal data.[44] Processing without consent is then permitted in six situations, three of which concern the processing agreed to by the data

subject or to protect the data subject's vital interests, and the other three concern processing for the purposes of carrying out of the legal obligations of the data user, the functions under any law of any third party, or the administration of justice.[45] This results in an extremely broad 'authorized by law' type of exception to everything to do with personal data, and to all other principles, because of the broad meaning of 'processing'. These exceptions do not apply to sensitive personal data, which may only be processed in compliance with section 40 (see section 4.5 of this chapter).

Regulations provide considerable detail on what is required for such consent.[46] Consent must be in a form that can be recorded and properly maintained. If consent is required for multiple matters, each requirement for consent must be distinguishable in how it is presented. Consent must be required from parents or guardians concerning those under 18, and similarly for those whose affairs are under court-appointed management. The onus of proof of all these matters is on the data user. These requirements for 'unbundling' of consents, and the onus of proof, are unusual and otherwise only found in Asia in South Korea's law.

4.2. Other general processing limitations—lawfulness, necessary, and 'not excessive'

Section 6(3) sets out three other general limits on processing, based on its purpose: (a) it must be for a lawful purpose, and one directly related to an activity of a data user; (b) it must be necessary for or directly related to that purpose; and (c) the personal data must be 'adequate but not excessive in relation to that purpose'. Given the breadth of the meaning of 'processing', these limits must be considered concerning all uses of personal data.

(p.326) 4.3. Collection and notice principles

Data users must obtain data subject consent to processing of their data.[47] They must give 'written notice' of the purpose of collection[48] no matter how the data is collected, whether from the data subject or otherwise. The notice must be given 'as soon as practicable', and where data is collected from the data subject it is implied that notice must be either (a) when the data subject is first asked to provide it (i.e. before provision), or (b) when it is collected (i.e. at the time of provision).[49] However, 'in any other case' (i.e. when collected from third parties or by other means), the notice must be given before use for other directly related purposes, or before disclosures, but not before the data is used for the purpose for which it was collected.[50] If data subjects do not always receive notice about data collected from third parties, then it is difficult to see that processing always requires consent. Regulations specify that the notice must provide the designation of the contact person, and their phone number, plus fax and email contacts if they have them.[51]

4.4. Use and disclosure principles

The Malaysian Act has considerable ambiguities concerning use and disclosure. There is no separate principle concerning use, so personal data may only be used with consent (or under one of the six exceptions where consent is not required for processing),[52] and subject to section 6(3) which requires that personal data:

> shall not be processed unless—
>
> (a) the personal data is processed for a lawful purpose directly related to an activity of the data user; [and]
>
> (b) the processing of the personal data is necessary for or directly related to that purpose.

Secondary *uses* are therefore based on consent, not on being directly related to the purpose of collection. On the other hand, personal data may only be *disclosed* for the purpose of collection or purposes 'directly related' to it,[53] and[54] must also be to 'the class of third parties' about whom the data user has given notice that they 'may disclose' the data.[55] The data user will still have to establish that such notice constitutes the data subject's implied consent to process the data. Such notice is therefore not a complete 'blank cheque' for data users to disclose personal data to anyone they choose, by the device of a general statement about the possibility of disclosure, because these conditions must still be satisfied. Alternatively, the disclosure may come under one of the six exceptions to processing without consent (see section 4.1 of this chapter).[56] Regulations require that data users must maintain a list of such disclosures for 'directly related' purposes.[57] But where disclosures are made under the exceptions to section 6, no such logging is required.

These restrictions on disclosures by data users are backed up by offences which are committed by third parties who collect, or disclose, or sell personal data held by a data user, unless the third party can show that they acted under conditions justifying their acts.[58]

(p.327) 4.5. Sensitive personal data

'Sensitive personal data' includes physical or mental health or condition; political or religious or similar beliefs; allegations of commission of offences (convictions are not mentioned); and any other personal data the minister may determine by order to be 'sensitive'. Sensitive data must also be 'personal data',[59] and since 'personal data' is limited to 'information in respect of commercial transactions', this also restricts the scope of protection of 'sensitive' data. Malaysia includes only a subset of the EU categories, omitting racial or ethnic origin, trade union membership, and sex life, despite these being sensitive topics in Malaysian life.

The processing of sensitive personal data requires 'explicit consent' (which suggests that 'consent' by itself includes implied consent), or for other exceptions to apply.[60] Among the list of very broad exceptions to the consent requirement are that the use is necessary 'for the exercise of any functions conferred on any person by or under any written law' or 'for any other purpose as the Minister thinks fit'. There is also an exception where a person has made public their own sensitive personal data,[61] which is not an exception for ordinary personal data. However, such disclosure might be considered to be implied consent to processing of ordinary personal data.

There is a danger that this provision will be abused by the Malaysian state (which is in effect exempt from the legislation) whereas those who attempt to raise allegations of criminality or discuss other sensitive issues could be prosecuted if they fall outside the media exemptions. The danger is reduced somewhat by the 'commercial transaction' limitation. The provisions are complex, but the danger is there.

4.6. Security principle

The security principle requires data users to 'take practical steps', having regard to six specified security factors.[62] Data users are required by Regulations to have security policies which comply with the 'security standard' set periodically by the Commissioner.[63] They must also ensure that any data processors acting on their behalf comply with those policies. The security principle is not included in many of the exemptions in Part III, so it applies to a much broader range of data than the other principles, and therefore has additional importance. Although it does not require 'reasonable steps' as is often required, this is unlikely to make any real difference given how specific the Commissioner's requirements may be.

4.7. Data retention principle and rights to block processing

Personal data cannot be retained for longer than the fulfilment of the purposes for which it is legitimately processed, and it is the data user's responsibility to ensure that the data is then 'destroyed or permanently deleted'.[64] No option of anonymization is explicitly given, and the wording of the section would seem to preclude it. Data users must comply with any 'retention standard' that the Commissioner may prescribe.[65]

(p.328) In addition to these deletion rights, data subjects can, under section 38, withdraw consent to the processing of their data at any time and data users must comply.[66] It must be assumed that this is subject to the exceptions to section 6 where consent to processing is not required. Data subjects may also give a data user a 'data subject notice' requesting cessation of processing, or for processing not to commence, for a specific period or for a specific purpose, if (for reasons stated) the processing is likely to cause substantial and unwarranted damage or distress to the data subject or another person.[67] This blocking of processing does not seem to be restricted to processing requiring consent, and is therefore broader than the section 38 right to withdraw consent. The enforcement procedures are discussed in section 7 of this chapter.

Direct marketing implications

The right to withdraw consent to processing under section 38 is of particular importance to direct marketing. Since direct marketing is not one of the exceptions to the requirement for consent to processing, consent is necessary, and can therefore be withdrawn. The result is a right to 'opt out' of direct marketing uses of personal data at any time, and irrespective of prior consent.[68]

4.8. Data integrity principle

The data integrity principle is comprehensive: 'A data user shall take reasonable steps to

ensure that the personal data is accurate, complete, not misleading and kept up-to-date by having regard to the purpose, including any directly related purpose, for which the personal data was collected and further processed.'[69] Data users must comply with any 'data integrity standard' that the Commissioner may prescribe.[70]

4.9. Access and correction principle

Data subjects have standard rights to access their personal data and to correct it where it is 'inaccurate, incomplete, misleading or not up-to-date', except where their requests are refused in accordance with the Act.[71] The grounds for, and procedures relevant to, compliance with or refusal of access and correction requests are set out in sections 30–37. Regulations set out the requirements for acknowledgement of access and correction requests, and the identification details that data users may legitimately require from data subjects (name, address, and ID number, unless the Commissioner specifies otherwise).[72]

Where correction of personal data is refused by a data user in relation to an expression of opinion (including an assertion of fact which is unverifiable), then the data subject is entitled to have a note of their opinion of the correct state of affairs added to their file. It must be added in such a way that the contested opinion cannot be accessed without the data subject's note also being accessed.[73]

(p.329) ### 4.10. Conclusions concerning the privacy principles

Although constrained by the excessively limited overall scope of the Act, the privacy principles found in the PDPA cover all of the elements in the minimum privacy principles. The influence of the EU Directive results in many stronger 'European' elements also being included. Strong points of the principles include the requirement for consent (with few exceptions) for collection and subsequent processing, the requirement to 'unbundle' consents, and the right to opt out from processing requiring consent. The weaknesses of the principles include the broad 'authorized by law' exceptions, and the right to create exceptions allowing secondary uses by giving notice (Malaysia is not alone).

5. International data flows and controller–processor relationships in Malaysia

This section considers the six key issues concerning international data flows (see Chapter 3, section 3.3), and controller-processor relationships.

5.1. Extraterritoriality

The PDPA applies to anyone 'established in Malaysia'[74] or who 'uses equipment in Malaysia' (except for transit through Malaysia).[75] Those using equipment in Malaysia must nominate a representative established in Malaysia.[76] The Act has no application to 'personal data processed outside Malaysia', with the interesting exception of where data is 'intended to be further processed in Malaysia'.[77] Temporary exports of data from Malaysia for purposes of such processing (whether on economic grounds, or in an attempt to avoid requirements of the Act) will therefore be subject to the PDPA. So would personal data pre-processed outside Malaysia, if it was at that time intended that it be further processed in Malaysia.

5.2. Data export rules

Personal data may not be transferred outside Malaysia unless the destination is on a 'whitelist' specified by the minister, after receiving the Commissioner's advice.[78] The minister can so specify a place (including a country but not restricted to countries—for example, Hong Kong SAR) if it has in force a law 'substantially similar' to the Malaysian Act, or the place ensures 'an adequate level of protection…which is at least equivalent to the level of protection' provided by Malaysia's Act. There are exceptions similar to those found in Article 26 of the EU Data Protection Directive, but some which go considerably further than the Directive, including where 'the data user has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not in that place be processed in a manner which, if that place is Malaysia, would be a contravention of this Act'.[79] This applies whether the transfer is to third parties for their own processing purposes, or to a data processor to process on behalf of the Malaysian data user.

(p.330) Unless the Commissioner takes a strict interpretation of when a data user has 'taken all reasonable precautions and exercised all due diligence', section 129 will essentially provide a front door to data exports (the 'whitelist') which appears to be shut, while the back door is wide open to transfers to anywhere, with exporters absolved from any accountability for what goes wrong provided they go through a 'due diligence' ritual. A data user which contravenes section 129 will, upon conviction, be liable to a fine of up to 300,000 Ringgits (US$91,000) or up to two years' imprisonment.

5.3. Relationship between controller (data user) and processor, and their liabilities

The Act imposes obligations only on local data controllers ('data users'), and not on processors unless and until they process personal data for their own purposes and not those of the data controller (see section 3.6 of this chapter). Similarly, an overseas data processor which acts solely within the terms of the processing contract will not have any liability under the PDPA, because obligations are imposed only on data users. If the overseas processor acts outside those obligation then it becomes a data user with potential obligations under the PDPA, but the Act will have extraterritorial effect if (and only if) the data is intended to be further processed (i.e. used in any way) in Malaysia. But this will be of little use to Malaysian data subjects if it is necessary for them to take action against a data processor located overseas. Although the Malaysian-based data user is only liable for the actions of the overseas processor if those actions are 'authorized' within the terms of the processing contract, in many instances that may give data subjects an action in a Malaysian court against a Malaysian data user.

5.4. Data imports and an 'outsourcing exemption'

If personal data is imported into Malaysia for the purpose of processing on behalf of an overseas company by a Malaysian company, the Malaysian company is a data processor, not a data user, and therefore does not have liabilities under the Act. Whether the overseas company can be classified as a data user depends on whether the company is 'established in Malaysia', because it is unlikely that it can be said that it 'uses equipment in Malaysia'.[80] It seems, therefore, that personal data sent to Malaysia for processing is

subject to an 'outsourcing exemption'. This exemption is likely to undermine any attempt by Malaysia to achieve adequacy status in relation to the EU, and is likely to complicate Malaysia's position in relation to data exports from other countries whose laws include data export restrictions.

6. Malaysia's Personal Data Protection Commissioner and Appeal Tribunal

Malaysia has a Personal Data Protection Commissioner appointed by the minister.[81] A separate Department has also been established to administer the Act.[82] The Commissioner is appointed for up to three years, and may be re-appointed,[83] but he or she may also **(p.331)** be dismissed by the minister, who only needs to 'state the reason'.[84] The Commissioner's remuneration and allowances are also determined by the minister.[85] The Commissioner's annual report goes to the minister,[86] with no requirement that it goes to the Parliament or be made public. In order to further underline the Commissioner's lack of independence, it is explicitly stated that 'the Commissioner shall be responsible to the Minister' and 'the Minister may give the Commissioner directions of a general character consistent with the provisions of the Act'.[87] However, the Commissioner is protected against legal actions while carrying out his or her duties in good faith.[88]

The Act provides the Commissioner with a normal range of functions and powers.[89] The Commissioner is required to provide reasons for any decisions made, upon request by any person aggrieved by such a decision[90] (typically a data subject or data user). Complaints to the Malaysian data protection authority (DPA) can only be by individuals: there is no provision for class complaints. The enforcement powers of the Commissioner are tied to the existence of a complaint (even if it has been withdrawn), so there is no provision for enforcement of any 'own motion' investigations.

6.1. Appeal Tribunal

Any decisions by the Commissioner may be appealed to an Appeal Tribunal, including questions of registration of data users, registration of codes of practice, issuance of enforcement notices, and even 'the refusal of the Commissioner to carry out or continue an investigation initiated by a complaint'.[91] The minister appoints the Appeal Tribunal of at least three members.[92] Appointment is for a term of up to three years (with one further term allowed).[93] Appointments may be revoked by the minister, who must state the reasons for revocation.[94] There is no right of appeal to the courts from a decision of the Appeal Tribunal.[95]

6.2. Independence

A Commissioner who is not independent may still be effective, at least while he or she has a minister sympathetic to privacy. Unlike the Privacy Commissioners in Australia, New Zealand, Canada, South Korea, and Hong Kong, which have statutory provisions underwriting their independence, those in Malaysia and Singapore do not. If the Malaysian Commissioner applies for accreditation to either or both of the International Conference of Data Protection and Privacy Commissioners (ICDPPC) or the Asia-Pacific Privacy Authorities (APPA), it will be a litmus test of the accreditation requirements of

both bodies. As discussed in section 6 of chapter 2, these accreditation standards previously required that a DPA must have 'an appropriate degree of autonomy and independence' and be able 'to operate free from political or governmental interference' and be removed 'only for inability to perform the office, neglect of duty or serious, misconduct', but have been weakened. The Malaysian legislation does not establish an office that would meet requirements of independence, and local experts have noted that the Commissioner' would not be independent'.[96] **(p.332)**

7. Reactive enforcement provisions in Malaysia under the PDPA

The PDPA is unusual is that prosecution of offences is almost the only significant means by which the Act can be enforced, except for an injunction-like procedure by which the Commissioner can stop certain processing.

7.1. Enforcement notices and directions by Commissioner

If the Commissioner, after investigation, considers that a data user is (currently) contravening the Act, or has done so in the past and is likely to continue or repeat doing so, then the Commissioner can issue an enforcement notice requiring the contravention to be remedied.[97] Breaches that have caused harm, but are unlikely to be repeated, fall outside the scope of enforcement notices, but can be prosecuted as offences simply because of the breach of the principle concerned (as discussed in section 7.2 of this chapter). The issuing of an enforcement notice gives the Commissioner a more flexible approach when breaches are ongoing or likely to be repeated, but no role to play when 'the damage has been done'.

In an enforcement notice, the Commissioner may, after specifying the nature of the contravention and the relevant provisions, direct the data user to take two types of actions: (i) to take such steps as are specified to remedy the contravention, within a specified period (not less than the period allowed for an appeal); and (ii) to cease processing the personal data pending the remedial actions being taken by the data user.[98] The notice may specify alternative steps that can be taken.[99]

Failure to comply with an enforcement notice is an offence, with conviction resulting in a fine of up to 200,000 Ringgits (US$60,000).[100] There is a right of appeal against issuance of an enforcement notice to an Appeal Tribunal.[101] There is no right of appeal against non-issuance of an enforcement notice, which seems somewhat unfair to data subjects, and surprising since there is a right of appeal against the Commissioner's failure to investigate a complaint.[102] This does not count as a 'right of appeal' against the Commissioner's decisions, since it is only one-sided, in favour of data users.

The reliance on enforcement notices is less of a problem than it is under Hong Kong's law, at least in theory, because under Malaysia's PDPA breaches of principles are in themselves potential offences. However, the fact that these are only criminal offences, depending on a decision to prosecute, and are not accompanied by any right to pursue a civil action, leaves complainants powerless.

Blocking of processing following 'data subject notices'

A data subject may give a notice to a data user requiring processing of personal data to cease, or not to begin, on the basis that the processing 'is causing or is likely to cause substantial damage or substantial distress to him or to another person' and 'the damage or distress is or would be unwarranted'.[103]

(p.333) 7.2. Offences

Data users who breach one of the seven principles in sections 6–12 (subject to any defences and exceptions) commit an offence which can on conviction result in a fine of 300,000 Ringgits (nearly US$90,000) or two years' imprisonment.[104] Further offences can be committed by failure to comply with various 'rights of the data subject', including the right to have an 'expression of opinion' recorded where correction is refused, the withdrawal of consent to processing, the requirements for processing of sensitive data, and the right to opt out of direct marketing.[105] Contravention of various regulations requiring obtaining consent, or failure to adhere to the various standards set by the Commissioner can also on conviction result in fines of 250,000 Ringgits (US$75,000) or up to two years' imprisonment.[106] In summary, failure to comply with the substantive obligations set out in the Act generally constitutes an offence, no matter where those obligations are located. Prosecutions must be by or with the written consent of the Public Prosecutor,[107] and are within the jurisdiction of a Sessions Court,[108] one of the subordinate courts. As criminal offences, the normal provisions for appeal under Malaysian law will apply.

7.3. A deficient 'enforcement pyramid'

There are major, probably crippling, deficiencies in the PDPA's 'enforcement pyramid'. Although the provisions concerning offences and enforcement notices are comprehensive enough concerning ongoing breaches (or those likely to be repeated), the Commissioner can do nothing to assist complainants where the damage is already done but the breach is unlikely to be repeated. This is the same deficiency as the pre-2012 Hong Kong law. The Act is also defective in only providing some rights of appeal against the Commissioner's decisions to respondent companies, but not to complainants.

The criminal offences are broad, potentially applying to any breaches of the principles, but they depend on a decision to prosecute (which will rarely be exercised), and are not accompanied by any right to pursue a civil action, leaving complainants powerless. There are no provisions by which complainants may seek compensation for damage: the Commissioner cannot award damages; data subjects cannot seek compensation in court proceedings under the Act; and Malaysia has not developed a tort of invasion of privacy.

No matter how diligent privacy Commissioners may be, if they do not have the necessary enforcement tools, there are severe limits to what they can achieve. Malaysia's Commissioner will need more arrows in the quiver than this Act provides.

8. Systemic enforcement under the PDPA

8.1. Systemic enforcement measures—inspections only

The Commissioner has powers to inspect data user's systems.[109] Data users are required to keep records of any application, notice, request, or any other information relating to personal data, and the Commissioner can determine how it will be kept.[110] Regulations specify what the Commissioner may require a data user to provide on such an inspection, including records of consent to processing, the notices issued to data users, the list of **(p.334)** disclosures to third parties, and the records of compliance with various standards issued by the Commissioner.[111]

8.2. Registration of data users

Registration of specific classes of data users may be required by the minister on the recommendation of the Commissioner.[112] The minister made such regulations on the day the Act came into force, both to specify the classes of data users required to register,[113] and the procedure for registration.[114] Existing data users in classes requiring registration had three months to register from 15 November 2013.[115] The classes of data users required to register are such that they cover most significant data users. Therefore, this is not registration limited to those whose activities might justify intensive surveillance and supervision by the Commissioner (an aspect of enforcement), but rather a revenue-raising approach to offsetting the cost of running the Commissioner's office. Registration will cost between 100–400 Ringgits (US$30 and US$120), depending on the type of business entity, possibly annually. Failure to register or renew may result in fines of up to 250,00 Ringgits (US$75,000).[116]

In summary, the classes of data users requiring registration are:[117] licensees under communications and postal laws; banking and financial institutions; insurers; licensed health care and pharmacy providers; tourism and hospitality service operators, and tourist accommodation providers; aviation transport providers; private educational institutions; licensed direct selling organizations; companies or partnerships carrying on business as lawyers, auditors, accountants, engineers, or architects; those conducting retail or wholesale dealings under the Control of Supplies Act 1961; private employment agencies; various categories of housing developers; and named utilities. A very wide range of Malaysian businesses are therefore required to register, and they appear to be primarily those which would hold substantial amounts of personal information.

8.3. Codes of practice and 'data user forums'

The Commissioner can also designate a body (such as an industry association) as a 'data user forum', which is then able to prepare a code of practice, which the Commissioner may then issue. Data users belonging to that class must then comply with this code, with breaches subject to fines of up to 100,000 Ringgits (US$30,000).[118] No such bodies have yet been designated. While such codes could be useful, used sparingly, experience in other jurisdictions in Asia and Australasia has not shown them to be important in many industry sectors as yet (credit is an exception in some jurisdictions).

9. Evaluation—an Act of uncertain effectiveness

The PDPA has very limited scope, and an extremely defective and limited method of enforcement. On the other hand, the principles contained in the Act are generally **(p.335)**

reasonable, subject to deficiencies in relation to secondary uses, and often include stronger 'European' elements. While the PDPA has many such deficiencies, this data privacy legislation will be a significant step forward for Malaysians. In the hands of a Commissioner committed to privacy protection, and a government which does not impede this, much will be achievable. Nevertheless, the enforcement mechanisms in the Act are very deficient, and unless there are vigorous prosecutions of offences, complainants will be left powerless because of their lack of any rights to take civil actions. The enforcement provisions are worse than the pre-2012 Hong Kong law.

However, if the Act is well managed and vigorously enforced, and gains credibility, Malaysian politics may deliver further improvements to it in future, particularly in expansion of scope to cover the public sector, and provision of some avenue for compensatory damages. For Malaysians to be able to focus on real issues in data protection, because of the existence of this Act, will inevitably increase the demand for better protection. The main 'democratic deficit' in the law is the omission of the public sector. However, Malaysia developed separate e-commerce Acts for each of its private and public sectors, so it is possible it may develop separate government sector privacy legislation some time in the future, under a different regime.

Notes:

([1]) Abu Bakar Munir, 'Malaysia Introduces Personal Data Protection Bill' (2008) 102 *Privacy Laws & Business International Newsletter*, pp. 18–19; Graham Greenleaf, 'Limitations of Malaysia's Data Protection Bill' (2010) 104 *Privacy Laws & Business International Newsletter*, pp. 5–7, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2025357>.

([2]) Personal Data Protection Regulations, 2013; Personal Data Protection (Registration of Data User) Regulations 2013. The PDPA (Malaysia) is at <http://www.pdp.gov.my/images/LAWS_OF_**MALAYSIA**_PDPA.pdf>.

([3]) For a short history, see Peter Church, ch. 6 'Malaysia' in *A Short History of South East Asia* (5th Edn., John Wiley and Sons, 2009), from which the following summary is principally derived.

([4]) See Church, *A Short History of South East Asia*, ch. 6 for a summary. For more detailed analysis, see William Case, ch. 4 'Malaysia: Semi-democracy with Strain Points' in *Politics in Southeast Asia* (Curzon Press, 2002); Adbul Razak Baginda (Ed.) *Governing Malaysia* (Malaysian Strategic Research Centre, 2009); and John Pike, *Empires at War: A Short History of Modern Asia Since World War II* (I B Tauris, 2010), chs. 17 and 45, and pp. 713–14.

([5]) See Wong Chin Huat and Noraini Othman, ch. 1 'Malaysia at 50—An "Electoral One-Party State"' in Baginda (Ed.), *Governing Malaysia*, pp. 1–2.

([6]) Sheik Mohamed Noordin and Lim Pui Keng, 'Update: An overview of the Malaysian legal system and research' (Globalex, June 2011)

<http://www.nyulawglobal.org/Globalex/Malaysia1.htm>.

([7]) Noordin and Keng, '4 Judicial authority—Sources of case law'.

([8]) Constitution of Malaysia, art. 3(1).

([9]) Tsun Hang Tey, ch. 7 'Malaysia: The Undermining of Its Fundamental Institutions and the Prospects for Reform' in E. Ann Black and Gary F. Bell (Eds.), *Law and Legal Institutions of Asia* (2011, Cambridge), pp. 220–1; Abu Bakar Munir and Siti Hajar Mohd Yasin, *Personal Data Protection in Malaysia: Law and Practice* (Sweet and Maxwell Asia, 2010), p. 14.

([10]) Tey, ch. 7 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, pp. 240–50.

([11]) Tey, ch. 7 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, p. 247, citing the Hong Kong-based Political Economic Risk Consultancy survey.

([12]) It was previously 'used to suppress both political opposition and peaceful dissent', with nearly 100 people still estimated to be imprisoned under it as of 2006. For details, see EPIC, 'Malaysia' in *Privacy & Human Rights* (Electronic Privacy Information Center, 2006) <http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Malaysia.html>. See also Internal Security Act (Malaysia) <http://www.agc.gov.my/Akta/Vol.%202/Act%2082.pdf>.

([13]) The Security Offences (Special Measures) Act 2012 removed the government's right to detain a person without trial, but still allowed detention without warrant for 24 hours in case of suspected security offences, and reduces the maximum detention period for investigation of crime from two years to 28 days.

([14]) EPIC, 'Malaysia' in *Privacy & Human Rights.*

([15]) '1.13 mil Malaysian Don't Apply or Renew MyKad: Ahmad Zahid' (*New Straits Times*, 16 February 2014).

([16]) Constitution of Malaysia, pt. II.

([17]) Constitution of Malaysia, art. 5(1).

([18]) Munir and Yasin, *Personal Data Protection in Malaysia*, pp. 14–15.

([19]) *Sivarasa Rasiah v Badan Peguam Malaysia* [2009] MYFC 80 <http://www.asianlii.org/my/cases/MYFC/2009/80.html>.

([20]) Munir and Yasin, *Personal Data Protection in Malaysia*, pp. 13–14.

([21]) *Dr Bernadine Malini Martin v MPH Magazine Sdn Bhd & 2 Lagi* [2010] MYCA 48 <http://www.asianlii.org/my/cases/MYCA/2010/48.html>.

([22]) Munir and Yasin, *Personal Data Protection in Malaysia*, p. 225.

([23]) Munir and Yasin, *Personal Data Protection in Malaysia*, ch. 15.

([24]) Munir and Yasin, *Personal Data Protection in Malaysia*, p. 234.

([25]) Munir and Yasin, *Personal Data Protection in Malaysia*, p. 235.

([26]) Freedom of Information Enactment (Selangor) and Freedom of Information Act (Penang).

([27]) PDPA (Malaysia), s. 4, definition of 'personal data'.

([28]) PDPA (Malaysia), s. 4, definition of 'personal data', conditions (a)–(c).

([29]) PDPA (Malaysia), s. 4, definition of 'relevant filing system'.

([30]) PDPA (Malaysia), s. 2.

([31]) PDPA (Malaysia), s. 4, definition of 'personal data'.

([32]) PDPA (Malaysia), s. 4, definition of 'commercial transactions'.

([33]) PDPA (Malaysia), s. 45(1).

([34]) PDPA (Malaysia), s. 3(1).

([35]) Interpretation Acts 1948 and 1967.

([36]) Munir and Yasin, *Personal Data Protection in Malaysia*, p. 79.

([37]) PDPA (Malaysia), s. 45(2)(e).

([38]) PDPA (Malaysia), s. 45(2)(f).

([39]) PDPA (Malaysia), s. 46.

([40]) PDPA (Malaysia), s. 4, definition of 'data user'.

([41]) PDPA (Malaysia), s. 4, definition of 'data processor'.

([42]) PDPA (Malaysia), s. 6.

([43]) PDPA (Malaysia), ss. 38, 42, and 43 respectively.

([44]) PDPA (Malaysia), s. 4, definition of 'processing'.

([45]) PDPA (Malaysia), s. 6(2).

([46]) Personal Data Protection Regulations, 2013, s. 3.

([47]) PDPA (Malaysia), s. 6.

([48]) PDPA (Malaysia), s. 7.

([49]) PDPA (Malaysia), s. 7(2)(a) and (b).

([50]) PDPA (Malaysia), s. 7(2)(c).

([51]) Personal Data Protection Regulations, 2013, s. 4.

([52]) PDPA (Malaysia), ss. 6(1) and (2) respectively.

([53]) PDPA (Malaysia), s. 8(a).

([54]) The effect of s. 8's structure of 'if not (not a or not b)' is logically the same as 'if (a and b)'.

([55]) PDPA (Malaysia), ss. 7(1)(e) and 8(b).

([56]) PDPA (Malaysia), s. 6.

([57]) Personal Data Protection Regulations, 2013, s. 5.

([58]) PDPA (Malaysia), s. 130.

([59]) PDPA (Malaysia), s. 4 definition 'sensitive personal data'.

([60]) PDPA (Malaysia), s. 40.

([61]) PDPA (Malaysia), s. 40(2).

([62]) PDPA (Malaysia), s. 9.

([63]) Personal Data Protection Regulations, 2013, s. 6.

([64]) PDPA (Malaysia), s. 10.

([65]) Personal Data Protection Regulations, 2013, s. 7.

([66]) PDPA (Malaysia), s. 38.

([67]) PDPA (Malaysia), s. 42.

([68]) See Abu Bakar Munir, ch. 7 'Malaysia's Data Protection Law' in Simon Chesterman, *Data Protection Law in Singapore* (Academy Publishing, 2014), p. 194.

([69]) PDPA (Malaysia), s. 11.

([70]) Personal Data Protection Regulations, 2013, s. 8.

([71]) PDPA (Malaysia), s. 12.

([72]) Personal Data Protection Regulations, 2013, ss. 9–11.

([73]) PDPA (Malaysia), s. 37.

([74]) PDPA (Malaysia), s. 2(2), s. 2(4) defines the circumstances under which business entities are 'established in Malaysia'.

([75]) PDPA (Malaysia), s. 2(2).

([76]) PDPA (Malaysia), s. 2(3).

([77]) PDPA (Malaysia), s. 3(2).

([78]) PDPA (Malaysia), s. 129.

([79]) PDPA (Malaysia), s. 129(3)(f).

([80]) PDPA (Malaysia), s. 2(2).

([81]) PDPA (Malaysia), s. 47.

([82]) Bernama.com (2011), 'New Department to Oversee Implementation of Malaysian Personal Data Protection Act 2010', 20 June 2011 at <http://www.bernama.com.my/bernama/v5/newsgeneral.php?id=595355>.

([83]) PDPA (Malaysia), s. 53.

([84]) PDPA (Malaysia), s. 54.

([85]) PDPA (Malaysia), s. 57.

([86]) PDPA (Malaysia), s. 60.

([87]) PDPA (Malaysia), s. 59.

([88]) PDPA (Malaysia), s. 139.

([89]) PDPA (Malaysia), ss. 48 and 49.

([90]) PDPA (Malaysia), s. 94.

([91]) PDPA (Malaysia), s. 93.

([92]) PDPA (Malaysia), s. 85.

([93]) PDPA (Malaysia), s. 87.

([94]) PDPA (Malaysia), s. 88.

([95]) PDPA (Malaysia), s. 99.

([96]) Shahanaaz Habib, 'Personal Data Still Open to Abuse' (*The Star Online*, 16 October 2011). The quotation is from Professor Abu Bakar Munir, who also said: 'The problem with this is that the Commissioner may not be able to enforce the Act effectively without fear or favour unlike in other countries. In other countries, the Commissioner is not accountable to the minister but is directly accountable to Parliament.'

([97]) PDPA (Malaysia), s. 108(1).

([98]) PDPA (Malaysia), s. 108(1).

([99]) PDPA (Malaysia), s. 108(3)(b).

([100]) PDPA (Malaysia), s. 108(8).

([101]) PDPA (Malaysia), pt. VII.

([102]) PDPA (Malaysia), s. 93.

([103]) PDPA (Malaysia), s. 42.

([104]) PDPA (Malaysia), s. 5(2).

([105]) PDPA (Malaysia), respectively ss. 37(3), 38(4), 40(3), and 43(5).

([106]) Personal Data Protection Regulations, 2013, s. 12, concerning ss. 3(1), 6, 7, and 8 of those Regulations.

([107]) PDPA (Malaysia), s. 134.

([108]) PDPA (Malaysia), s. 135.

([109]) PDPA (Malaysia), ss. 101–103.

([110]) PDPA (Malaysia), s. 44.

([111]) Personal Data Protection Regulations, 2013, s. 14.

([112]) PDPA (Malaysia), s. 14.

([113]) Personal Data Protection (Class of Data Users) Order, 2013.

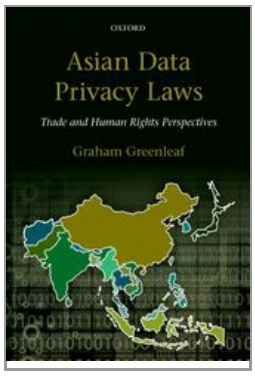
([114]) Personal Data Protection (Registration of Data User) Regulations, 2013.

([115]) PDPA (Malaysia), s. 146.

([116]) Personal Data Protection (Registration of Data Users) Regulations, 2013.

([117]) Class of Data Users Order, Schedule.

([118]) PDPA (Malaysia), pt. II, div. 3 'Data user forum and code of practice', ss. 21–29.



Asian Data Privacy Laws: Trade & Human Rights Perspectives
Graham Greenleaf

Print publication date: 2014
Print ISBN-13: 9780199679669
Published to Oxford Scholarship Online: December 2014
DOI: 10.1093/acprof:oso/9780199679669.001.0001

The Philippines and Thailand—ASEAN's Incomplete Comprehensive Laws

Graham Greenleaf

DOI:10.1093/acprof:oso/9780199679669.003.0012

[–] Abstract and Keywords

Completion of the development of comprehensive data privacy laws in the Philippines and Thailand is important for Asian, and particularly ASEAN (South-East Asia), democracy and civil liberties. This chapter covers both countries. The Philippines will become the first ASEAN country to bring into force a comprehensive data privacy law covering the whole of the private and public sectors, the Data Privacy Act 2012, once the President appoints a data protection authority to complete the process. The National Privacy Commission, when appointed, will implement rules and regulations (IRRs) within 90 days of its appointment, to make the Act effective. It is an Act with many unusual elements, both strengths and weaknesses. Whether Thailand will enact a comprehensive law is unclear, as its current public sector law is defective, and the Bill before its legislature is limited to the private sector.

Keywords: data protection, privacy, Asia, Philippines, Thailand, ASEAN, National Privacy Commission, data

protection authority

1. Incomplete laws and comprehensiveness

Data privacy laws of limited scope are in effect in Singapore and Malaysia (private sector only), and in Indonesia and Vietnam (IT-sub-sector only). The Philippines will become the first Association of Southeast Asian Nations (ASEAN) country to bring into force a comprehensive data privacy law covering the whole of the private and public sectors, once the President appoints a data protection authority to complete the process. Whether Thailand will follow suit is unclear, as its current public sector law is defective, and the Bill before its legislature is limited to the private sector. The development of comprehensive data privacy laws is important for Asian (and particularly ASEAN) democracy and civil liberties.

2. The Philippines—a comprehensive and ambiguous law

The Philippines Data Privacy Act 2012 (DP Act) was signed into law by President Benigno Aquino on 15 August 2012, and came into effect 15 days after its publication.[1] However, by December 2013 it was still not effectively in force, because the President had not appointed the membership of the National Privacy Commission (NPC). The NPC must make implementing rules and regulations (IRRs) within 90 days of its appointment, but then '[e]xisting industries, businesses and offices affected by the implementation of this Act' are given one year from the effective date of the IRRs (or such other period as the NPC may **(p.338)** determine) to comply with the requirements of the Act.[2] The Philippines legislation is therefore unlikely to come into effect until mid-2015 or later, depending on when a NPC is appointed. This chapter therefore analyses the content of the Act only, without benefit of the IRRs. First, however, it is necessary to consider the context of the law, and such other privacy protections as Philippines' law provides.

2.1. Context

The Philippines has achieved a relatively stable but low-quality democracy, with a judicial system to match.

The Philippines—historical and political context

Spain ceded the Philippines to the USA in 1898 at the end of the Spanish-American War. The USA occupied the Philippines (except for the ruinously destructive Japanese occupation 1942–44), including as a self-governing commonwealth from 1935, until it was granted independence in 1946. From then until Ferdinand Marcos declared martial law in 1972, the 1935 Constitution applied. The 'People Power' revolution overthrew Marcos' dictatorship in 1986, and the Philippines then resumed a presidential style of democracy.[3] However, the 'revolution' is also described as 'a return to the oligopolistic rule of the landed families'.[4] President Corazon Aquino's main achievement, apart from surviving a series of coup attempts from the farcical to the bloody, was the peaceful democratic transition to her successor, Fidel Ramos. Despite the corruption of the next two succeeding presidents, and further failed coup attempts, more than a quarter of a century of uninterrupted democracy, with regular changes in which parties succeed in Presidential elections, has made democracy the norm in the Philippines. Thailand has not achieved this. Philippines democracy is seen by Case as essentially low quality despite its stability. The Philippines did not develop the strong bureaucratic elites of neighbouring Thailand, Malaysia, or Singapore. In the Philippines, government resources have been viewed not so much as tools with which to exercise power, but more as sources of patronage and plunder for political parties based on traditional landholding elites.[5]

Legal system of the Philippines

The Philippines 1987 Constitution[6] is based on the US Constitution, but creates a unitary state, not a federation. Legislation is passed by the bicameral Congress, and may be vetoed by the President, whose signature (plus subsequent publication) is required for Acts to come into force. Judicial power is vested in one Supreme Court which supervises all lower **(p.339)** courts. There are no regional high courts. The Supreme Court is also the Constitutional Court, with powers to determine the constitutionality of legislation, and certiorari powers expanded under the 1987 Constitution to review executive actions. The Philippines judiciary has a poor reputation in relation to corruption in surveys of Philippines lawyers, and was placed 6 of 12 Asian countries in an international survey.[7] An equally significant problem for enforcement of any laws are the lengthy backlogs in the Philippines courts, which tends to deter the less wealthy from pursuing cases to conclusion. Court officers state that 'protracted litigations are viewed as simply normal' and 'delay resulting from collective inefficiency seriously erodes public trust in the courts'.[8]

The Philippines legal system is to a significant extent influenced by a US common law approach. There is also still some influence in Philippines civil law from Spanish law: the Civil Code of Spain of 1889, extended to the Philippines in that year, was for a long period the local law.[9]

State surveillance context and social attitudes in the Philippines

The Philippines does not have a national ID system, and an attempt to create one by regulation was struck down as unconstitutional in 1998 (see section 2.2 of this chapter). However, its Unified Multi-Purpose ID (UMID), introduced in 2010, is the single identity card for four main government-related agencies,[10] with other uses such as during elections, being proposed. It is close to being a de facto national ID, because few Filipinos will be able to do without one. There are no significant legal controls on the UMID. It is not a chip-based card, and only carries limited identification data about the holder, plus a photo.

2.2. Other privacy protections

Separate from the Data Privacy Act, the Philippines has substantial potential protections for privacy, found under its constitution and treaty obligations, and in its novel (for Asia) development of the writ of habeas data, as well as various fragmented statutory protections.

Constitutional protections and the Civil Code

The 1987 Constitution includes various protections relevant to privacy including the general protection against being 'deprived of life, liberty, or property without due process of law'; 'against unreasonable searches and seizures of whatever nature and for any purpose'; against violations of 'privacy of communication and correspondence… except upon lawful order of the court, or when public safety or order requires otherwise, as prescribed by law'; and the right of access to official records.[11] These constitutional protections are supported by provisions in the Civil Code, articles 26 and 32 of which in effect create a right for individuals to take civil actions against the conduct of any person (not only government) that would be contrary to the constitutional rights relevant to privacy.

(p.340) A good example of the operation of these constitutional protections is that the Philippines Supreme Court in 1998 declared unconstitutional (upholding the petition of Senator Blas Ople) the national identification card which the government of former President Ramos had attempted to implement by a 1996 administrative order, ostensibly as a means to fight crime. The court held that the administrative order violated the constitutional right to privacy, and could not be implemented without a legislative basis.[12]

Treaty obligations

The Philippines has ratified the International Covenant on Civil and Political Rights 1966 (ICCPR), Article 17 of which requires privacy protections, and has also ratified (in 1989) the First Optional Protocol, allowing complaints ('communications') by their citizens to be made to the UN Human Rights Committee. Only one such communication has alleged a breach of Article 17, and it was found not to be substantiated.[13] The Philippines is also considered to be a monist state, regarding international legal obligations such as ICCPR Article 17 as part of its domestic law.

Writ of habeas data

The Supreme Court adopted in 2008 as a rule of court, a 'Rule on the Writ of Habeas Data',[14] which defines the writ as follows:[15]

> The writ of habeas data is a remedy available to any person whose right to privacy in life, liberty or security is violated or threatened by an unlawful act or omission of a public official or employee, or of a private individual or entity engaged in the gathering, collecting or storing of data or information regarding the person, family, home and correspondence of the aggrieved party.

While the writ is primarily aimed against government abuses of power in collecting and using personal information, it is also available against unlawful acts or omissions by a 'private individual or entity'. It should not be able to be used to force disclosure of media sources, because of the conflicting constitutional protection of freedom of the press. The relief requested under the writ 'may include the updating, rectification, suppression or destruction of the database or information or files kept by the respondent', as well as injunctions against threatened acts, and 'such other relevant reliefs as are just and equitable'.[16]

While there are many ways in which the writ of habeas data may overlap with the DP Act, it may often have significant procedural advantages. It must be issued immediately after a valid petition is filed, with a date for summary hearing within 10 days. The respondent has to file a verified response within five days of service (with specified contents). The court must render judgment within 10 days of the hearing, and thereafter a designated officer must enforce it within five days.[17]

(p.341) The writ of habeas data is of recent origin, having first appeared as a new right in the Brazilian constitution of 1988, and subsequently been adopted in numerous South American constitutions.[18] Its basis in Philippines law is considered to be the constitutional right of privacy of communications and correspondence, coupled with the Supreme Court's power to promulgate rules concerning the protection and enforcement of constitutional rights.[19]

There has started to be some use of the writ, with a petition for the issuance of a writ of habeas data against members of a constitutional body, the Commission on Elections (COMELEC), by a group of academics and activists called the Automated Election System Watch (AES Watch), who sought relief from being placed under surveillance by COMELEC, and disclosure of information already gathered about them.[20] In July 2013 the Supreme Court is reported to have granted the petition, issued the writ (which forces the respondents to reply to it), and referred the case to the Court of Appeals.[21] The petition was heard on 30 July 2013, the respondents did not appear, and the matter was re-scheduled.[22] At the time of writing, these proceedings are not known to have progressed.

Other legislation

The Electronic Commerce Act (2000) set a general principle that businesses operating online should give users choice in relation to privacy, confidentiality, and, where

appropriate, anonymity, but it and a set of government guidelines have had little effect. Numerous other statutes give other scattered and limited protection to privacy, including provisions of the Revised Criminal Code,[23] various anti-pornography laws, and various provisions of the Cybercrime Prevention Act of 2012 (although other provisions are considered to endanger privacy[24]).

A Freedom of Information bill has been before the Philippines legislature, unenacted, for some time. From a privacy perspective it is not very important, because the DP Act, once it is in force, will provide access and correction rights to government records.

2.3. Data Privacy Act 2012

A Data Privacy Bill influenced by the European Union (EU) Data Protection Directive with reasonably strong enforcement powers and a Commissioner had been before the **(p.342)** Philippines Congress since 2009.[25] The Joint Foreign Chambers of commerce and the business processing outsourcing (BPO) industry in the Philippines warned that lack of data privacy legislation concerned prospective investors and hindered development of the outsourcing sector.[26] In July 2011 the House of Representatives passed the Data Privacy Bill (HB 4115), with a number of strong principles. In September 2011 Senator Angara, chair of the Senate Committee on Science and Technology, introduced in the Senate a version of the Bill supported by the BPO industry, and the Senate passed it in March 2012.[27] A bicameral conference committee 'reconciled' the differing versions of the Bills before the two houses to produce the DP Act which was then enacted. It was signed into law by the President on 15 August 2012 but, as already noted, it is not yet effectively in force. The DP Act claims to be human rights legislation sensitive to commercial benefits: the stated policy is 'to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth'.[28] It is also to be interpreted liberally, 'in a manner mindful of the rights and interests' of data subjects.[29]

2.4. Scope of the DP Act

The starting point of the Act, different from any other Act in the ASEAN region, is that it is comprehensive, applying to 'the processing of all types of personal information and to any natural and juridical person involved in personal information processing'.[30] Both public and private sectors are covered, subject to specific exceptions.

Personal information, processing, controllers, and processors

The definition of 'personal information' is a conventional one, referring to information 'from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual'. It is unusual in specifying that it refers to information 'whether recorded in a material form or not'.[31]

'Processing' is defined as broadly as possible, as 'any set of operations performed on personal information', including both collection and such 'passive' operations as storage.[32] A 'personal information controller' (controller) is a person or entity that

controls processing or instructs another person to carry out processing.[33] The controller is 'responsible for ensuring that proper safeguards are in place to ensure the confidentiality of the personal information processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of this Act and other laws for processing of personal information'.[34] This appears to be a direct obligation on the controller to exercise something like due diligence and continuous supervision, rather than making the controller vicariously liable for the acts of the processor.

(p.343) The person or entity that carries out such instructions is not a controller, but is defined separately as a 'personal information processor' (processor).[35] Although such a controller/processor distinction is made, processors are required 'to comply with all the requirements of this Act and other applicable laws',[36] in contrast with jurisdictions like Hong Kong where only the 'data user' (controller) is subject to most obligations. Data subjects will therefore sometimes have the option of making complaints or taking other legal actions against either or both of controller and processor, and may be prudent to proceed against both until the meaning of the law is clarified.

Exceptions to the DP Act's scope.

The main exceptions to the scope of the Act are:

(i) Processing of information in connection with an individual's personal, family, or household affairs is exempted.[37]
(ii) Information about a person's position or functions as a government employee, and similar information about the performance of government contracts, and information 'relating to any discretionary benefit of a financial nature such as the granting of a [government] license or permit' is exempted.[38]
(iii) 'Personal information processed for journalistic, artistic, literary or research purposes',[39] is exempted, further underlined by section 5 entitled 'Protection Afforded to Journalists and Their Sources', and a proviso to section 4 requiring compliance with section 5. Freedom of speech, for these specified purposes, is therefore given comprehensive priority over data privacy rights by the Act, probably more so than in any other Asian country.
(iv) There is an exemption from the Part IV user rights where personal information is 'used only for the needs of scientific and statistical research and, on the basis of such, no activities are carried out and no decisions are taken regarding the data subject'.[40] The more general exemption of processing for the purposes of research should be given a narrow interpretation, or this section would be redundant.
(v) 'Information necessary in order to carry out the functions of public authority' is exempted,[41] as is processing for the purposes of investigation of criminal, administrative, or tax liabilities (but only from the Part IV user rights).[42]
(vi) Information necessary for banks to carry out obligations under various money-laundering laws is exempted.[43]

No government bodies or other entities have blanket exemptions from the Act. There is

no discretion provided for ministerial regulations, or the National Privacy Commission, to create new exceptions from the Act. In these respects the Philippines law is unusually comprehensive, and very different from the laws of its Malaysian and Singaporean neighbours.

Rights of the data subject survive death (or incapacity) and may be exercised by the data subject's heirs and assigns, a relatively unusual provision.[44]

(p.344) 2.5. Data privacy principles

The Act's data privacy principles are stated in relatively brief fashion in Chapter III 'Processing of Personal Information', Chapter IV 'Rights of the Data Subject', and Chapter V 'Security of Personal Information'. They can be summed up as including all of the 'minimum' or first generation principles, a significant number of 'European' or second generation principles, with the notable exception of data export limitations. In addition, the DP Act contains some innovative principles such as data breach notification, and a user right of portability of data. The Philippines DP Act takes the European approach of first imposing a set of obligations that apply to all aspects of processing, and then imposing additional obligations only relevant to specific aspects of processing.

General requirements for fair processing

All processing of personal data is subject to a general requirement of 'adherence to the principles of transparency, legitimate purpose and proportionality'.[45] The purpose of collection must be 'legitimate', and processing must be both 'lawful' and 'fair'.

Lawful processing requires the consent of the data subject, or that one of five exceptions be satisfied.[46] Lawful processing without consent may occur: for contractual fulfilment; where necessary to protect vitally important interests of the data subject; where necessary to respond to national emergencies, or for public order and safety; or 'to fulfil functions of public authority' which require such processing (a very broad exception); and finally:

> The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

Although this exception is not dissimilar to EU provisions,[47] it is impossible to know what it means in the Philippines context until the NPC and the courts interpret it. It is clearly intended as a justification for disclosures (as one aspect of processing).

Data collection, use, disclosure, quality, and deletion

The controller is required to 'ensure implementation' of the processing principles.[48]

The purpose of collection must be declared before or 'as soon as reasonably practicable' after collection. Collection is limited to data which is 'not excessive' in relation to purpose,

but the stronger 'European' approach of 'minimal' collection is not required. Data collection must be 'fair' but there is no specific prohibition on 'intrusive' collection. The collection principles are therefore relatively weak.

Subsequent use and disclosure (and other processing) must be for purposes 'compatible' with 'declared, specified and legitimate purposes'[49] and is also prohibited unless the data subject has given express or implied consent, or for various other usual exceptions.[50] There is also the ill-defined and potentially very broad exception where the processing is necessary for the legitimate interests of the controller or third parties to whom the data is **(p.345)** disclosed, except where those interests are overridden by the constitutional rights of the data subject. Requirements to give notice are not specified. Data quality is required in that data must be accurate, relevant, and up to date relative to purpose.[51]

The deletion and de-identification provisions are confusing and weak. Data must be retained only so long as needed for the purpose for which it was collected and processed, or in relation to legal claims, or 'for legitimate business purposes' (a broad and ill-defined exception) or as required by law.[52] However, it can only be 'kept in a form which permits identification' so long as needed for the purpose it was collected and processed (with uncertain exceptions for 'historical, statistical or scientific purposes'),[53] which is inconsistent with the deletion provision. In short, there is a requirement of deletion or de-identification with uncertain boundaries.

Special protection for sensitive and privileged information

In addition to the usual categories of sensitive information (information about 'race, ethnic origin,…color, and religious, philosophical or political affiliations', as well as health), the definition of 'sensitive personal information'[54] also includes marital status and age. It also includes 'education, genetic or sexual life of a person'. The inclusion of criminal record information is phrased broadly.[55] Businesses may find these Philippines requirements much stricter than elsewhere, and will need to take particular care when transferring personal information into and out of the Philippines. 'Privileged communications' (as constituted under Rules of Court and other laws),[56] are treated in essentially the same fashion as sensitive information. Other categories included as 'sensitive' in the Bills before enactment have been omitted from the Act.[57]

Processing of sensitive or privileged personal information is prohibited subject to very narrow exceptions, which will not normally allow commercial uses.[58] Six categories of exception allowing processing are specified, which can be summarized as follows (but some have complex provisos): specific data subject consent prior to processing; processing provided for by existing laws (only if they protect the information); necessary to protect the life or health of the data subject (or another person) who is not legally or physically able to consent; with consent of members of a public organization, necessary for its lawful and non-commercial activities; necessary for medical treatment; and necessary for court proceedings, or to establish or defend 'legal claims', or 'where provided to government or public authority'. This last exception seems like a broad and unrestricted loophole.

Data subject rights

The data subject's notification rights prior to processing have already been discussed. The right of access[59] is broadly stated and is specific in requiring disclosure of 'name and address of recipients' (which would involve disclosing whether they are overseas). It also includes information on 'automated processes where the data will or likely to be made as **(p.346)** the sole basis for any decision significantly affecting or will affect the data subject'. This partially implements an EU Directive principle not found in the 'minimum' standards. However, the Act says nothing about charges for access beyond the requirement of 'reasonable access'. This practical issue should have been addressed.

The correction provision requires 'immediate' corrections, but also that the (incomplete, out-of-date, or false) information prior to correction will continue to be provided to any recipients.[60] Inconsistently, data subjects can require blocking or deletion of data which is incomplete, out of date or false, or which has been unlawfully obtained or unlawfully used, or which is no longer necessary for the purpose for which it was collected.[61] In relation to corrected information, it is not clear which principle will prevail. Adding confusion, the data subject decides which previous recipients should be informed about corrections, but the controller decides who should be informed about blocking.

The data subject has a novel 'right to data portability', a right still only under discussion in the EU's consideration of a new Regulation:[62]

> The data subject shall have the right, where personal information is processed by electronic means and in a structured and commonly used format, to obtain from the personal information controller a copy of data undergoing processing in an electronic or structured format, which is commonly used and allows for further use by the data subject. The Commission may specify the electronic format referred to above, as well as the technical standards, modalities and procedures for their transfer.

Here, an Asian jurisdiction is leading in development of a 'third generation' data privacy principle.

The data subject is entitled to be 'indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information'.[63] This supports the brief reference to 'award indemnity' in the functions of the NPC, and does not relate solely to correction or blocking, but nor is it broad enough to amount to a right to be indemnified for the breach of any privacy principle that may cause damage.

Security and data breach notification

The controller must implement reasonable security safeguards,[64] and Chapter V gives considerable detail of what these must contain, including regular monitoring for breaches and a requirement to ensure that contracted processors implement the level of security standards required. Further requirements on security of sensitive personal information

by government agencies are in Chapter VII, and contractors processing such information concerning more than 1,000 persons must comply and register with the NPC.[65]

A controller must 'promptly notify the Commission and affected data subjects' of a data breach[66] (when personal information is 'reasonably believed to have been acquired by an unauthorized person') if:

> (i) the information is either 'sensitive personal information' or 'other information that may, under the circumstances, be used to enable identity fraud'; and
> **(p.347)** (ii) 'the personal information controller or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject'.

However, the NPC can exempt a controller from notifying data subjects on the very general grounds that 'such notification would not be in the public interest or in the interests of the affected data subjects'. It can also authorize postponement where criminal investigations may be hindered.

2.6. International data flows, and processor contracts

As explained in Chapter 3, section 3.3, interlocking issues must be considered in relation to international data flows.

Extraterritorial application

The Act has extraterritorial application to 'personal information controllers and processors…not found or established in the Philippines' but is ambiguous concerning its scope. It will apply to those foreign companies 'who use equipment located in the Philippines',[67] such as a company that hires processing facilities in the Philippines but controls all aspect of the processing itself. Such a company will be a 'controller' subject to the Act, despite it not being established in the Philippines.

The extraterritorial operation will also apply to an entity that, although not 'established' in the Philippines, does 'maintain an office, branch or agency in the Philippines subject to the immediately succeeding paragraph'.[68] Because of the insertion of a new section 5, it is now section 6 that deals with extraterritoriality, so this must be the paragraph to which section 4 refers. Section 6 sets out three requirements for the extraterritorial operation of the Act:

> (a) it is limited to personal information 'about a Philippine citizen or resident'; and
> (b) the entity 'has a link with the Philippines' including a contract entered into in the Philippines, or a business not incorporated in the Philippines but with its central management there, or where overseas parents or affiliate of a Philippines business entities have 'access to personal information' (presumably about Filipinos); and
> (c) the entity 'has other links in the Philippines' (including carrying on business in the Philippines, or the personal information was collected in the Philippines).

These sections are drafted in such a confusing way that all that can be said is that foreign processing of personal information 'about a Philippine citizen or resident' with more than one link of any type to the Philippines could potentially come under the Act. So the Act purports to have (at least in theory) broad but unclear application to information about Filipinos which is processed overseas.

Data export limitations—'accountability' by controllers

There are no express data export limitations to foreign countries, but instead an 'accountability' principle operates. In addition to the general obligation on controllers to 'ensure implementation' of the processing principles, the notion of 'accountability' in the **(p.348)** minimum privacy principles, a specific 'principle of accountability' has been added.[69] It states that the data controller is 'responsible' and 'accountable' for compliance with the Act, including for when data is disclosed to third parties 'whether domestically or internationally'. The controller must use 'contractual or other reasonable means to provide a comparable level of protection', but whether this means that the controller still has legal liability for any breaches of this protection by a processor, or by the third party, remains uncertain but unlikely. The doctrine of privity of contract in Philippines law also means that any contractual protections will not be enforceable by the data subject. If controllers do not at least have vicarious liability for outsourced processors, their 'accountability' will usually be worthless to data subjects. Because the DP Act does not include any restrictions on data exports, this provision is intended as a substitute, but it is difficult to see that it is one of any value to data subjects.

Exempting (some) outsourcing—Pyrrhic victory?

There is a complete exemption in the Act (not found in the House Bill) for '[p]ersonal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines'.[70] The intention is clearly that outsourced processing in the Philippines of data collected overseas is exempt, so as to 'protect' the Philippines BPO industry. This might make it easier for Philippines companies to obtain outsourcing contracts from the USA or from other countries which do not have any significant restrictions on data exports, because the personal data will not come within the ambit of the Philippines law. Also, neither foreign data controller nor Philippines processor will have to bear compliance costs or be at risk of actions for breach.

However, this exemption would seem to make it impossible for the Philippines to be considered by the EU to provide 'adequate' data protection, since the main purpose of adequacy findings concerns the protection given to data about Europeans. This provision means that Philippines companies are not required even to provide data security protections, or protections against further use and disclosure. EU-based data controllers and their Philippines processors (BPOs) will have to continue to rely on contractual clauses or binding corporate rules (BCRs) to legitimate data exports from EU member states. For companies in both EU countries and any other countries that have data export restrictions, outsourcing to the Philippines will remain cumbersome.

An additional question is whether Philippines companies operating call centres for overseas companies can utilize this exemption? They collect information directly from 'residents of foreign jurisdictions', so it seems they can only utilize the exemption if they collect the personal data 'in accordance with the laws of those foreign jurisdictions'. Otherwise, they will have to comply with the Philippines law. How is a Philippines call centre staffer to know how to apply the data collection rules in Australian, UK, USA, or South Korean law?

2.7. The National Privacy Commission

The National Privacy Commission (NPC) is created by Chapter II, providing for a Commissioner and two Deputies to be appointed by the President for a three-year term, and **(p.349)** eligible for reappointment for one term. They will have the ranks of Secretary and Undersecretaries, respectively. All must be experts in IT and data privacy. The NPC is attached to the Department of Information and Communications Technology (DICT), or the office of the President if the DICT has not been established.[71] DICT has not yet been established, and the President is reported to be insistent that it is not necessary.[72] NPC is authorized to establish a secretariat. The NPC is stated to be 'independent',[73] and there are no provisions allowing ministers to give it directions, although nothing is specified concerning removal of Commissioners from office, or provision of a budget. The extent of its actual independence will need to be assessed in practice.

The NPC is given a wide range of functions.[74] Those of ensuring compliance, and dealing with complaints, are discussed in section 2.8 of this chapter. It can give advisory opinions on the meaning of this or other Acts, can comment on proposed legislation, and can propose legislation.[75] It is supposed to provide a compilation of government agency record systems,[76] but is unlikely to do so unless it is given considerable resources. The NPC can also approve (or reject) voluntary privacy codes, which can include private dispute resolution mechanisms.[77] The consequences of such approval on the operation of the Act are not specified, so this provision seems incomplete and ill-considered.

The NPC can coordinate with overseas privacy regulators and 'private accountability agents' and participate in international and regional privacy initiatives.[78] This will clearly allow it to participate in the Global Privacy Enforcement Network (GPEN) and the Asia-Pacific Economic Cooperation (APEC) Cross-border Privacy Enforcement Arrangement (CPEA) (see Chapter 2, section 6). It may allow it to facilitate cooperation in the APEC Cross-Border Privacy Rules (CBPR) processes, because the Philippines has no significant restrictions on data exports, if the Philippines decides to join the APEC CBPR.

2.8. Enforcement provisions

The Act has a considerable range of enforcement mechanisms, but they are generally marred by confusing drafting, apparent gaps, and lack of procedural detail. Failure to comply with any of the principles could result in a complaint investigation by the NPC, but only a specific subset of breaches will result in prosecutions under Chapter VII 'Penalties'.

Enforcement by the NPC, following complaints

The NPC has a general function of 'ensuring compliance' by controllers with the Act (processors are not mentioned).[79] In relation to complaints, it has broad functions:[80]

> Receive complaints, institute investigations, facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matters affecting any personal information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicize any such report…

(p.350) The NPC can 'institute investigations', presumably equivalent to 'own motion' powers of investigation in other jurisdictions. Its enforcement powers (including awarding 'indemnity') seem to be able to be exercised in relation to both complaints it receives and to own motion investigations. The broad power to carry out 'investigations' presumably also provides scope for some type of collective or class complaints to be made. However, the brief above statement is all that the Act has to say on these matters, so this remains uncertain until the IRRs add more detail and are put into practice.

The NPC can 'compel…any entity, government agency or instrumentality to abide by its orders or take action on a matter affecting data privacy'.[81] The function of awarding indemnity (compensation) is not backed up with any provisions to enforce such awards, other than this general power to compel compliance with its orders. Other than this vague provision, there is no specific reference to the award of remedies other than indemnity. The explicit power to publicize its reports on complaints is valuable, and an important sanction in itself, if well used.

The NPC can also ban processing (temporarily or permanently) that it considers 'detrimental to national security and public interest'.[82] It is odd that there is no mention of a significant effect on the privacy interests of the data subject, so how the NPC is supposed to take that interest into account is not clear.

Offences where the NPC can recommend prosecution

The NPC cannot issue administrative penalties or fines. Instead, it can recommend to the Department of Justice (DOJ) the prosecution and imposition of penalties specified in sections 25 to 29.[83] There is no general offence resulting from any breaches of the privacy principles set out in Chapters III–VII, only the following specific offences, some of which apply to third parties, not only to data controllers. The penalties for offences (i)–(iv) are higher if the data is sensitive personal information:[84]

> (i) 'unauthorised processing of personal information' ('without the consent of the data subject, or without being authorized under this Act or any existing law');
> (ii) both accessing personal information and providing unauthorized access to personal information, in either case 'due to negligence';
> (iii) 'improper disposal of personal information', which means wrongly leaving personal information 'in an area accessible to the public' or in a 'container for trash collection';

(iv) processing of personal information for purposes, which are not authorized by the data subject, nor otherwise authorized under this Act, nor or under existing laws;
(v) 'knowingly and unlawfully…break[ing] in any way into any system' storing personal information.

The most general offences are 'processing of personal information for unauthorised purposes' and 'unauthorised processing of personal information' (which addresses the means of processing, not the purpose), one or other of which will cover breaches of many of the privacy principles. However, some breaches such as refusals to effectuate user rights (Chapter IV), failure of security systems (Chapters V and VII), or accountability for transfers (Chapter VI), may be difficult to fit within these offences. The effectiveness of some offences may be further reduced by what appears to be careless drafting.

(p.351) Other offences where the NPC has no role

Further offences are specified in sections 30 to 32, but the NPC has no role in recommending prosecution. There is no apparent reason for the distinction between the two sets of offences: both include offences which can be committed by personal information controllers and processors, and only the first includes offences which can be committed by third parties. The NPCs role should logically include the offences in sections 30 to 32. These other offences cover:[85]

(i) where a controller knowingly fails to inform the NPC of a security breach, where there is an obligation to do so under section 20(f);
(ii) where a controller or processor 'with malice or in bad faith, discloses unwarranted or false information';
(iii) where a controller or processor or their employees or agents 'discloses to the third party personal information…without the consent of the data subject' (with no exception provided for other justifiable reasons for disclosure).

This last offence seems over-broad due to faulty drafting.

Penalties and personal liability of company officials

Penalties for offences under sections 25–32 can include fines ranging from 100,000 pesos (US$2,278) to two million pesos (US$45,500), and imprisonment for up to five years. Maximum penalties are required to be imposed where the personal information of more than 100 persons is affected.[86] Where the 'responsible officers' of a company or partnership or juridical person (such as an agency) have 'participated in, or by their gross negligence, allowed commission of a crime', the penalties for offences 'shall be imposed' upon them.[87] Public officials also face disqualification from office.[88]

Civil actions following offences

Actions for damages ('restitution') may also be possible via the courts in an action under the New Civil Code, but the Act only provides for this when an offence has been proven.[89] In some Asian jurisdictions (e.g. Hong Kong), a data subject can commence a civil action because of a breach of any privacy principle, without a prior criminal

prosecution having occurred. The Hong Kong approach is preferable, because few if any plaintiffs will be able to commence actions under the Philippines approach. As matters stand, in the absence of a prior successful prosecution, a data subject would have to rely upon a breach of a privacy principle also being regarded as a breach of the Civil Code, articles 26 and 32 (see section 2.2 of this chapter).

Systemic enforcement measures largely lacking

The Act provides no details of systemic enforcement measures, but does give the NPC functions in the public sector of 'monitoring' compliance by government agencies (but **(p.352)** without powers of inspection or audit), and publication of a 'compilation of agency systems'.[90] These are unlikely to occur unless the NPC is given significant resources.

Privatized enforcement via codes?

The NPC can 'approve, reject or require modification of privacy codes voluntarily adhered to' by private sector bodies, which 'may include private dispute resolution mechanisms', provided such codes 'adhere to the underlying data privacy principles embodies in the Act'.[91] The relationship between such codes, once approved, and a company's obligations under the Act, are unstated. So is whether data subjects can be forced to accept such private dispute resolution, which is not likely to include equivalents to statutory remedies. This provision is so vague that it risks Filipinos losing their statutory rights.

2.9. Conclusions—an ambitious, ambiguous, and unimplemented Act

This Act creates a potentially credible data protection authority (once it is appointed and has a budget), and range of enforcement mechanisms of uncertain effectiveness. But the delay of more than 18 months in bringing the Act into effect raises suspicions that it has been enacted as 'window dressing', for foreign trade-related consumption, rather than having much to do with improving the human rights of Filipinos. Until it is in force, and actively enforced, it remains a legitimate suspicion that this legislation is merely public relations for the Philippines data processing outsourcing industry, and is not intended to be implemented seriously (a distinction shared with India's current law). Interpretation of both privacy principles and enforcement provisions, and the appointment of a sufficiently well-resourced National Privacy Commission, will be crucial to whether this law is effective. The Act is unlikely to come into effective force until 2015, so there is both time, and need, for the Philippines legislature to amend it to add some clarity.

Vague principles, with potential strengths

The principles in the Act generally implement OECD standards, but often in a weak fashion, such as the very ambiguous restrictions on use and disclosure, and the bizarre interpretation of 'correction'. The Act's principles add some additional 'European' standards such as deletion rights and protection of sensitive information, but lack 'border control' data export restrictions. They add the post-Directive requirement of data breach notification and personal data portability. The 'accountability' provisions may be strong or weak, the outsourcing exemptions broad or narrow.

Largely reactive enforcement measures

It is difficult to predict how effective this enforcement regime will be prior to its implementation. On its face, it has many of the desired features of a system of responsive regulation, with a variety of forms and instigators of enforcement measures—remedies from the NPC following complaint investigation, prosecution for offences, and civil actions in the courts by data subjects—but all of these enforcement provisions have ambiguities **(p.353)** and deficiencies. Weak systemic enforcement measures and dangerously vague provisions for codes also detract.

3. Thailand—defective public sector law, private sector Bill

Thailand is an unstable democracy, where periodic (and usually peaceful) military coups give way to the reintroduction of democratic institutions, but usually only for a few years at a time. In the last decade this cycle has interrupted and slowed down the development of data privacy laws. An incomplete public sector law has existed for nearly 15 years, and a series of government Bills for a private sector law have been under development for as long, with one finally introduced into the legislature in 2013. Little privacy protection has been provided in the interim.

3.1. Thailand—contexts

History and politics

Unlike most other Asian countries, Thailand was never colonized. European colonialism was not significant in mainland southeast Asia until the nineteenth century (unlike in its island regions). Under colonial pressure, the Thai empire lost much of its territorial acquisitions in Cambodia, Laos, and the Malay States, but an 1896 treaty involving Britain and France guaranteed the independence of most of the territory today comprising Thailand. The county remained an absolute monarchy until 1932 when a military/bureaucratic coup forced the King to accept the status of a constitutional monarch. Professed intentions to introduce democracy came to nothing, and a semi-appointed legislature was little more than a cover for military rule, throughout World War II (where Japanese occupation was avoided) and up to the Vietnam War (where Thailand hosted US bases and provided troops). Post-World War II US aid and investment assisted economic progress. A 'student's revolution' in 1973 led to a short-lived fully elected parliament and democratic government in 1975–76. This was followed by a period of the so-called 'semi-democracy' in which a primarily elected government and legislature were run under an appointed Prime Minister, usually a military general. Semi-democracy gave way to a fully civilian government under Chatichai Choonhavan in 1990, but it was short-lived, toppled by another military coup in 1991. Massive repression of student and other protesters by the military government in 1992 prompted the King to intervene and a negotiated return to democracy. Elected governments ruled until 2006 when another coup (allegedly supported by some business groups and the monarchy) removed the government of business tycoon Thaksin Shinawatra (elected in 2001 and re-elected in 2005). New elections a year later returned another pro-Thaksin party as government, until the Constitutional Court (where pro-Thaksin judges had been removed) destroyed the government by declaring the party illegal.[92] The end of this second 14 years of democratic government showed how fragile such institutions still were in Thailand. From

2006–11 governments alternated between pro- and anti-Thaksin coalitions, with further anti-Thaksin interventions by the Constitutional Court, until further elections in 2011 returned a government headed by Thaksin's sister, Yingluck Shinawatra. Since then, constant extra-Parliamentary protests, **(p.354)** blockages in Bangkok, an opposition boycott of 2014 elections (as in 2006, because the opposition believed it would lose the election), and Constitutional Court invalidation of the election result, has resulted in a stalemate. Thai politics has therefore failed to achieve acceptance of democratic institutions by 2014, and the cycle of coups involving the military, business groups, the courts, and the monarchy may continue. As Pike summarizes, there appears to be 'an insoluble split in the country between [the anti-Thaksin parties] supported by the largely urban establishment and military-backed elite, which has traditionally enjoyed the spoils of office, and the rurally supported [Thaksin-aligned parties]'.[93] Passage of a data privacy law has been one of the casualties of this paralysis.

Despite this political instability, Thailand's economic growth remained very strong for four decades, at between 5 and 10 per cent depending on the year (except for 1998–99 negative growth), but has slowed considerably to around 3 per cent in various years from 2008 to 2013. Despite both political chaos and a slower economy, Thailand in 2013 was moving closer towards development of a data privacy law in the private sector, although not in the public sector.

Legal system of Thailand

Thailand is 'a civil law country with strong common law influences'.[94] A constitutional monarchy since 1932, it has had 18 constitutions, most recently that of 2007. Legislation is by a bicameral National Assembly consisting of a House of Representatives and Senate. It is a parliamentary system, with the Prime Minister a member of the House of Representatives and holding a parliamentary majority, but limited to an eight-year term.[95]

The Constitution provides for four types of courts: the Constitutional Court; the Courts of Justice (with the Supreme Court at the apex); the Administrative Courts; and the Military Courts. The nine-member Constitutional Court comprises three judges elected by the Supreme Court, two elected by the Administrative Court, plus two legal experts and two social science experts chosen by a special panel and approved by the Senate. The court can declare provisions of any law or regulation to be unconstitutional. Decisions of higher courts are not binding on lower courts, but decisions of the Supreme Court are considered to be highly influential on lower courts and on the Supreme Court itself.[96]

State surveillance in Thailand

It has been asserted that 'Thailand has always been a surveillance state. From the ancient to the modern period, extensive collection of people's personal information has been a long-standing practice.'[97] Before the nineteenth century labour controls involved registration and tattooing of subjects to indicate residence and administrative superiors.[98] Current surveillance practices are documented by Ramasoota and Panichpapibul, and by Privacy International.[99] From 2005, Thailand has replaced its

existing ID card with a chip-based **(p.355)** card linked to a registration database, containing a photo, fingerprints, and iris scan, and with a great deal of additional data on the chip.[100]

Public opinion and civil society in Thailand

Ramasoota and Panichpapibul find that 'there is a dearth of advocacy and works in the Thai civil society when it comes to privacy', with the civil society focus being more on freedom of expression and right to information issues.[101] Their extensive 2012 attitudinal survey of 800 Thai internet users found that:[102]

> the studied population is found to rate their privacy perception high in off-line contexts, such as polling booth privacy, police intrusion, and physical notion of privacy (the right to be let alone). Meanwhile, they rate their perception about privacy at a medium level with regard to surveillance cameras in the workplace, wiretapping for police investigation and quality assurance of services. Lastly, they rate their perception of privacy issues in the following contexts at a low level: consumer database and corporate data sharing, state surveillance such as citizen ID card and job screening through criminal record checks.

The same study also found that:[103]

> in an online context respondents perceive that these Internet applications, in ranking order, are most prone to privacy violation: social networking applications such as Hi5 and Facebook, email, online media, search engines and electronic commerce websites. Moreover, the survey finds that more than half of the surveyed population (58.3 per cent) feels that public participation is needed in order to accomplish personal data protection advocacy, while 25 per cent of respondents indicate that the state should be a main mechanism in personal data policy formulation. Only 16.8 per cent of respondents believe that current personal data protection in the private sector is already sufficient and no more personal data protection is required.

The high percentage of people who considered that social activism is necessary to achieve privacy protection is surprising, as is high concern about criminal record checks for employment. However, while varying in such details, these results do not seem surprising for internet users in an economically advanced country, and do not indicate a low level of privacy concern or awareness.

3.2. Existing privacy protections

Thailand has some potentially significant (but under-explored) constitutional rights, but no obligations under international agreements that can be used to protect privacy.

Constitutional protections

The Constitution of Thailand 2007[104] provides a number of rights relevant to privacy protection: a general protection of 'the rights and liberty in his life and person'; a right of **(p.356)** peaceful habitation in a dwelling, including against warrantless searches; 'family

rights, dignity, reputation and the right of privacy'; 'the liberty of communication by lawful means' (including protection against disclosures); and the right to obtain public information from state agencies (except personal data of others).[105] The general protection of privacy by section 35 is elaborated in two sub-clauses, both of which are potentially broad as privacy protections, and neither of which is clear in its meaning:

> (i) 'The assertion or circulation of a statement or picture in any manner whatsoever to the public, which violates or affects a person's family rights, dignity, reputation or the right of privacy, shall not be made except for the case which is beneficial to the public.'
> (ii) 'Personal data of a person shall be protected from the seeking of unlawful benefit as provided by the law.'

Violation of a person's Constitutional rights creates an explicit right to invoke them as a defence, or 'to bring a lawsuit', but it is implied that such actions can only be brought against the state.[106]

Treaty obligations

Thailand is a party to the International Covenant on Civil and Political Rights 1966 (ICCPR), Article 17 of which requires privacy protection. It has not adopted the First Optional Protocol, so Thai citizens cannot complain of breaches of Article 17 to the UN Human Rights Committee. Since Thailand is not a monist state, Article 17 is not part of Thai domestic law.[107] Thailand is a member of APEC (but not yet a party to APEC's CBPR scheme), and of ASEAN (and thus to the ASEAN Human Rights Declaration). It has been a member of the World Trade Organization (WTO) since 1995.

Other statutory provisions

There are scattered statutory protections of privacy in the 'Credit Information Business Act 2002, the National Health Act 2007, the Statistics Act 2007 and the Broadcasting and Television Business Operations Act 2008',[108] and in the Civil Code, Penal Code, Telecommunications Act 2001, and Computer-related Offences Act 2007.[109]

3.3. Public sector—Official Information Act 1997

Thailand's Official Information Act 1997[110] has been described as a 'historic law, the first of its kind in Southeast Asia'[111] in relation to its primary role as a freedom of information (right to information) Act. It was largely the result of civil society pressure.[112] It also **(p.357)** provides some basic but incomplete data protection in relation to government agencies, including principles concerning limits on personal data collection and its retention, limits on disclosures, and security, as well as providing access and correction rights. However, only the access and correction rights are enforceable, so the Act does not qualify as a data privacy law for the public sector.

Official Information Board and Information Disclosure Tribunal

The Act sets up an Official Information Board (OIB) of 24 persons (15 senior officials and nine qualified persons appointed by the Council of Ministers)[113] chaired by a minister designated by the Prime Minister, and a secretariat which serves it. Members are

appointed to the OIB for three years, can be re-appointed, and can only be removed for specified good cause. The Board or its members do not have any specific duty to act independently. With nearly three-quarters of its members being appointed government officials, it could not be regarded as independent of government, despite having some of the trappings of independence. The Information Disclosure Tribunal (IDT) is also appointed by the Council of Ministers, and has four divisions. The OIB and IDT have published a handful of their decisions.[114]

From 1999–2005 there had been 880 appeals from agencies to the OIC or the Information Disclosure Tribunal, from 1,300 complaints against government at all levels.[115] From January to September 2013 there were 354 complaints and 136 appeals.[116] Evidence of the effectiveness of the law in relation to privacy issues is not readily accessible, partly because the available statistics do not distinguish between complaints concerning access and correction and other complaints. However, it seems that up to 2005, the number of complaints concerning privacy issues (other than access and correction) was insignificant.[117]

Access and correction rights

Individuals have the right to obtain personal information concerning themselves from agencies, subject to some exceptions.[118] Medical reports may be disclosed only to doctors entrusted by the data subject. As in other freedom of information Acts, agencies may refuse to disclose any information on the grounds that disclosure would 'unreasonably encroach on the right so privacy' of another person.[119] Data subjects have a right to request correction or deletion of incorrect personal information, and if an agency refuses they have a right of appeal to the Information Disclosure Tribunal. Irrespective of appeal result, the data subject can have their request attached to the contested information.[120]

Data privacy principles—but unenforceable

Although the other data privacy principles in Chapter III 'Personal Information' are not enforceable, they indicate the types of principles the Thai government has been willing to **(p.358)** enact. Their main elements are that state agencies are 'required to take the following actions with regard to provision of a personal information system':[121]

> (i) only provide such systems to the extent necessary for achievement of agency operations, and terminate such systems when they become unnecessary;
> (ii) aim to collect personal information directly from the data subject, particularly where the person's interest will be directly affected;
> (iii) publish information about personal information systems (similar to the OECD 'Openess' principle);
> (iv) provide appropriate security systems;
> (v) where information is directly collected from the data subject, provide notice before or upon collection of the purpose of collection, normal uses, compulsory powers, etc.;
> (vi) not disclose personal information 'to other State agencies or other persons,

> without prior or immediate consent given in writing' by the data subject, except under nine specified exceptional circumstances, and maintain a log of disclosures except for where disclosures are within the purposes of its own agency, or the information system.

While these provisions (in combination with access and correction rights) do constitute a set of 'basic' or first generation data privacy rights, if the Board receives complaints alleging agency failure to comply with any of these requirements, all it is empowered to do is to 'give advice' to the agency concerning the implementation of the Act.[122] It cannot enforce its recommendations. There is also no explicit power for the Board to receive and investigate complaints about such matters, whereas there is in relation to access and correction issues, but it is implied that individuals have a right to complain.[123] The Act therefore seems to provide an 'ombudsman' approach to enforcement of data privacy rights, but that is all, and it needs amendment to provide proper enforceability.

3.4. Private sector—a decade of unenacted draft Bills

For nearly a decade, various officially drafted Bills have included coverage of the private sector, and a data protection authority, but none have yet become law, partly due to the political turmoil in Thailand. From 1998, the National Information Technology Committee (NICT) of the Ministry of Science, Technology and Environment worked on six information and communications technology (ICT) laws, one concerning data protection. Accommodation of the standards of the EU's Data Protection Directive was one of objectives from that early stage.[124]

Significant progress on a draft law started in 2005, under the new Ministry of Information and Communications Technology (MICT).[125] In 2006 the Council of State put forward the MICT's Data Protection Bill, which was apparently EU-influenced.[126] Another version of a law to cover the private sector was submitted by the Official Information Commission (OIC) to Cabinet. It proposed that the OIC become the central administrative **(p.359)** agency for privacy issues.[127] The two Bills appear otherwise similar in many respects, from the brief details published: both would establish a data protection authority; private sector organizations would be required to have a 'registrar' or data protection officer responsible for security; and would report annually to the authority; no processing of personal data without consent would be allowed; change of use, or disclosure, or overseas transfers would require written consent, with very limited exceptions; notification of the data subject would be required after overseas transfer; and enforcement would be primarily through criminal offences. The main difference was that the MICT draft proposed that the DP Act would be an independent regulatory agency situated outside the bureaucracy, whereas the OIC draft proposed a DP Act that was essentially an expansion of the existing OIC.[128] Progress on both Bills was halted by the 2006 coup.

In 2009, during the government led by the Democrat party, two further Bills were proposed to Parliament, one based on the MICT Bill from the Thaksin administration, the other submitted by Democrat Party legislators. In 2011 a Personal Data Protection Bill

including a DP Act, a registration system, and a certification scheme,[129] was approved by the previous Democrat party government. Ramasoota and Panichpapibul provide a detailed analysis[130] of these 2009 Bills, which were in most respects similar. The main aspects they identify are:

(i) A Personal Data Protection Commission (PDPC) of a dozen or more persons, comprising public and private sector representatives, and individual experts. The PDPC was not based on the existing OIC, but the Office of the OIC would be the secretariat for the PDPC.
(ii) The PDPC and OIC would create what appears to be a register of 'personal data controllers', and a 'Data Protection Mark' for controllers complying with standards.
(iii) The law would exclude public sector bodies that come under the OIC, and use for the purposes of mass communication, art, literature, and also personal use.
(iv) Rights of data subjects would be enforced through complaints to 'inspection sub-committees' of the PDPC.
(v) Written consent was emphasized as the basis of uses and disclosures.
(vi) Administrative fines and criminal offences would be the main means of enforcement.

Civil society critics of the 2009 proposed laws identified weaknesses such as the lack of any capacity for actions against misuse of personal information by government; dominance of the PDPC by government representatives; the exceptions from consent requirements being too broad; and the proposed law not being reconciled with other more restrictive surveillance laws.[131]

Personal Data Protection Bill 2013 before Parliament

In 2012 the new Cabinet of Prime Minister Yingluck Shinawatra used the 2009 draft Bill as one basis for development of yet another Bill, that it submitted to the Coordinating Committee of the Parliament, for preparation for submission to the House of **(p.360)** Representatives, and then the Senate.[132] This required commissioners to be appointed to organize the reading of the draft.[133] This Bill for the Personal Data Protection Act was introduced into Parliament on 30 October 2013 passed its first reading and was submitted to a scrutiny committee ('Ad Hoc Committee') which was working on the review. Commissioners had been appointed for the tabling of the draft law. At the end of 2013 the committee was still reviewing the definitions, at which point Thai politics became chaotic and progress ceased.

The main features of this Bill are, as far as is known, similar to what was reported in 2012:[134]

(i) Consent is central, with new consents being required for changes of use or disclosure.
(ii) International transfers of personal data to countries with less stringent data protection laws are prohibited.

(iii) It is not clear whether the law would apply to processors or only to data controllers.
(iv) Civil, criminal, and administrative penalties apply, with some vicarious personal liabilty for company officials.
(v) A Committee on Data Protection would establish policies and standards, and set up a Personal Data Inspection Board to deal with disputes.
(vi) The law would only apply to the private sector, leaving the public sector under the Official Information Act. Other exceptions cover the media, literary, and personal purposes.

This is essentially the same as the Bill being considered in 2012, discussed earlier.[135] It is not expected to have a rapid passage. The dissolution of Parliament for the 2014 elections, further complicated by the Constitutional Court's decision that the elections were unconstitutional, is likely to mean that the legislative process will have to start again.

3.5. Conclusion—democratic comprehensiveness or not?

If a Bill similar to the reported Shinawatra Cabinet Bill of 2012 is eventually enacted, it might be closer to the Singaporean or Malaysian law than that of the Philippines, particularly since it would cover only the private sector, leaving the public sector with the partial, defective protection and unenforceable protections provided by the Official Information Act. It is very significant for the future of data privacy in Asia whether Thailand opts for a law similar to those of the Philippines, and the North east Asian jurisdictions of South Korea, Japan, Taiwan, Hong Kong, and Macau, by enacting a comprehensive law which applies to both public and private sectors. Alternatively, the Official Information Act could also be reformed. If Thailand took either path to comprehensive data privacy legislation, it would also be strengthening its democratic institutions, and giving encouragement for similar development in Indonesia and other ASEAN countries.

Notes:

([1]) DP Act (Philippines), s. 45.

([2]) DP Act (Philippines), s. 42.

([3]) See for sources of this summary, Elizabeth Aguiling-Pangalangan, ch. 11 'The Philippines: Native Culture, Transplanted Institutions and Women's Rights' in E. Ann Black and Gary F. Bell (Eds.), *Law and Legal Institutions of Asia* (Cambridge, 2011), pp. 374–6. For accounts of Philippines history and politics, see 'The Philippines' in Peter Church et al., *A Short History of South-East Asia* (5th Edn., Wiley, 2009), pp. 122–39, William Case, ch. 6 'The Philippines: Stable, but Low Quality Democracy' in *Politics in Southeast Asia—Democracy or Less?* (Curzon, 2002), and Francis Pike, *Empires at War: A Short History of Modern Asia Since World War II* (I B Tauris, 2011), chs. 12, 19, and 49, and p. 716.

([4]) Pike, *Empires at War*, p. 577.

([5]) Case, *Politics in Southeast Asia*, pp. 203–5.

([6]) Constitution of the Republic of the Philippines (1987) (Official Gazette) <http://www.gov.ph/the-philippine-constitutions/the-1987-constitution-of-the-republic-of-the-philippines/>.

([7]) Aguiling-Pangalangan, ch. 11 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, pp. 392–3.

([8]) J. Martin and S. Villarama, Jr, 'Culture of delay' (Philippines Court of Appeals, undated) <http://ca.judiciary.gov.ph/index.php?action=mnuactual_contents&ap=j6040>.

([9]) Aguiling-Pangalangan, ch. 11 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, pp. 373–4.

([10]) The Social Security System (SSS), and also Government Service Insurance System (GSIS), Philippine Health Insurance Corporation (PhilHealth), and the Pag-IBIG Fund (Home Development Mutual Fund).

([11]) Constitution of the Republic of the Philippines (1987), art. III Bill of Rights, ss. 1, 2, 3, and 7, respectively.

([12]) Graham Greenleaf and Nigel Waters, 'Philippines Supreme Court Cans ID Card' (1998) 5 *Privacy Law & Policy Reporter*, p. 80 <http://www.austlii.edu.au/au/journals/PLPR/1998/66.html>; Privacy International *Privacy and Human Rights 2006*, 'Identity systems' <http://gilc.org/privacy/survey/intro.html>.

([13]) UN Human Rights Committee, 'Communication No. 1560/2007' (UNHRC, 30 October 2008).

([14]) Resolution, 'The Rule on the Writ of Habeas Data' (Supreme Court of the Philippines, 22 January 2008) <http://www.chanrobles.com/writofhabeasdata.html#.UpG-II39qG0>.

([15]) Rule on the Writ of Habeas Data, s. 1.

([16]) Rule on the Writ of Habeas Data, ss. 6(e), (f).

([17]) Rule on the Writ of Habeas Data, ss. 7, 9, 10, and 16 respectively.

([18]) Mark Tolentino, 'On the Information Highway: Unsettled Questions on the Writ of Habeas Data' (4 November 2012), 'Introduction' <http://www.marktolentinolaw.com/legal-blog/on-the-information-highway-unsettled-questions-on-the-writ-of-habeas-data>. Tolentino lists Paraguay, Peru, Argentina, Ecuador, and Columbia.

([19]) Article III, s. 3(1) and art. VIII, s. 5, respectively; see Tolentino, 'On the Information Highway', section 'What is the nature and scope of the writ of habeas data?'.

([20]) 'Petition for the Issuance of the Writ of Habeas Data' (Roque and Butuyan Law Offices, Makati City, Philippines, 15 February 2013)

<http://harryroque.com/2013/07/03/writ-of-habeas-data/>.

([21]) Philippines News Agency, 'SC Issues Writ of Habeas Data vs. Comelec in Case Filed by AES Watch' (Interaksyon, 16 July 2013) <http://www.interaksyon.com/article/66511/sc-issues-writ-of-habeas-data-vs-comelec-in-case-filed-by-aes-wat%96h>.

([22]) CenPEG.org, 'Comelec Officials are No Show at Writ Hearing' (Centre for Empowerment in Government, 5 August 2013) <http://www.cenpeg.org>.

([23]) The Revised Criminal Code provisions are surveyed in Privacy International, *Privacy in the Developing World: Philippines* (Privacy International, 28 October 2012) <https://www.privacyinternational.org/reports/philippines>.

([24]) Privacy International, ch. 'I. Legal framework: Cybercrime' in *Privacy in the Developing World: Thailand* (PI, 22 October 2012) <https://www.privacyinternational.org/reports/thailand>.

([25]) Claro Parlade, 'Philippines Likely to Adopt EU-style Privacy and DP law' (2008) 95 *Privacy Laws & Business International Newsletter*, pp. 16–18.

([26]) B. Cahiles-Magkilat, 'Lack of Legislation on Data Privacy Protection Worries Investors—JFC' (Manila Bulletin, 7 June 2011) at <http://www.highbeam.com/doc/1G1-258157161.html>.

([27]) The Senate Bill is at <http://www.senate.gov.ph/lisdata/1218710275!.pdf>.

([28]) DP Act (Philippines), s. 1.

([29]) DP Act (Philippines), s. 38.

([30]) DP Act (Philippines), s. 4.

([31]) DP Act (Philippines), s. 3(g) definition of 'personal information'.

([32]) DP Act (Philippines), s. 3(j) definition of 'processing'.

([33]) DP Act (Philippines), s. 3(i) definition of 'personal information controller'.

([34]) DP Act (Philippines), s. 14.

([35]) DP Act (Philippines), s. 3(i) definition of 'personal information processor'.

([36]) DP Act (Philippines), s. 14.

([37]) DP Act (Philippines), s. 3(h)(2).

([38]) DP Act (Philippines), s. 4(a), (b), and (c) respectively.

([39]) DP Act (Philippines), s. 4(d).

([40]) DP Act (Philippines), s. 19.

([41]) DP Act (Philippines), s. 4(e).

([42]) DP Act (Philippines), s. 19.

([43]) DP Act (Philippines), s. 4(f).

([44]) DP Act (Philippines), s. 17.

([45]) DP Act (Philippines), s. 11.

([46]) DP Act (Philippines), s. 12.

([47]) European Union Agency for Fundamental Rights (FRA), *Handbook on European Data Protection Law* (FRA, 2013), pp. 84–90; see EU Directive, Art. 7(f).

([48]) DP Act (Philippines), s. 11.

([49]) DP Act (Philippines), s. 11.

([50]) DP Act (Philippines), s. 12.

([51]) DP Act (Philippines), s. 11(c).

([52]) DP Act (Philippines), s. 11(e).

([53]) DP Act (Philippines), s. 11(f).

([54]) DP Act (Philippines), s. 3(l).

([55]) It includes 'any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings'.

([56]) DP Act (Philippines), s. 3(k).

([57]) These included government ID numbers, tax or adverse licensing information, and information regarded by law as 'classified'.

([58]) DP Act (Philippines), s. 13.

([59]) DP Act (Philippines), s. 16(c).

([60]) DP Act (Philippines), s. 16(d).

([61]) DP Act (Philippines), s. 16(e).

([62]) DP Act (Philippines), s. 18.

([63]) DP Act (Philippines), s. 16(f).

([64]) DP Act (Philippines), s. 20.

([65]) DP Act (Philippines), s. 24.

([66]) DP Act (Philippines), s. 20(f).

([67]) DP Act (Philippines), s. 4.

([68]) DP Act (Philippines), s. 4.

([69]) DP Act (Philippines), s. 21.

([70]) DP Act (Philippines), s. 4(g).

([71]) DP Act (Philippines), ss. 9 and 42.

([72]) Malou Mozo, 'Palace Against Information Department Establishment' (Manila Bulletin, 3 September 2013) <http://www.mb.com.ph/palace-against-information-department-establishment/>.

([73]) DP Act (Philippines), s. 7.

([74]) DP Act (Philippines), s. 7.

([75]) DP Act (Philippines), s. 7(l)–(m).

([76]) DP Act (Philippines), s. 7(h).

([77]) DP Act (Philippines), s. 7(j).

([78]) DP Act (Philippines), s. 7(n)–(q).

([79]) DP Act (Philippines), s. 7(a).

([80]) DP Act (Philippines), s. 7(b).

([81]) DP Act (Philippines), s. 7 (d).

([82]) DP Act (Philippines), s. 7(c).

([83]) DP Act (Philippines), s. 7(i).

([84]) DP Act (Philippines), ss. 25–29 respectively.

([85]) DP Act (Philippines), ss. 30–32 respectively.

([86]) DP Act (Philippines), s. 35.

([87]) DP Act (Philippines), s. 34.

([88]) See both DP Act(Philippines) ss. 34 and 36.

([89]) DP Act (Philippines), s. 37.

([90]) DP Act (Philippines), s. 7(e) and (h).

([91]) DP Act (Philippines), s. 7(j).

([92]) This paragraph is primarily based on Church et al., 'Thailand' in *A Short History of South-East Asia* pp. 158–75. See also Case, ch. 5 'Thailand: An Unconsolidated Democracy' in *Politics in Southeast Asia—Democracy or Less?*, and Pike, *Empires at War: A Short History of Modern Asia Since World War II* (I B Tauris, 2011), chs. 11, 40, and 57, and pp. 711–13.

([93]) Pike, *Empires at War*, p. 713.

([94]) Joe Leeds, 'Update: Introduction to the Legal System and Legal Research of the Kingdom of Thailand' (*GlobaLex*, April 2011) <http://www.nyulawglobal.org/globalex/thailand1.htm>.

([95]) Leeds, 'Introduction to the Legal System of Thailand', '2. Government'.

([96]) Leeds, 'Introduction to the Legal System of Thailand', '2.3. Judicial Branch' and '3.4. Judicial decisions'.

([97]) Pirongrong Ramasoota and Sopark Panichpapibul, 'Online privacy in Thailand: Public and Strategic Awareness (Year 1)' (Thai Media Policy Centre, Privacy International and IRDC Canada, 2012), p. 44.

([98]) Church, *A Short History of South-East Asia*, p. 163.

([99]) Privacy International, ch. III 'Surveillance policy' in *Privacy in the Developing World: Thailand*.

([100]) '…the card holder's name, addresses, date of birth, religion, nationality, blood type, allergies and medical conditions, biometric images, parents' names, marital status, social security, health insurance or healthcare scheme, driving licence details, and taxation data', Privacy International, ch. IV 'Privacy Issues' in *Privacy in the Developing World: Thailand*.

([101]) Ramasoota and Panichpapibul, 'Online privacy in Thailand', p. 2.

([102]) Ramasoota and Panichpapibul, 'Online privacy in Thailand', p. 12.

([103]) Ramasoota and Panichpapibul, 'Online privacy in Thailand', 'I Background'.

([104]) Constitution of Thailand 2007 (AsianLII) <www.asianlii.org/th/legis/const/2007/>.

([105]) Constitution of Thailand 2007, ss. 32, 33, 35, 36, and 56 respectively.

([106]) Constitution of Thailand 2007, s. 28: 'A person whose rights and liberties recognised by this Constitution are violated can invoke the provisions of this Constitution to bring a lawsuit or to defend himself in the Courts. A person may bring a lawsuit against the State directly so as to act in compliance with the provisions in this Chapter. If there is a law enforcing the exercise of any right and liberty as recognised by this Constitution, the exercising of that right and liberty shall be in accordance with such law.'

([107]) Tae-Ung Baik, *Emerging Regional Human Rights Systems in Asia* (Cambridge, 2012), p. 72.

([108]) UNCTAD Report (Galexia, 2013), <http://www.galexia.com>.

([109]) Ramasoota and Panichpapibul, 'Online privacy in Thailand', p. 46.

([110]) <http://www.oic.go.th/content_eng/act.htm>.

([111]) Privacy International, *Privacy in the Developing World: Thailand*.

([112]) Ramasoota and Panichpapibul, 'Online privacy in Thailand', p. 46.

([113]) OIC, 'Official Information Commission' <http://www.oic.go.th/content_eng/committee.htm>.

([114]) OIC 'Reports Information Disclosure Tribunals' (English version) <http://www.oic.go.th/content_eng/report.htm>.

([115]) Nakorn Serirak, 'Personal Information Protection in Thailand: A Proposed Model' (Thammasat University, PhD dissertation paper, unpublished, 2006), pp. 10–11.

([116]) OIC, 'Diagram of Appeal and Complain' (2013) <http://www.oic.go.th/iwebstat/istatyear.asp?language=En>.

([117]) Serirak, 'Personal Information Protection in Thailand', pp. 10–11.

([118]) OIA (Thailand), s. 25, subject to exceptions in ss. 14, 15.

([119]) OIA (Thailand), s. 15(5).

([120]) OIA (Thailand), s. 25.

([121]) OIA (Thailand), s. 23, except in relation to disclosures which are covered by s. 24.

([122]) OIA (Thailand), s. 28.

([123]) OIA (Thailand), s. 25, refers to the right to take actions under ss. 23 and 24 on behalf of a minor or a person who is incompetent.

([124]) Ramasoota and Panichpapibul, 'Online privacy in Thailand'.

([125]) Ramasoota and Panichpapibul, 'Online privacy in Thailand', p. 49.

([126]) Wanchai Raksirivorakul, 'Introducing Thailand's data protection law' (Martindale.com, 17 July 2008) <http://www.martindale.com/computer-data-services/article_Mayer-Brown-JSM-%28Thailand%29-Limited_456798.htm>.

([127]) Serirak, 'Personal Information Protection in Thailand', p. 19.

([128]) Ramasoota and Panichpapibul, 'Online privacy in Thailand', p. 50.

([129]) David Duncan, 'Personal Data Protection in Thailand' (Tilleke & Gibbins, 20 July 2011) <http://www.mondaq.com/x/139148/Privacy/Personal+Data+Protection+in+Thailand>.

([130]) Ramasoota and Panichpapibul, 'Online privacy in Thailand', pp. 51–9.

([131]) Ramasoota and Panichpapibul, 'Online privacy in Thailand', pp. 57–8.

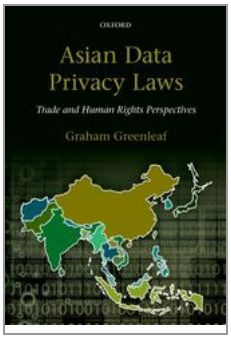
([132]) Dhiraphol Suwanprateep and Nont Horayangura, 'Thailand's Cabinet Approves a Draft Data Protection Act' (2012) 120 *Privacy Laws & Business International Report*, p. 8.

([133]) Ramasoota and Panichpapibul, 'Online privacy in Thailand'.

([134]) This list paraphrases Suwanprateep and Horayangura, 'Thailand's Cabinet Approves a Draft Data Protection Act'.

([135]) Dhiraphol Suwanprateep, personal email, 6 December 2013.

University Press Scholarship Online
Oxford Scholarship Online



Asian Data Privacy Laws: Trade & Human Rights Perspectives
Graham Greenleaf

Print publication date: 2014
Print ISBN-13: 9780199679669
Published to Oxford Scholarship Online: December 2014
DOI: 10.1093/acprof:oso/9780199679669.001.0001

Vietnam and Indonesia—ASEAN's Sectoral Laws

Graham Greenleaf

DOI:10.1093/acprof:oso/9780199679669.003.0013

[–] Abstract and Keywords

Vietnam and Indonesia both have substantial data privacy laws limited to their e-commerce sub-sectors, but it is probable that in the medium term, those laws will develop into comprehensive laws for their entire private sectors. This chapter sets out the constitutional, civil law, and criminal law aspects of data privacy protection in each country, and then examines in detail the specific data privacy laws. Vietnam's brief privacy provisions in its Law on E-Transactions of 2005 and 2006 Law on Information Technology are supplemented by detailed provisions in Decree No. 52/2013 on e-commerce of 2013. Some privacy provisions are also found in the 2010 Law on Protection of Consumers' Rights. In 2012 Indonesia enacted a Regulation under its 2008 law on electronic transactions (previously dormant in relation to data protection), adding components of a brief but enforceable privacy code and a data breach notification requirement. A comprehensive law is under development.

Keywords: data protection, privacy, Asia, Vietnam, Indonesia, ASEAN, sectoral, e-commerce, consumer

1. Introduction—sectoral data privacy laws, and future possibilities

Vietnam and Indonesia both have substantial data privacy laws limited to their e-commerce sub-sectors, but it is quite likely that in the medium term, those laws will develop into comprehensive laws for at least their entire private sectors. Extension to the public sector is more likely in democratic Indonesia than in Vietnam's one-party state.

2. Vietnam—privacy and commerce in a one-party state

Vietnam is officially a socialist market economy, with its politics still under the firm control of the Communist Party. It has a thriving private sector which accounts for about 40 per cent of GDP, operating beside state-owned enterprises. With a population of over 90 million, it is the fourteenth most populous country in the world. It has been a World Trade Organization (WTO) member since 2007, and is a negotiating partner in the Trans-Pacific Partnership discussions. Vietnam has an export-oriented economy, and has considerable foreign direct investment running at over US$10 billion per annum. Although GDP growth slowed in 2012 it is still growing at around 5 per cent per annum. The fact that a high proportion of its population are young is a significant driver. Vietnam therefore has one of the more significant and growing economies in the Association of Southeast Asian Nations (ASEAN) region and Asia generally.

Data privacy laws in the private sector are likely to be of increasing significance as Vietnam becomes more involved in international trade in goods and services.[1] For the past eight years, Vietnam has steadily expanded and strengthened its legislative protections of privacy **(p.362)** in relation to e-commerce, and in consumer transactions generally. The Government Decree 52 of 16 May 2013 on e-commerce,[2] which took effect on 1 July 2013, replacing a previous Decree,[3] is Vietnam's most detailed data privacy regulation so far.

2.1. Contexts

Vietnam was and is the subject of complex influences. It is now a leading member of ASEAN (originally established to limit communist expansion) since 1995, and its Chair in 2001. However, its longest and deepest historical influences are from China, with which it has a complex relationship. Vietnam has been described as belonging culturally 'to the Confucian world of East Asia', a factor distinguishing it from the predominantly Buddhist cultures of its Southeast Asian neighbours.[4]

History, politics, and economics of Vietnam

From the second century BC to 907 AD northern Vietnam was ruled by China for over a thousand years, followed by 500 years of conflict between independent Vietnamese regimes and reassertions of Chinese power. From the founding of the Le dynasty in 1428, an independent Vietnam expanded southward for three centuries, separated into southern and northern states, and was re-united by the first of the Nguyen emperors in 1802. From 1859–85 the French conquered Vietnam in stages, and French colonial policies, while bringing aspects of modernity to

Vietnam, did not bring significant economic benefits to the Vietnamese. The Japanese occupation from 1940 was initially aided by a French colonial collaborationist regime, but this collapsed in 1945. The communist and nationalist Vietminh, under the leadership of Ho Chi Minh, quickly seized power in north and central Vietnam, whereas the French were able to reassert control in the south.[5]

From 1946 Ho's forces fought the French, defeating them in the conclusive battle of Dien Bien Phu in 1954. At the Geneva peace conference Ho's government accepted partition, to be followed by national elections in 1956. Diem's government in the south refused to hold elections, and 20 years of war followed between the governments of the north (with aid from China and the USSR) and the south (aided by massive troop numbers from the USA and its allies). The Paris Peace Agreement in 1973 and US troop withdrawal was followed by north Vietnamese military victory in 1975. Reunification involved the subordination of the capitalist south to the austere socialist north, and recovery from the human and environmental devastation of 30 years of war. A decade of economic stagnation (including the flight of Chinese and Sino-Vietnamese citizens) was replaced in 1986 by adoption of the policy of *doi moi* ('renovation'), resulting in the gradual but constant reintroduction of private property, modern legal institutions and elements of the rule of law, and private enterprise. Vietnam's 1978 invasion of Cambodia delayed the normalization of its relationships with its neighbours and the USA, and it did not join ASEAN until the mid-1990s. By 2007 it was also admitted to the WTO and the USA was its largest trading partner. **(p.363)** It remains a one-party state, but is increasingly a hybrid economy, 'with a free-enterprise economy operating alongside state enterprises'.[6]

E-commerce has been the main factor in Vietnam's adoption of data privacy laws. According to Sharbaugh, in 2013 'Internet penetration in the nation has grown over 12,000% in the past decade —among the fastest rates of growth in the world—to a total current penetration of 31% (compared to a world average of 32.7%, Europe's 61% average, and an overall penetration across Asia of 26.2%) (Internet World Stats, 2012)'.[7]

Government and legal system of Vietnam

Vietnam's legal system is a hybrid that has resulted from many influences, and despite some continuing influences from its French civil code history it is argued that it 'has little in common with civil law jurisdictions as a matter of substance', having since 1986 'created a mix, blending many different legal concepts, rules and principles from various jurisdictions (depending on the background of the domestic drafters and the international advisers) with the socialist ideologies of the ruling Communist Party and the policies of the Vietnamese Government prevailing at the relevant time'.[8] Dang Xuan Hop argues that 'an entire new legal system' has been created since the start of the Doi Moi policy in 1986 in order to accommodate private ownership and businesses, and foreign investment, despite state institutions staying largely unchanged. This impetus was heightened by the processes of WTO accession in 2007, and its market economy requirements. He sees the result as 'a one way street toward a system of rule of law',[9] although the substantive extent of the rule of law in Vietnam remains highly debatable.[10] 'Toward' may, however, be correct.

The hierarchy of legal sources in Vietnam is similar to that in China, with at least 12 levels of legislative instruments identifiable,[11] headed by the Constitution (1992, with amendments), Laws and Resolutions of the National Assembly (which holds all state powers), and Ordinances and Resolutions of the Standing Committee of the National Assembly, followed by many different instruments from differing levels of the government.[12] Decision of courts are not officially regarded as sources of law or interpretations of it (although they may be useful guides to other

courts), whereas Resolutions of the Judges' Council of the Supreme Court instructing lower courts how to decide cases are regarded as legislation.[13] Lower level instruments must not contradict those at a higher level, and higher levels of government have the responsibility of checking that this does not occur at lower levels within their responsibility.[14] The Ministry of Justice may issue unfavourable (and influential) opinions if it considers this has occurred,[15] though these do not have direct legal effect. The National Assembly only meets twice per year for month-long **(p.364)** sessions, with mainly part-time members, and its Standing Committee exercises significant legislative power between sessions.[16]

Partly because the legal system now comprises over 10,000 legal instruments, potential conflicts between instruments, and unclear drafting, often arise, and a practice has arisen of citizens and businesses submitting enquiries requesting clarifications by 'official letters' from the authorities responsible for a particular instrument. Although these are not legal instruments, they are important until and unless a new legal instrument is passed or a court rules on a dispute concerning the matter (although that is not regarded as interpretation, nor binding).[17]

The People's Courts are a single system, with original jurisdiction confined to the lower courts (district and provincial), and the Supreme People's Courts (SPCs) only exercising appellate jurisdiction. The SPCs comprise general Courts of Appeal, and specialized Civil, Criminal, Economic, Labour and Administrative Courts. Lower courts comprise a judge and two elected people's jurors, whereas appeal courts comprise three judges.[18] Vietnam's courts are overloaded and subject to lengthy delays, and the quality of decision-making is not regarded as high. Enforcement of decisions has been regarded as poor but is improving.[19]

The Communist Party, although not a legal institution, is regarded as having 'the most important role' or a 'critical role and deep involvement' in Vietnam's legal system, including in the operation of its courts.[20] This makes assertions concerning the rule of law contentious because of the extent to which the Communist Party is still the final legal authority. Although legislation has proliferated since 1986 to regulate every area of life, Hop notes that 'the Vietnamese have been struggling to come to terms with the notion that the law dictates the behaviour in the society, that everyone must act pursuant to the law', and that informal means of dispute resolution through social connections or administrative hierarchies are not the only ways to resolve disputes.[21]

Public opinion and civil society in Vietnam

Sharbaugh's complex qualitative and quantitative study of Vietnamese attitudes to online privacy aims to answer (i) 'how do Internet users in Vietnam understand and conceive of online personal privacy', and (ii) 'how concerned are they about personal privacy on the Internet'?[22] Among its conclusions[23] are that:

> this study suggests that Vietnamese netizens may view privacy not as a right—that is, as a fundamental individual entitlement—but rather as a normative behavior, a socially prescribed manner of preventive action like locking one's door or brushing one's teeth, more responsibility than right. It is not their privacy per se that Vietnamese respondents seem to feel is threatened on the Internet; it is their wallets and their social capital.
>
> **(p.365)** This all suggests that Vietnamese conceptions of privacy may have more in common with notions of mere personal information and data security than with traditional Western ideals rooted in identity formation and personal autonomy.

He concludes that a definition of privacy appropriate for Vietnamese perceptions is that '[p]rivacy in Vietnam is the responsibility of individuals to keep themselves free from malign interference from

other individuals',[24] but that this does not include protection against the state. The Vietnamese government presented a somewhat different view in 2008, stating that opinion surveys showed that 'the safety and security of personal data' was 'voted No. 3 in the top 7 obstacles to the e-commerce development' in 2006, and as 'obstacle No. 1' in 2007. It claimed that 'these results show that the public and businesses are concerned and worried about safety and security of their information when involving in e-commerce',[25] but details of the survey are not provided.

There is relatively less regulatory space allowed to non-state actors in Vietnam than in other kinds of market economies, with high levels of approvals required of civil society organizations and regulation of non-profit organizations. The requirement that civil society organizations must 'belong' goes so far, says Hayton, that '[e]very formal organization must be linked by a chain of official ties to the Central Committee of the Communist Party'.[26]

State surveillance in Vietnam

At present, significant data privacy protections in Vietnam are largely confined to consumer activities, which is consistent with what has been described as Vietnam's 'low tech but effective system of near-total surveillance'.[27] Hayton describes how Vietnam's Communist Party has been able 'to co-opt traditional extended family structures into its vast state surveillance system'.[28] In recent years, the 'Cultured Families' system of neighbourhood surveillance, involving senior members of neighbourhoods and rewards for well-behaved families, has become more prominent than the previous system based substantially on the *ho khau* (family registration system), and the Public Security Ministry's system of political records (*ly lich*).[29] Political and religious content on Vietnam's Internet 'has to pass through a limited number of state controlled access points—making it easier to filter'.[30] While Vietnam's 2006 Law on Information Technology does not attempt to impose comprehensive surveillance and enforcement obligations on Internet service providers (ISPs) and similar organizations, it leaves open the option for state agencies to require surveillance cooperation.[31] In Vietnam, the context of any protections of privacy is one of very substantial state surveillance.

(p.366) 2.2. Legal protections of privacy in the general law

Vietnam has an increasing number of legislative privacy protections, including protections in the Civil Code and Criminal Code, a set of privacy principles in the Consumer Protection Law, and more extensive principles in e-commerce laws. The extent to which they are yet used or observed is, however, open to question (as it is in many countries). Sharbaugh says that the views of his survey respondents were that 'Vietnam's few legal regulations were deemed similarly without value, believed to exist only for the benefit of powerful Vietnamese government and corporate interests and influential private individuals'.[32] While the content of regulations is strengthening at present, as the rest of this chapter demonstrates, that is not yet supported by strong evidence of enforcement, although there is some evidence. The various sources of privacy protection in the general law are surveyed in this section, and the more detailed protections in e-commerce and consumer laws in the next.

Constitutional and treaty protections

Vietnam's Constitution (1992)[33] has a few clauses relevant to privacy protection. 'The citizen will enjoy inviolability of the person and the protection of the law with regard to his life, health, honour, and dignity.'[34] 'The citizen is entitled to the inviolability of his domicile. No one can enter the domicile of another person without his or her consent, except in cases authorized by the law. Safety and secrecy are guaranteed to the citizen's correspondence, telephone conversations, and telegrams. Domiciliary searches and the opening, control, and confiscation of a citizen's correspondence and telegrams can only be done by a competent authority in accordance with the

provisions of the law.'[35] Justiciability is implied, but not stated, by article 74. Constitutional amendments adopted in 2013 have not strengthened these or other clauses protecting human rights.[36]

In Vietnam 'international treaties take precedence over domestic legislation to the extent of any inconsistency', and there are often provisions in specific laws to this effect.[37] The most relevant treaty to which Vietnam is a party is the International Covenant on Civil and Political Rights 1966 (ICCPR), Article 17 of which requires privacy protection by law (see Chapter 2). A law which is inconsistent with ICCPR Article 17 could, in theory, have its validity challenged. This does not mean that Article 17 could be used, by itself, to mount a claim before a Vietnamese court.[38] Vietnam is not a signatory to the First Optional Protocol to the ICCPR (see Chapter 2, section 4.1), so its citizens cannot lodge complaints ('communications') with the UN Human Rights Committee.

Civil Code article 38 'Right to personal secrets'

Article 38 of Vietnam's Civil Code, entitled 'Right to Personal Secrets' provides a brief and general requirement of consent for the collection and publication of information about the **(p.367)** private life of a person, and protection of the confidentiality of mail, telephonic, and electronic communications. The article states that:[39]

> 1. An individual's rights to personal secrets shall be respected and protected by law.
> 2. The collection and publication of information and materials on the private life of an individual must be consented to by that person; in cases where that person has died, lost his civil act capacity, or is under full 15 years, the consent of his/her father, mother, wife, husband, adult children, or representative is required, except for cases where the collection and publication of information and materials are made by decision of a competent agency or organization.
> 3. Letters, telephones, telegrams, other forms of electronic information of individuals must be safely and confidentially guaranteed.
> 4. The inspection of an individual's letters, telephones, telegrams, and/or other forms of electronic information may be performed only in cases where it is so provided for by law and decided by competent state agencies.

This is a clear statement of an individual's rights in relation to electronic personal information in relation to both private sector and public sector organizations, and must be taken into account in assessing the extent to which Vietnam has a data privacy law. A Vietnamese court issued a judgment interpreting article 38 in 2012, in favour of a company's right to access and monitor an employee's work email account.[40] The employee had filed suit, alleging that the company accessed his personal emails, and published them by disclosure at a company meeting, without his permission, in violation of article 38. A summary of the case by Baker & McKenzie authors[41] identifies the key factors in the company's case that enabled them to defend the claim: the company had previously issued a 'computer policy' prohibiting personal use of the company-provided email service, and stating that it may access and monitor the contents of emails; the company said it did not rent the email account to the employee as a commercial service, but provided it at no cost as a 'labour tool'; as such it was subject to the 'labour contract' between employer and employee, and company policies. 'The company argued that, given the issuance of the company's computer policy, the employee knew or should have known about this policy but did not protest or leave the company, therefore giving the employer implicit consent to this policy.'[42]

The Civil Code provides that when a personal right of an individual (such as in article 38) is infringed, the person has the right to (1) 'Make rectification him/herself'; (2) 'Request the infringer

or request competent agencies, organizations to order the infringer to terminate the infringement and make a public apology and/or rectification'; or (3) 'Request the infringer or request competent agencies or organizations to order the infringer to pay compensation for damage'.[43]

Criminal law

Revisions to Vietnam's Criminal Code in June 2009 included an offence of disclosing personal information without consent. It is an offence to violate the confidentiality of mail, **(p.368)** telephone, or facsimile transmissions.[44] Over a decade ago, two Vietnamese computer hackers were prosecuted for 'stealing personal assets' (i.e. Internet passwords) and illegal use of computers to access other people's Internet accounts, and fined substantial amounts by the Ho Chi Minh City People's Court. The case was the first of its kind in Vietnam.[45]

2.3. Data privacy laws (e-commerce and consumer sectors)

The most detailed data privacy protections in Vietnam are found in these sectoral laws.

IT and e-commerce laws

The systematic development of data privacy laws in Vietnam[46] commenced with its e-commerce laws. The Law on E-Transactions of 2005 provided a brief broad statement of an individual's right to consent to the use of their personal information in e-commerce.[47] The 2006 Law on Information Technology[48] (the 'IT Law') provided more detailed regulations concerning collection, processing, use, storage, and provision of personal information. 'Network environment' is defined to mean 'an environment in which information is supplied, transmitted, collected, processed, stored and exchanged via information infrastructure'.[49] Where there are 'other laws on the same matters related to information technology application and development activities', the provisions of this law will prevail. The law applies to bodies 'engaged in information technology application and development activities'.[50] It applies to 'agencies, organizations and individuals' even where they are referred to only as 'organizations and individuals', and therefore it may apply to public sector bodies,[51] but this would need to be specified in regulations.[52] It explicitly applies to 'foreign organizations and individuals' carrying out such activities 'in Vietnam'.[53]

Articles 21 and 22 set out obligations on organizations covered by the law in relation to consent, exceptions for processing without consent, notice, use, retention/deletion, security, access (perhaps), correction (including blocking until corrected), disclosure, and compensation. These obligations cover most of the matters normally found in a data privacy law. Their content is now substantially repeated (often in very similar terms), but also made more detailed, in the 2013 Decree, as discussed later in this section.

The IT Law contains a number of other privacy-protective provisions. The anti-spam provision includes an obligation to ensure that where consumers provide notice that they do not wish to receive 'advertisement information' that wish is observed,[54] and to assure their 'ability to reject' such advertisements.[55] Using false names to send information is also prohibited.[56] Article 70 constitutes a direct marketing opt-out protection. The prohibition on those who 'create, install or spread computer viruses or harmful software' specifically refers to the purposes of 'collecting other people's information' and 'modifying or deleting **(p.369)** information'.[57] Article 72, in addition to a very general obligation to protect confidentiality of personal information,[58] prohibits a range of activities (most types of 'computer crime') including a 'catch all' prohibition of acts which endanger individuals' information.[59]

Consumer Protection Law

The 2010 Law on Protection of Consumers' Rights[60] (the Consumer Law) took effect on 1 July

2011, replacing the 1999 Ordinance on Protection of Consumers Rights. Its provisions strengthen the rights of consumers, including those on the use, collection, and transfer of consumer information, in a brief but broad data privacy code. Terms such as 'personal information' and 'consent' are not defined in this law, but other laws shed some light on their meaning. The new law expands those obligations in regard to all consumers, not just in the context of e-transactions (as was the case with earlier laws), but does not change the substance of those obligations.[61]

Business entities 'trading goods and/or services', including individual traders, have to satisfy the requirements of article 6 'Protection of consumer information'. This includes a general confidentiality and security obligation (with a broad exemption for state agencies): 'Consumers' information shall be kept safe and confidential when they participate in transactions, use of goods or services, except where competent state agencies required the information'. It also includes five more specific obligations concerning the collection, use and transfer of consumer information:

> a) Notify clearly and openly the consumer of the purpose of the collection and use of consumer information before such activities being done; b) Use information in conformity with the purpose informed to consumers, and with the consent by the consumers; c) Ensure safety, accuracy, completeness during collection, use and transfer of consumer information; d) Update or adjust by themselves or help consumers to update and adjust as the information is found to be incorrect; e) Only transfer consumer information to third parties upon the consent of consumers, except where otherwise provided by law.

There are some other provisions in the Consumer Law, which could also be valuable for privacy protection (and affect direct marketing), including article 10 (Prohibited behaviours) which includes:

> (1) 'Attempt of organizations or individuals trading goods and/or services in deceiving or misleading consumers via advertising activities, or hide or provide information that is incomplete, false or inaccurate about one of the following details:…c) The contents and characteristics of transaction between consumers and organizations or individuals trading goods and/or services.'
> (2) 'Organizations or individuals trading goods and/or services [which] harasses consumers through the marketing of goods and/or services contrary to the wishes of **(p.370)** consumers [two] or more times or [undertake] other acts that obstruct or affect normal works or activities of consumers.'

The 2013 Decree 52 on e-commerce and consumer law

In summary, the protection of data privacy in Vietnam first occurred through a number of e-commerce, IT, and consumer laws enacted by the National Assembly, the highest source of law in Vietnam. The most recent development, in 2013 is Decree No. 52/2013 on e-commerce[62] (Decree 52) made by the Government pursuant to both the IT and Consumer Laws (and other laws), and is what in some other countries would be considered a regulation, although one made by the government as a whole, not one made by a ministry. Under the IT Law, the Ministry of Post and Telematics has the prime responsibility for data privacy, but this Decree gives the implementation responsibility to the Ministry of Industry and Trade (MoIT), which is responsible for the Consumer Law. Although Decree 52 therefore seems to state that MoIT now has the responsibility for data privacy in Vietnam (at least in relation to all forms of consumer-oriented business), local experts point out[63] that the new Decree 72 on Internet management imposes the obligation to implement this broader decree on Internet management onto the Ministry of Information and Communication (MoIC), and consider that this is likely to spill over into the data privacy aspects of Decree 72 as

well. Article 2.2 of Decree 52 requires MoIT to coordinate with MoIC.

Decree 52 defines e-commerce activity broadly, as the conducting of any part of commercial activities 'by electronic means connected to the Internet, mobile telecommunications network or other open networks'.[64] 'Personal information' is defined as 'the information contributing to identify a specific individual, including his/her name, age, home address, phone number, medical information, account number, information on personal payment transactions and other information that the individual would like to keep confidential' but 'does not include work contact information and other information that the individual has published himself on mass media'.[65] Collection of personal information is also defined as 'the collection of information to put it into a database'.[66]

The scope of the Decree limits it to those businesses 'involved in e-commerce activity in Vietnam's territory', including 'foreign individuals residing in Vietnam' and 'foreign traders and organizations with their presence in Vietnam through investment operation, establishment of branches and representative offices or website set-up under Vietnamese domain name'.[67] So some extraterritorial activities may be subject to the law, but the requirement of 'e-commerce activity in Vietnam's territory' must still be satisfied. Decree 52 grants MoIT and MoIC authority to adopt separate regulations for purely foreign players conducting e-commerce with Vietnamese counter-parties, although local experts note that it is not yet clear when these will be adopted.[68]

Where a data controller authorizes a third party processor to collect personal information, there must be an agreement between the parties specifying which has responsibility for compliance with the various obligations of the Decree, and if they do not then the **(p.371)** controller will be liable.[69] Presumably the controller cannot exempt itself from liability for any processing that it actually carries out, only from that which it outsources.

One of the 'prohibited acts in e-commerce activities' is 'stealing, using, disclosing, transferring and selling information related to business secrets of other traders, organizations or individuals or personal information of consumers in e-commerce without the consent of the parties concerned, unless otherwise regulated by law'.[70]

2.4. Vietnam's data privacy principles

The 2013 Decree 52 makes the principles set out in articles 21 and 22 of the IT Law more specific, so references to the Decree are given below (unless the IT Law is specified). However, it should be remembered that the higher source of legal authority remains the more general IT Law. The most important aspects of these principles are summarized below.

Collection and notice

Businesses collecting personal information must publish (or give notice of) their data privacy policies so that it is clearly displayed before or at the time of collection, and if collected through a website is in a conspicuous place.[71] The data privacy policies must include the purpose of collection; scope of use; duration of storage; who has access; contact details of the unit gathering and managing information; and how consumers can access and modify their personal information.[72]

Businesses must obtain 'prior consent' to collection of personal information, obtained through a 'mechanism for the information subjects to clearly express their consent through online functions on the website, email, messages or other methods as agreed by the two parties'.[73] There is no requirement that the information collected must be the minimum necessary for the stated purpose.

Consent is not required for the collection of personal information (a) 'that has been publicized on e-commerce websites'; (b) 'to sign or perform contract of sale and purchase of goods and services';

or (c) to calculate prices and charges for online services.[74] The extent of the exceptions in (a) and (b) is unclear.

Use, disclosure, and transfer, including direct marketing

In addition to the requirement of collection by consent, there must also be a 'specific mechanism' for information subjects to permit or refuse (a) 'sharing, disclosure and transfer of information to a third party' or (b) 'using of personal information to send advertisements and introduce products and other commercial information'.[75] There must therefore be provisions which at least allow consumers to opt out of direct marketing. There are also anti-spam provisions.[76]

(p.372) Personal information can only be used (or shared, disclosed, or transferred) for the 'purpose and scope announced' except (a) where there is a separate agreement for additional uses; (b) to provide services or products at the request of the data subject; or (c) to perform obligations required by law.[77]

Security and data breach notification

'The information gathering unit must ensure the safety and security for personal information',[78] and some details are specified.

A very limited form of data breach notification requirement is included: 'In case the information system is attacked causing risk of loss of consumer's information, the information storing unit must notify the authorities within 24 hours after the detection of incident.'[79] This does not cover where the security breach is due to the system operator's own fault, rather than an 'attack'. There is also no obligation to inform the data subjects affected.

Consumer rights—access, correction, complaint, and deletion

The Decree is quite explicit on these rights, more so than the Laws on which it is based: 'The information subjects have the right to require the information gathering unit to perform the checking, update, modification or deletion of their personal information.'[80] The IT Law only stated that there was a right to 'request' these matters,[81] whereas here these rights are required (assuming the accuracy of the translations). The business may either take these steps for the data subject, or 'provide the information for the data subjects to check, update or modify their personal information by themselves'.[82]

The business must also 'have a mechanism to receive and settle the consumer's complaints concerning the improper use of personal information',[83] and the notice given to consumers refers to a 'way of contact for the consumers to ask about the collection and processing information related to them',[84] so it is clearly intended that data subjects should be able to query any aspect of how their personal information is processed.

2.5. Enforcement provisions

The IT Law states that 'individuals may claim compensation for damage caused by violations in the supply of personal information',[85] but this only refers to supply (disclosure) breaches. However, another provision states generally that businesses 'if causing damage, they shall pay compensations therefor in accordance with law'.[86] The 2013 Decree states in the section concerning 'administrative violations' that businesses 'that violate and cause damage to material interests of… individuals, they must make compensation as prescribed by law'.[87] It appears, therefore, that any breaches of the privacy principles can potentially result in a claim for compensation.

(p.373) The Decree provides that administrative sanctions will apply to 'violation of regulation on protection of personal information in e-commerce',[88] and that such sanctions will be handled

according to the provisions of the Law on Handling of Administrative Violations.[89] Various authorities could be involved: 'Inspector of the Ministry of Industry and Trade, the market management agency, inspector of the Service of Trade and Industry of centrally-affiliated provinces and cities and other state agencies have the right to sanction administrative violations in the e-commerce activities under the competence specified in the Law on Handling of Administrative Violations and the relevant documents.'[90] However, according to the relevant enforcement Circular, complaints about personal information are to be made to MoIT, and can be made online to the Management Portal of e-commerce activities.[91]

Businesses are subject to annual inspection by MoIT (and of equivalent province and city authorities) and are subject to a 'name and shame' provision in that the 'result of inspection shall be published in Management Portal of e-commerce activities'.[92] Once a business receives notice of a complaint from MoIT, it only has 10 days to reply before it goes on the 'name and shame' list on the MoIT website, and before administrative sanctions can be brought against it.[93]

The IT Law provides that 'disputing parties are encouraged to settle their disputes over information technology through conciliation; when parties fail to conciliate, their disputes shall be settled in accordance with law',[94] and the Decree reiterates that this applies to e-commerce disputes,[95] without requiring that conciliation must first occur.

Enforcement under the Consumer Law

The Consumer Law requires disputes to be settled through negotiation, conciliation, arbitration, or court adjudication, and there are short provisions setting out the basic rules for each type of resolution. Social organizations involved in consumer protection can represent complainants, or individuals can act for themselves.[96] However '[n]o negotiation or mediation is permitted in case of disputes causing damage to the interests of the State, the interests of many consumers, the public interest'.[97]

> The Law does not specifically prescribe administrative sanctions and criminal penalties in case of breach to the Law. Generally, the Law only states that depending on the nature and seriousness of the breach, whoever breaches the Law shall be subject to an administrative sanction or criminal prosecution and must pay compensation in accordance with law for any loss or damage caused.[98]

The Ministry of Trade and Industry (which has an E-commerce and Information Technology Department) is responsible for implementing the state administration on the protection of consumers' interests.[99] The ministry is given many of the responsibilities that would normally fall on a data protection authority (DPA), but not this does not include resolving **(p.374)** individual complaints. Enforcement under the Decree is now more specific. Chapter III sets out the roles of 'Social organizations to protect consumers' interests' (i.e. consumer non-governmental organizations (NGOs)), including '[t]aking legal action on behalf of consumers or taking legal action by virtue of the public interests'.

Self-regulatory measures—trustmarks

Vietnam has a number of competing 'trustmark' schemes, intended to increase confidence in e-commerce, some sponsored by ministries.[100] None are known to be specifically oriented toward privacy protection (unlike systems in Taiwan and South Korea), nor to have had any significant effect on privacy protection.

2.6. Conclusions—uncertain enforcement of 'minimum+' principles

Vietnam has enacted data privacy laws in the private sector, although limited to e-commerce and consumer transactions (very similar to the legal position in China). The privacy principles that are now made more explicit in the 2013 Decree are a reasonable approximation of the basic principles set out in the 1980 OECD Guidelines or the Asia-Pacific Economic Cooperation (APEC) Privacy Framework. On three points, namely deletion rights, direct marketing opt-out and data breach notification, they go significantly beyond those minimum sets of principles. These three provisions are becoming common in other Asian countries, and could be thought of as 'minimum+' provisions, a common intermediate position between the minimum and 'European' sets of principles (see Chapter 17 for further discussion).

To what extent these new additional rights will be observed by businesses in Vietnam, or enforced by MoIT or MoIC, or equivalent local authorities, remains to be seen. Some authors such as Sharbaugh are very sceptical about the value of legislative provisions such as the 2006 IT Law, concluding (based on interviews with lawyers in Vietnam) that 'the few existing regulations are obscure and widely ignored'.[101] However, the laws are now being made more precise. Vietnamese citizens, whether acting as consumers or otherwise, are not yet accustomed to using the legal system to enforce their rights, but Vietnamese society is in a process of rapid change and there may be more exercise of consumer rights in future.

3. Indonesia

Indonesia is often ignored in discussions of data privacy, but as an Asian democracy with a population of over 250 million (exceeded only by China and India), the third largest democracy (after India and the USA), and a fast-developing economy with over 6 per cent economic growth in 2012, its position is important to data privacy in Asia and globally. Although it is the largest ASEAN state, it has moved slowly to provide comprehensive legal protection for personal information, and is lagging behind its major ASEAN neighbours, all of which now have more extensive data protection laws. The absence of such laws in Indonesia is believed to have contributed to trading of personal data by insurance companies, banks, and mobile phone service providers for telemarketing.

(p.375) In 2012 Indonesia enacted a Regulation under its 2008 law on electronic transactions (previously dormant in relation to data protection), adding components of a brief but enforceable privacy code, and a data breach notification requirement. These laws are of somewhat limited scope, applying only to 'electronic system operators' and to actions 'through electronic media', somewhat similar to provisions in Vietnam and China. Indonesian scholars and privacy advocates do not regard this reform as sufficient, because the regulation is too broad and unclear, as well as limited in scope. Various ministries are taking steps to develop a full data protection law, for differing reasons discussed briefly at the end of this chapter.

3.1. Indonesia—contexts

Indonesia's development of data privacy laws needs to be understood against the complex backdrop of is modern struggle toward democratic institutions,[102] and the legal system that has been formed within that context.[103]

History and politics of Indonesia

For over a thousand years prior to European colonialism there were well-established, wealthy, and competing states in various parts of what is now Indonesia. The conversion of Indonesia to Islam from Buddhism and Hinduism began in the thirteenth century and by the time Dutch colonialism replaced early Portuguese influence in the seventeenth century, most parts of Indonesia had been Islamicized. Dutch colonialism, originally as a trading company based at Batavia (now Jakarta),

gradually expanded its control across Java from 1619, and then through much of the rest of Indonesia in the nineteenth century, creating a very centralized colonial regime. They created an economically successful plantation-based economy, but failed to manage urbanization so that living standards declined during the twentieth century. Dutch rule was destroyed by the Japanese in 1941. Sukarno and other nationalists used the opportunity to promote Indonesian nationalism, and declared unilateral independence in 1945 as the war ended. A war of resistance against the re-occupying Dutch continued for four years, until diplomatic victory involving threatened suspension of Marshall Plan aid made the Netherlands formally agree to end colonial rule.

Independent Indonesia under Sukarno as its first President from 1945–65 began as a liberal democracy, but was primarily a struggle between groups with different concepts of the Indonesian state. The army, which had always been significant, seized power under Suharto, and claimed an attempted Communist Party of Indonesia (PKI) coup as the justification for the murder of at least 400,000 people, eliminating the PKI as a force in Indonesian politics. Suharto's 'New Order' government from 1965–88 was a military regime operated through a military-dominated parliamentary faction ('Golkar') and controlled elections. Case describes it as 'an exemplar of pseudo-democracy, characterized by **(p.376)** few civil liberties and regular, though rigged elections'.[104] Early successful development of resource-based industries, and then export-oriented manufacturing, gave some degree of social stability and economic improvement, coupled with endemic corruption and kleptocracy, until the Indonesian economy collapsed in 1997. Constant street protests forced Suharto to resign, and his deputy, Habibi, to promise elections in 1999, the first experience of a genuine election for most Indonesians. Since then, 'the demand for greater openness and a return to a democratic society has dominated Indonesian public discourse'.[105] During the past 15 years, Indonesia has had three indirectly elected Presidents (B.J. Habibe, Abdurrahman Wahid, and Megawati Sukanoputri), and, since 2004, the first directly elected President, Susilo Bambang Yudoyono (SBY).

Throughout this period Indonesia has gradually strengthened almost all of its institutions supporting democracy and the rule of law. It has not reverted to being an authoritarian state, despite some repressive laws and the threat of terrorism. For issues such as the development of data privacy protections, this is the most important contextual factor, as it holds out the possibility that Indonesia will impose privacy restraints on the state, not only on the private sector. Some commentators see the 'optimistic scenario' that 'Indonesia may soon boast of possessing arguably the most open and democratic civil society in the whole of South-East Asia'.[106]

Government and legal system of Indonesia

Indonesia is characterized as 'one of the most legally diverse, and consequentially legally complex, countries in the world'. Although it is the largest Muslim majority country, and it does implement important parts of Islamic law, it is not an Islamic state. It is a civil law country, with a Dutch legal heritage (part of the French civil law tradition), but statutes have replaced much of its Civil Code and Commercial Code. Adat law (indigenous law of various ethnic groups) is important in some areas of law.[107] A civil law approach has often continued to be followed in new statutes, and the creation of new institutions such as the Constitutional Court and the Administrative Courts.[108] Lindsey and Santosa argue that 'Indonesian law is made up of several legal systems interwoven with each other operating simultaneously'.[109]

In 1959 after a period of constitutional conflict following Indonesian independence and the conclusion of World War II, Indonesian President Sukarno decreed that its 1945 Constitution would be reinstated as Indonesia's Constitution, and it remained unchanged for 40 years until 1999, when the Suharto era ended, and the rapid democratization and change of the Reformasi

(reform) era began. The 1945 Constitution, with significant post-1999 amendments, remains the Indonesian Constitution.[110] In particular, the amended Constitution has both an extensive list of human rights, and a means of protecting them (i.e. the Constitutional Court). Lindsey concludes that the four sets of Constitutional **(p.377)** amendments establish 'the broad principles of a more just and democratic system'[111] and that it is 'an incomparably better document' resulting from a constitutional reform process that few countries have ever achieved so well.[112]

Indonesia's House of Representatives (Dewan Perwakilan Rakyat or DPR) enacts statutes, which then require approval by the President. The President can also enact government regulations in lieu of a statute, but it must be approved at the next session of the DPR or it ceases to be in force. The President also issues government regulations to implement statutes. There is a Regional Representatives Council (Dewan Perwakilan Daerah or DPD) but it can only propose Bills to the DPR and otherwise has a consultative role.[113] Indonesia's parliamentary system is therefore essentially unicameral, and the overall political system presidential.

Although Indonesia is a unitary state, not a federation, the Constitution and regional autonomy laws mean that 'regional governments now exercise many more powers than before the Reform Era, resulting in a decentralisation of many rule-making powers',[114] and the governors and regional assemblies of 33 provincial governments adopt regulations. Such regional governments in the other largest Asian states, China and India, have already started to adopt regulations affecting data privacy, and in time this may also happen in Indonesia. It is not known to have occurred yet, although such laws are not centrally published and are very difficult to ascertain, resulting in legal uncertainty.[115] Residual legislative powers, covering all areas where the central government has not legislated, lie with the regional governments.[116]

The formal hierarchy of sources of laws in Indonesia, though it is sometimes disregarded, is: (i) the Constitution; (ii) statutes, or government regulation in lieu of statute; (iii) government regulation (i.e. regulations made to implement statutes); (iv) presidential regulation; and (v) regional regulation.[117] It is common for statutes, which are usually stated in very general terms, to come into force before the regulations to implement them are made, which causes confusion, and for implementing regulations to be significantly delayed or never enacted.[118] This has occurred with Indonesia's e-commerce laws affecting privacy.

Indonesia's Constitutional Court, created by Constitutional amendment in 2001, is the only court entitled to decide on the constitutionality of statutes, and stands outside the normal court hierarchy. Its powers of review are quite limited, and do not extend to review of the constitutionality of any of the forms of regulations, or of administrative actions by state agencies or officials.[119] The Constitutional Court therefore has a considerably narrower scope than courts such as the Indian Supreme Court, to consider whether regulations or administrative actions interfere with constitutionally guaranteed privacy rights. Nevertheless, as discussed in section 3.2 of this chapter, it has intervened in privacy-related issues arising from statutes.

Since 2004 all of Indonesia's courts, other than the Constitutional Court, have come under the 'one roof' of the Supreme Court, a step aimed at enhancing judicial independence. The **(p.378)** Supreme Court is the final court of appeal for decisions from all courts under its supervision, including the general Court of Appeal or High Courts which handle civil, commercial, and criminal matters, and the separate Administrative, Military and Religious courts.[120] Indonesia does have some specialized courts such as the Commercial Court (limited at present largely to bankruptcy/insolvency matters and some intellectual property matters),[121] but matters arising under legislation affecting privacy issues would normally be heard before the High Courts.

While the Constitutional Court has gained a reputation as 'competent, efficient and not corrupt', in general 'the reputation of the courts is one where corruption is too common, where competence and fairness are not always as high as they should be',[122] or as another author has put it more harshly 'a legal system that is…considered one of the most corrupt and incompetent in the world'.[123]

A review of reforms under each President since 1998 concluded that:[124]

> the politicians and bureaucrats of the Era Reformasi are facing the task of unravelling a pervasive system of institutionalised authoritarianism and rebuilding the dysfunctional legal system inherited from the first two presidents, and the pervasive, systemic corruption model inherited from the first Seoharto, without, at the same time, disintegrating the state.

State surveillance and ID card in Indonesia

The national ID system, the Electronic Identity Card Program (eKPT), was launched in 2010 and is being implemented across Indonesia by the Ministry of Home Affairs. The complexity of the biometrics involved makes the aim of enrolling all 172 million people and issuing cards an ambitious one:[125]

> The enrollment process consists of acquiring a photograph of the person's face, fingerprints of all 10 fingers, iris images of both eyes, a digitized signature, and biographical information. The bulk of the information is stored as a record associated with each electronic identity card, though each card is understood to contain two fingerprint templates, a photo, and personal information.

It is claimed that by 2012 enrolment was 80 per cent complete, and 60 million cards issued. As well as many government uses, financial institutions will be able to use the IDs as proof of identification.[126] The inclusion of the 'religion' field remains controversial, with Christian politicians calling for its removal.[127] The Law on Public Administration (No. 23/2006), one basis of the programme, contains general and brief provisions requiring that specific personal data[128] used in the system must be stored securely, kept accurate, and its confidentiality protected, and requires that more detail should be stipulated in government regulations.[129]

(p.379) Although there were plans to have the issue of cards completed in time for the 2014 national elections, technical difficulties have pushed this date back to at least 2015. Since Indonesia does not yet have any general data privacy law covering either its public sector or private sector, and the law dealing specifically with the eKPT will not deal with privacy issues, the control of the privacy aspects of the national ID scheme remains a major danger and deficiency of Indonesia's privacy protections.

Public opinion and civil society organizations in Indonesia

A Privacy International report suggests that:[130]

> There is no strong tradition of the right to privacy in Indonesia's collectivist culture, which expects the individual to melt within the group (family, clan, ethnic groups). However, such attitudes are gradually being influenced by international human rights instruments, the practices of other countries, and the use of information technology and the internet. Slowly, Indonesian civil society has begun to acknowledge the importance of privacy rights, and in the last ten years privacy has become an increasingly important issue, particularly with regard to the protection of personal data.

The Privacy International report states[131] that a number of NGOs and media organizations are now focused on privacy issues in Indonesia. These include ELSAM (the Institute for Policy Research and Advocacy), established in 1993 for the purpose of encouraging the development of a democratic political order by means of strengthening civil society through advocacy and promotion of human rights, and the now-independent Press Council which is no longer a government adviser but works to protect the freedom of the press and advocates privacy protections.

3.2. Constitutional and treaty protection of privacy, and human rights laws

Indonesia is a member of APEC, ASEAN, and the WTO (since 1995).

Constitutional protections, and cases, limit telecommunications interception

Although privacy is not explicitly protected in Indonesia's constitution, its courts have recently found implied protection of privacy through interpretation of article 28G(1) of the Constitution, which states: 'Each person is entitled to protection of self, his family, honor, dignity, the property he owns, and has the right to feel secure and to be protected against threats and fear to exercise or not exercise his basic rights.'

A very significant decision[132] of Indonesia's Constitutional Court in 2010 restricts the giving of authority to perform wiretapping to government agencies without a court warrant, based on Indonesia's constitutional protection of privacy. In *Anggara v Kominfo*[133] the Constitutional Court annulled article 31(4) of the Electronic Information and Transactions Law (No. 11 of 2008) because the article authorized the government to issue a regulation concerning wiretapping. As a result of this annulment, the Ministry of **(p.380)** Communication and Information Technology is not allowed to regulate the mechanism of legal wiretapping by government regulation but must do so by legislation. The Court held that article 31(4) of the Law contradicted article 28G of the Constitution relating to privacy rights, and is therefore no longer binding. The claimant argued that privacy is a fundamental human right and since interception is a limit on the individual privacy right, such limits should not be in the form of government regulation. In its verdict, the Court said that there is no comprehensive law or regulation regarding wiretapping. The rules for wiretapping are spread throughout several existing laws (such as the Electronic Information and Transactions Law, Telecommunications Law, Narcotics Law, Corruption Law) and regulations, with different mechanisms and procedures. The court held:

> The prevailing laws and regulations do not provide clear instructions on wiretapping, such as warrants, limits, and authorized officials. This can lead to violations of constitutional rights, since all of this is based on each institution's policy. Therefore the Court considers that the wiretapping is a violation of the right to privacy, which is part of the fundamental human rights. Even though the right itself can be limited, this should be governed by a law, as regulated under Article 28J (2) of the 1945 Constitution. Therefore, a specific law on wiretapping is needed if wiretapping is going to take place, since mere government regulation cannot limit human rights.

In this judgment the Court reaffirmed two previous cases, which reviewed the KPK (Eradication of Corruption Commission). In *KPKPN v KPK*[134] the court held that privacy rights are derogable rights, and therefore the state can place restrictions on them. However, to 'prevent the abuse of authority through wiretapping and recording, laws and regulations on wiretapping and recording procedures are needed'. The Court also referred to its decision in *Mulyana v KPK*,[135] which stated that human rights limitations by wiretapping have to be regulated by law to prevent human rights violations by abuse of authority. Furthermore, the Court found that such laws should describe among other things who has the authority to issue an order for wiretapping and

recording of conversations, and whether the order may only be issued after adequate initial evidence is obtained.

The decision in *Anggara v Kominfo* is considered a landmark case that has shown that privacy rights are protected in Indonesia as a basic human right, and that the constitutional right is a legal basis upon which government could found the drafting of other related legislation such as on data protection, wiretapping, or legal interception. The MoIC is in the process of drafting a comprehensive bill on wiretapping.

Treaty provisions and the Law on Human Rights

Indonesia has enacted a number of laws relevant to human rights, and therefore to privacy. The Human Rights Law of 1999[136] adopted the United Nations' Universal Declaration of Human Rights (UDHR), which includes the right to privacy. Articles 31 and 32 of this Law state that no one shall be subjected to arbitrary interference with his home and with his correspondence.[137] Indonesian scholars consider that this Law is evidence that Indonesia has accepted a moral and legal responsibility to respect, execute, and uphold the UDHR and **(p.381)** several other international instruments ratified by Indonesia concerning human rights. Where there are alleged violations of articles 31 and 32, the Human Rights Law 1999 provides for mediation and settlement conducted by the National Commission of Human Rights.[138]

Indonesia has ratified the ICCPR[139] but not every right guaranteed under the ICCPR has been followed by domestic implementing legislation, including Article 17 concerning privacy. Indonesia has not ratified the First Optional Protocol to the ICCPR (see Chapter 2, section 4.1), so its citizens cannot lodge complaints ('communications') with the UN Human Rights Committee. However, the Human Rights Law in article 7(2) explicitly states that 'Provisions set forth in international law concerning human rights ratified by the Republic of Indonesia, are recognized under this Act as legally binding in Indonesia'.[140] This provision implies the direct applicability as part of national law of every human right treaty ratified by Indonesia. International human rights treaties therefore do not need domestic implementing legislation in order to be applied at the national level. This gives considerable long-term scope for Indonesia's courts to import human rights considerations into Indonesian law.

The Human Rights Commission (Komnas HAM) and Human Rights Courts

The Human Rights Law 1999 substantially strengthened the legal basis of the position of the National Commission on Human Rights (Komisi National Hak Asasi Manusia—Komnas HAM), and gave it greater budgetary and other independences, although it had existed prior to the Act. Komnas HAM has powers to 'investigate and examine incidents… which…may constitute violations of human rights'.[141] Its Commissioners are empowered to mediate if it finds a violation has occurred, and their written resolutions are supposed to be 'legally binding and officially valid' and enforceable in court. In practice, persuasion is more often used.[142] In the absence of a DPA in Indonesia, Komnas HAM is probably the only body that could investigate complaints of invasions of privacy (as breaches of ICCPR, Article 17), although this is not likely to be one of its own priorities because of more pressing human rights abuses in Indonesia.

The Human Rights Court Law 2000[143] created the Human Rights Court, but it is usually not relevant to privacy issues, as its jurisdiction is generally limited to genocide or crimes against humanity,[144] which would only incidentally include any data privacy issues. The Indonesian government established a State Minister on Human Rights Affairs in 1999, which in 2000 was merged with the Ministry of Justice and Human Rights.[145]

(p.382) 3.3. Other privacy-related laws

Although the Law and Regulation on Electronic Information and Transaction, discussed in section 3.4 of this chapter, is the main data privacy law in Indonesia, there are some other protections deserving mention.

Right to information legislation

As in many countries, one of the first steps toward data privacy rights in Indonesia is the establishment of the right of individuals to access their own records held by public agencies. The Public Information Disclosure Law[146] took effect in 2010. The key right provided by the Law is that 'Every individual has the right to obtain Public Information pursuant to the provisions of this Law'.[147] Applicants must 'state the reason for such request'.[148] Applicants may sue in court if they are obstructed from obtaining information,[149] but there are alternative dispute resolution procedures provided via the Information Committees established under the Act. 'Public information' is given a rather confusing definition,[150] but seems to be sufficient to cover most personal information held by public agencies:

> Public Information means information that is produced, stored, managed, sent and/or received by a Public Agency relating to the organizer and the organizing of the state and/or the organizer and the organizing of other Public Agencies pursuant to this law and other information pertaining to the interest of the public.

'Public agency' is given a wide definition,[151] extending access rights to parts of the private sector including state-funded bodies and many NGOs:

> Public Agency means an executive, legislative, judicative and other agencies whose function and main duties are related to the organizing of the state, where part or all of its funds originate from the state budget and/or the regional budget, or a non-governmental organizations that part or all of its fund originate from the state budget and/or the regional budget, the contribution from the people and/or from overseas sources.

The Law attempts to protect personal data from disclosure to third parties by providing that access to 'classified information' may be refused by a public agency on various grounds (most unrelated to privacy protection) but including 'information relating to personal rights'.[152] Article 17(h) (in Chapter V 'Classified Information') elaborates that the exceptions to access include among others:

> (h) information that, if disclosed and supplied to the Public Information Applicant, may reveal a personal secret, ie.
>
> 1. the history and condition of a member of the family;
> 2. the history, condition and care, physical medical treatment, and physic of an individual;
> 3. the financial condition, assets, income and bank account of an individual;
> **(p.383)** 4. evaluation results of the capability, intellectuality and recommendations on the capability of an individual; and/or
> 5. personal notes of an individual pertaining to his/her formal education and non-formal education activities.

This 'privacy exception' to access is very specific, and not balanced by any public interest test. There are other exceptions in Article 17 that may also in some cases protect privacy interests.[153] Although such information is exempt from disclosure, an exception is made where 'the party whose

secret is disclosed gives his/her approval in writing',[154] so this cannot be used to block individuals from obtaining access to their own records.

The Law establishes an 'Information Committee' as 'an independent institute that functions to implement this Law and its implementing regulations, to provide the standard technical directives of public information services and to settle Public Information Disputes by Mediation and/or non-litigation Adjudication'.[155] It consists of the Central Information Committee of seven members 'who reflect elements of the government and elements of the society' and similar five-person committees in each province, and 'if required' committees at municipal or district level.[156] Where provincial committees have not been formed, the Central Information Committee takes their role.[157]

The duties of the Central Information Committee is to '(a) to receive, check and decide on a request for the settlement of a Public Information Dispute through Mediation and/or non-litigation Adjudication; (b) to determine the general policy of the Public Information service; and (c) to determine the implementing directives and the technical directives'. Provincial committees only have the first function. The Central Information Committee is therefore the implementing agency for the Law. Detailed procedures are set out for settlement of disputes concerning access in Chapter IX of the Law, including rights of appeal to the courts,[158] and ultimately to the Supreme Court.[159]

The Law does not include a right to correction of incorrect personal data. However, it does establish a number of offences punishable by prison sentences or fines, which may indirectly protect privacy interests. Offences include: where an individual 'deliberately uses Public Information against the law';[160] where a public agency 'deliberately ignores [fails] to supply, give and/or publish' public information, including 'on the basis of a request' and that failure 'results in a loss to others';[161] where an individual 'deliberately and against the law demolishes, destroys and/or loses Public Information documents of any form of media that is protected by the state and/or is related to the interest of the public';[162] and where an individual 'deliberately and with no right accesses and/or acquires and/or supplies information that is classified', including under article 17(h) concerning personal information. The procedures for compensation payments by public agencies (relevant to article 52) are to be included in regulations which, at the time of writing, have not yet been published.[163]

(p.384) The implementation of the Law has been criticized as not yet very effective. Napu,[164] in a 2012 study, notes that although the Central Information Committee was established in 2009, only 8 of 33 provinces had appointed provincial committees despite the law requiring them to do so by 2010;[165] that the Indonesian people are still not accustomed to asking for information that is important to them, even if they have the right to do so; and public officials had not adjusted to the new procedures required of them. Supreme Court decisions have been required to force agencies to disclose information, and even then disclosure has been delayed for months.[166]

Other legislation

Other laws providing some privacy protection are the Health Law (No. 36/2009), providing that health information should not be disclosed without the patient's written permission. The Banking Law (No. 10/1998) and regulations, provide similarly in relation to bank disclosure of consumer data. However, it is claimed that these provisions have not been implemented, and databases of credit information are bought and sold freely.[167]

3.4. Law and Regulation on Electronic Information and Transaction

The Government of the Republic of Indonesia has issued implementing legislation[168] as required

by the Information and Electronic Transactions Law (No. 11 of 2008) in the form of the Regulation on the Operation of Electronic Systems and Transactions (No. 82 of 2012).[169] The Regulation is complex, including 90 articles dealing with 7 of the 9 other issues relating to electronic transactions which require regulations to be made under the law,[170] ranging from electronic signatures to domain names. As a government regulation, this is the second-highest form of legislation in Indonesia, under a law (Undang-Undang)[171] and above regulations made by a ministry or agency.

Until now, the Information and Electronic Transactions Law 2008 has only provided a very broad right to compensation for misuse of personal data by electronic media. Article 26 provides that:

> (1) Unless provided otherwise by Rules, use of any information through electronic media that involves personal data of a Person must be made with the consent of the Person concerned.
>
> (2) Any Person whose rights are infringed as intended by paragraph (1) may lodge a claim for damages incurred under this Law.

(p.385) The restriction of scope to uses 'by means of electronic media' also applies to the Regulation. Under Indonesian law, the 'Elucidation' (or Explanatory Statement) that accompanies a Law is part of the law.[172] The Elucidation of article 26 is brief, stating that:[173]

> In the utilization of Information Technology, personal data shall be a part of the privacy rights to be protected. Privacy rights shall contain the following meaning:
>
> a. A privacy right shall be the right to enjoy personal life and be free from any invasion.
>
> b. A privacy right shall be the right to communicate with other Persons without surveillance.
>
> c. A privacy right shall be the right to inspect access to information about personal life of and data on individuals.

Item (c) implies that data subjects have the right to access personal data held on them. No equivalent right to correct personal data is provided, here or elsewhere, but there are references in the Regulation to the obligation of Electronic Service Operators to maintain the 'integrity' or 'authenticity' of personal data,[174] so a right of correction may be implied.

Article 26 of the 2008 Law is the only law that that explicitly mentions privacy. Its terms, including in the Elucidation, are very broad and unclear. It does not specify whether it applies to both public and private sectors, so that and other aspects of the scope of its coverage (including the significance of the three matters mentioned in the Elucidation) are up to the courts to interpret. But it is a key provision because it gives aggrieved persons an opportunity for the use of personal data to be tested in court.

More specific requirements for the management of electronic personal data are now stipulated through the Electronic Transactions Regulation. Article 15[175] is the key data protection provision, stating that the obligations of an electronic system operator are:

> (i) To ensure the 'secrecy, integrity, and availability' of personal data.
> (ii) To ensure that the 'acquisition, use, and utilization' of personal data is based on the consent of the personal data owner, unless otherwise provided by laws and regulations.
> (iii) To ensure that the use or disclosure of the personal data is based on the consent of the data subject and is in accordance with the purpose of acquisition, which was disclosed to

> the owner of the personal data at the time of data acquisition.[176]

The scope of the Regulation

The definition of 'personal data' in the Regulation is that personal data is data about specific individuals that is stored, treated, and guarded so as to protect the truth and the confidentiality of the data,[177] although various translations differ in their precise wording.[178] The **(p.386)** definition is different from standard definitions because of what appears to be a limitation to data 'that is stored, treated, and guarded so as to protect the truth and the confidentiality of the data', but it is unclear whether this really is a limitation. The BSA website offers a broad interpretation that '"Personal data" is not limited to information that by itself enables the identification of individuals and is broadly defined under the regulation as any information of individuals that is kept, stored, and protected as confidential information'.[179]

Neither article 26, nor the Regulation, are limited in their terms to some specific sector, and may apply to both the private and public sectors, although this is not completely clear. However, the Regulation only applies to an 'electronic system operator' (ESO) which is defined in the Regulation to mean 'any person, state agency, business entity, and community that provide, manage, and/or operate electronic system individually or jointly to electronic system user for its interest or other party's interest',[180] although translations vary slightly.[181] The key point here is that an ESO within the meaning of the Regulation may include public sector operators as well as those in the private sector, and non-profit organizations as well as business entities. So the scope of the Regulation is as broad as the 2008 Law. The Regulation does not distinguish between data controllers and data processors: both are ESOs. For an ASEAN country, this is a broad scope.

Data breach notification required

The Regulation has added a data breach notification requirement. Article 15(2) states that, in the event of a failure in the protection of confidential personal data they manage, the ESO shall notify this in writing to the owner of personal data. Article 15(3) states that this will be further regulated in the form of ministry regulations. Article 17 also requires notification to be made to the relevant regulatory agency where failures or disruptions caused by a third party have serious effects.

Enforcement

Breaches of article 15.1, and various other articles, are subject to administrative sanctions, which can include warnings, an 'administrative fee' (a fine), or temporary or permanent suspension of the service.[182] However, such sanctions do not eliminate civil or criminal liability,[183] such as the right to sue for compensation under article 26 of the 2008 Law. The 2008 Law does not provide criminal penalties for breaches of article 26, but does provide such penalties for various 'computer crime' activities which may involve personal data. Law firm commentators note that compensation may also be available under the Indonesian Civil Code:[184]

> **(p.387)** This is based on the general law of tort under Article 1365 of the Indonesian Civil Code and allows an aggrieved data subject to claim damages for actual loss suffered by the data subject where that loss is caused by an unlawful act of an electronic system operator. In this context, the term 'unlawful act' is interpreted broadly, including not only violations of statutory law, but also violations of public morals or the duty of care owed to other persons' interests. There is no clear definition in Indonesian law on what violates 'public morals' or 'duty of care'. The meaning of these terms varies over time and in different places.

A short enforceable privacy code?

In addition to article 15, other aspects of the Regulation are relevant to data protection: openness

of system operations is required, and can be specified further by ministerial and other regulations;[185] an ESO must provide an audit trail, which can be used in enforcement and dispute resolution;[186] it must provide a 'security system' to 'prevent and solve the threats and attacks that cause disruption, failure and loss';[187] it must 'maintain the confidentiality, integrity, authenticity, accessibility, availability and traceability' of information and documents 'in accordance with the provisions of the regulation',[188] which in this context means the 2008 law (Undang-Undang).

One of the most controversial provisions of the Regulation, particularly in light of its possible effects on cloud computing services, is the requirement on an ESO to locate 'the data center and disaster recovery center in Indonesian territory'.[189]

We could therefore conclude that article 15 of the Regulation, coupled with article 26 of the 2008 Law, and various other provisions in the Regulation, provide between them most of the elements of a brief data protection code, enforceable through court actions. These elements include notice of purpose at time of collection; consent to the use disclosed; limits on use and disclosure to the purpose disclosed; a right of access (and possibly correction); obligations on ESOs to maintain 'integrity' and security of personal data; and (in addition) to notify data breaches.

If Indonesia becomes interested in APEC's Cross-border Privacy Rules (CBPR) system, when and if it becomes functional, the provisions in Chapter VII of the Regulation concerning 'Reliability Certification Agencies' may become relevant, because their certificates can concern item (e) (i.e. 'safeguard on the confidentiality of personal data').[190]

3.5. Proposed comprehensive data privacy law

A draft Personal Data Bill was prepared in 2008 under the Ministry of Administrative Reform, but the full contents were not made public and it has not proceeded further. It was a comprehensive Bill covering both public and private sectors, influenced by the OECD Guidelines and other international instruments, and creating an independent national Privacy Commissioner.[191] This ministry is also responsible for the Freedom of Information Act of 2008, and the two responsibilities may have been seen as inconsistent. The Ministry of Communication and Information will now take the lead role to draft a Personal Data **(p.388)** Bill, as part of its 2014 Program. In accordance with Indonesian practice[192] the government will prepare an academic draft first (planned for 2014), to be followed by the government draft.

Pressures for development of a comprehensive law include: the launching of the national Electronic Identity Card Program, which has caused public concern; the international demands of partners of Indonesia in economic cooperation, including those in ASEAN and APEC; a desire to further Indonesia's strategic position on international trade including e-commerce;[193] and human rights considerations, which are seen as an increasingly important factor. In addition, the constitutional cases, which have decided that there is an implied constitutional right of privacy, may affect both the government's obligations to enact data protection laws, and the interpretation of any laws so enacted. Whether the new Indonesian draft Bill will comprehensively cover the both public and private sectors will be a very important question for the development of data privacy laws in the ASEAN region, and for the strengthening of democracy in Indonesia. Privacy issues in Indonesia go well beyond e-commerce.

Notes:

([1]) For background see Peter Church, ch. 11 'Vietnam' in *A Short History of South-East Asia* (5th Edn., John Wiley and Sons, 2009); Bill Hayton, *Vietnam—Rising Dragon* (Yale University Press,

2010). For readily accessible current statistics, see the 'Vietnam' pages of both the CIA Factbook and Wikipedia.

([2]) Decree No. 52/2013/ND-CP dated 16 May 2013 of the Government on e-commerce (Unofficial translation) <http://luatminhkhue.vn/copyright/decree-no-52-2013-nd-cp-dated-may-16,-2013-of-the-government-on-e-commerce.aspx>.

([3]) It supersedes Decree No. 57/2006/ND-CP dated 9 June 2006 of the Government on e-commerce.

([4]) Church, *A Short History of South-East Asia*, p. 182.

([5]) Vietnam's modern history is covered in digestible depth in Francis Pike, *Empires at War: A Short History of Modern Asia Since World War II* (I B Tauris, 2010), chs. 10, 30, 32, 36, and 57, and p. 724.

([6]) Church, *A Short History of South-East Asia*, p. 197. The previous paragraph is largely drawn from Church, pp. 190–7.

([7]) Patrick Sharbaugh, 'What's Mine is Yours: An Exploratory Study of Online Personal Privacy in the Socialist Republic of Vietnam' in A. Maj (Ed.), *Cyberculture Now: Social and Communication Behaviours on the Web* (Interdisciplinary Press, Oxford, 2013), p. 9.

([8]) Dang Xuan Hop, ch. 6 'Vietnam—The Past 25 Years, the Present and the Future' in E. Ann Black and Gary F. Bell (Eds.), *Law and Legal Institutions of Asia* (Cambridge University Press, 2011), p. 187.

([9]) Hop, ch. 6 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, p. 188.

([10]) See Sharbaugh, 'What's Mine is Yours' in Maj (Ed.), *Cyberculture Now.*

([11]) Hop, ch. 6 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, p. 188. See also Le Thi Hanh, 'Update: Vietnam Legal Research' (GlobaLex, May 2013, updating 1st Edition by Anh Luu) <http://www.nyulawglobal.org/globalex/vietnam1.htm>.

([12]) Law on the Promulgation of Legal Instruments 2008, art. 2.

([13]) Hop, ch. 6 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, p. 189.

([14]) Law on Legal Document Issuance.

([15]) Hop, ch. 6 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, p. 195.

([16]) Hanh, 'Update: Vietnam Legal Research', 'National Assembly'.

([17]) Hop, ch. 6 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, p. 196.

([18]) Hanh, 'Update: Vietnam Legal Research' 'Court system'; Hop, ch. 6 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, pp. 200–1.

([19]) Hop, ch. 6 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, pp. 201–2.

([20]) Hop, ch. 6 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, p. 203 and Hanh,

'Update: Vietnam Legal Research', 'The Communist Party of Vietnam', respectively.

([21]) Hop, ch. 6 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, pp. 207–8.

([22]) Sharbaugh, pt. 3 in Maj (Ed.), *Cyberculture Now.*

([23]) Sharbaugh, pt. 3 in Maj (Ed.), *Cyberculture Now*, pp. 78–9.

([24]) Sharbaugh, pt. 3, in Maj (Ed.), *Cyberculture Now*, p. 79.

([25]) Minh, Duong Hoang, 'Data Privacy and Data Protection in e-Commerce in Vietnam'. PPTs for Paper presented at the Seminar on International Implementation of the APEC Privacy Framework, Lima, Peru, 19–20 February 2008.

([26]) Hayton, *Vietnam—Rising Dragon*.

([27]) Hayton, *Vietnam—Rising Dragon*, p. 73.

([28]) Hayton, *Vietnam—Rising Dragon*, p. 77.

([29]) Hayton, *Vietnam—Rising Dragon*, pp. 68–73.

([30]) Hayton, *Vietnam—Rising Dragon*, p. 77.

([31]) IT Law (Vietnam), art. 20(2): 'Except when requested by competent state agencies, organizations and individuals engaged in information technology application are neither responsible for monitoring or supervising digital information of other organizations and individuals nor for investigating law violations committed in the course of transmitting or storing digital information of other organizations and individuals.' However, 2012 regulations on Internet management do impose some surveillance and reporting obligations on ISPs.

([32]) Sharbaugh, pt. 3, in Maj (Ed.) *Cyberculture Now*, p. 77.

([33]) Constitution of Vietnam (1992) <http://www.na.gov.vn/htx/English/C1479/#u96Ea6fNiK2G>.

([34]) Constitution of Vietnam, art. 71.

([35]) Constitution of Vietnam, art. 73.

([36]) Human Rights Watch, 'Vietnam: Amended Constitution a Missed Opportunity on Rights' (3 December 2013) <http://www.hrw.org/news/2013/12/02/vietnam-amended-constitution-missed-opportunity-rights>.

([37]) For example the 2006 Information Technology Law provides in art. 2: 'When a treaty to which the Socialist Republic of Vietnam is a contracting party contains provisions different from those of this Law, the provisions of that treaty prevail.'

([38]) The Law on Signing, Joining and Implementing International Agreements does not provide any procedures for this.

([39]) Civil Code (Vietnam), art. 38 (Legal Normative Documents, Ministry of Justice, 14 June 2005) <http://vbqppl.moj.gov.vn/vbpq/en/Lists/Vn%20bn%20php%20lut/View_Detail.aspx?ItemID=6595>.

([40]) Tran Manh Hung, Seck Yee Chung, and Quach Minh Tri (Baker & McKenzie Vietnam),

'Company's Right To Monitor Employee Emails Affirmed By Court', 21 September 2012, 12 *World Data Protection Report* p. 31. They cite a Supreme People's Court decision of 4 July 2012.

([41]) Hung et al., 'Company's Right To Monitor Employee Emails'.

([42]) Hung et al., 'Company's Right To Monitor Employee Emails'.

([43]) Civil Code (Vietnam), art. 25.

([44]) Criminal Code (Vietnam), art. 125.

([45]) Paraphrase of N. T. Hai, 'Government Promotes the Development of E-Commerce Applications in Vietnam' (APEC-TEL Workshop, 19–21 June 2002, Bangkok).

([46]) This part is based on Graham Greenleaf, 'Vietnam's 2013 E-Commerce Decree Consolidates Data Privacy Protections' (2013) 125 *Privacy Laws & Business International Report*, pp. 22–5.

([47]) Article 46(2): 'Agencies, organizations and individuals must not use, provide or disclose information on private and personal affairs or information of other agencies, organizations and/or individuals which is accessible by them or under their control in e-transactions without the latter's consent, unless otherwise provided for by law.'

([48]) *Law on information technology* (No. 67/2006/QH11), <http://www.asianlii.org/vn/legis/laws/oit264/oit264.html>.

([49]) IT Law (Vietnam), art. 4.

([50]) IT Law (Vietnam), art. 1.

([51]) IT Law (Vietnam), art. 1.

([52]) IT Law (Vietnam), art. 7(5).

([53]) IT Law (Vietnam), art. 2.

([54]) IT Law (Vietnam), art. 70(3).

([55]) IT Law (Vietnam), art. 70(2).

([56]) IT Law (Vietnam), art. 70(1).

([57]) IT Law (Vietnam), art. 71.

([58]) Article 72(1): 'Organizations' and individuals' lawful personal information which is exchanged, transmitted or stored in the network environment shall be kept confidential in accordance with law.'

([59]) Article 72(2)(e): 'Other acts of causing unsafety to, or disclosing confidentiality of, other organizations' or individuals' information which is exchanged, transmitted or stored in the network environment.'

([60]) *Law on Protection of Consumer's Rights*, 17 November 2010, <http://vbqppl.moj.gov.vn/vbpq/en/Lists/Vn%20bn%20php%20lut/View_Detail.aspx?ItemID=10489>.

([61]) Baker & McKenzie (2011), 'Consumer Protection Law' *Client Alert*, January 2011; Baker & McKenzie (2010) 'Vietnam's New Consumer Protection Law Consolidates Consumer Rights on Protection of Personal Information' *Client Alert*, December 2010.

([62]) Decree No. 52/2013/ND-CP (Vietnam) dated 16 May 2013 of the Government on e-commerce <http://luatminhkhue.vn/copyright/decree-no-52-2013-nd-cp-dated-may-16,-2013-of-the-government-on-e-commerce.aspx>.

([63]) Email communication from My Doan and Christian Schaefer of Hogan Lovells, Ho Chi Minh City.

([64]) Decree No. 52/2013 on e-commerce (Vietnam), art. 3(1).

([65]) Decree No. 52/2013 on e-commerce (Vietnam), art. 3(13).

([66]) Decree No. 52/2013 on e-commerce (Vietnam), art. 3(14).

([67]) Decree No. 52/2013 on e-commerce (Vietnam), art. 2(1).

([68]) Email communication from My Doan and Christian Schaefer of Hogan Lovells, Ho Chi Minh City.

([69]) Decree No. 52/2013 on e-commerce (Vietnam), art. 68(2).

([70]) Decree No. 52/2013 on e-commerce (Vietnam), art. 4(4)(a).

([71]) Decree No. 52/2013 on e-commerce (Vietnam), art. 69.

([72]) Decree No. 52/2013 on e-commerce (Vietnam), art. 69.

([73]) Decree No. 52/2013 on e-commerce (Vietnam), art. 70.

([74]) Decree No. 52/2013 on e-commerce (Vietnam), art. 70(4).

([75]) Decree No. 52/2013 on e-commerce (Vietnam), art. 70(3).

([76]) Decree No. 90 Against Spam (Vietnam) of 2008 requires services sending e-mail marketing to be established in Vietnam; to provide opt-out facilities, and to comply with a considerable number of other regulatory requirements.

([77]) Decree No. 52/2013 on e-commerce (Vietnam), art. 71.

([78]) Decree No. 52/2013 on e-commerce (Vietnam), art.72(1).

([79]) Decree No. 52/2013 on e-commerce (Vietnam), art. 72(3).

([80]) Decree No. 52/2013 on e-commerce (Vietnam), art. 73.

([81]) IT Law (Vietnam), art. 22.

([82]) Decree No. 52/2013 on e-commerce (Vietnam), art. 73(2).

([83]) Decree No. 52/2013 on e-commerce (Vietnam), art. 72(2).

([84]) Decree No. 52/2013 on e-commerce (Vietnam), art. 69(1)(e).

([85]) IT Law (Vietnam), art. 22(3).

([86]) IT Law (Vietnam), art. 77.

([87]) Decree No. 52/2013 on e-commerce (Vietnam), art. 78(3).

([88]) Decree No. 52/2013 on e-commerce (Vietnam), art. 78(1)(h).

([89]) Decree No. 52/2013 on e-commerce (Vietnam), art. 78(4).

([90]) Decree No. 52/2013 on e-commerce (Vietnam), art. 78(5).

([91]) Article 24(1)(d) and (2), Circular No. 12/2013/TT-BCT, 20 June 2013 of the Ministry of Industry and Trade promulgating the regulation on notification, registration and information publication procedures related to e-commerce. The portal is at <www.online.gov.vn>.

([92]) Decree No. 52/2013 on e-commerce (Vietnam), art. 77.

([93]) Article 24(3), Circular No.12/2013/TT-BC.

([94]) IT Law (Vietnam), art. 75(2).

([95]) Decree No. 52/2013 on e-commerce (Vietnam), art. 76(5)(c).

([96]) Consumer Law (Vietnam), ch. 4.

([97]) Consumer Law (Vietnam), art. 30(2).

([98]) Baker & McKenzie, 2011, interpreting art. 11.

([99]) Consumer Law (Vietnam), art. 47(1).

([100]) 'Building Trust in E-Commerce Websites' (Vietnam Economic News, 29 August 2013) <http://ven.vn/building-trust-in-ecommerce-websites_t77c195n38405tn.aspx>. These include TrustVN, NganLuong.vn, and the officially supported SafeWeb, described as 'a Vietnamese representative to join the World Trustmark Alliance'.

([101]) Sharbaugh, pt. 3, in Maj (Ed.), *Cyberculture Now*, p. 75.

([102]) A concise history of modern Indonesia is Church, ch. 4 'Indonesia' in *A Short History of South-East Asia*. An analysis of the competition between elites in the 'New Order' era and its collapse, is Case, ch. 2 'Indonesia: Perpetuating and Changing a Pseudo-democracy' in *Politics in Southeast Asia: Democracy or Less*. For an overview of modern Indonesian history, see Pike, *Empires at War*, chs. 16, 31, 46, and 57, and pp. 716–17.

([103]) A comprehensive account of Indonesian legal developments is Tim Lindsey (Ed.), *Indonesian Law and Society* (2nd Edn., Federation Press, 2008).

([104]) Case, *Politics in Southeast Asia: Democracy or Less*, p. 79.

([105]) Church, *A Short History of South-East Asia*, p. 57. Much of the previous two paragraphs is based on Church, pp. 41–63.

([106]) Church, *A Short History of South-East Asia*, p. 63.

([107]) Gary F. Bell, ch. 8 'Indonesia: The Challenges of Legal Diversity and Law Reform' in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, p. 262.

([108]) Bell, ch. 8 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, pp. 270–1.

([109]) Tim Lindsey and Mas Achmad Santosa, ch. 1 'The Trajectory of Law Reform in Indonesia: A Short Overview of Legal Systems and Change in Indonesia', in Lindsey (Ed.), *Indonesian Law and Society*, p. 3.

([110]) Bell, ch. 8 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, pp. 266–7.

([111]) Tim Lindsey, ch. 2 'Constitutional Reform in Indonesia: Muddling Towards Democracy' in Lindsey (Ed.), *Indonesian Law and Society*, p. 24.

([112]) Lindsey, ch. 2 in Lindsey (Ed.), *Indonesian Law and Society*, p. 45.

([113]) Bell, ch. 8 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, pp. 271–2.

([114]) Bell, ch. 8 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, p. 272.

([115]) Bell, ch. 8 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, p. 272.

([116]) Bell, ch. 8 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, p. 273.

([117]) Bell, ch. 8 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, p. 273.

([118]) Bell, ch. 8 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, p. 275.

([119]) Bell, ch. 8 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, pp. 279–81.

([120]) Bell, ch. 8 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, p. 282.

([121]) Bell, ch. 8 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, p. 287.

([122]) Bell, ch. 8 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, p. 281.

([123]) Simon Butt, '*Surat sakti*: The Decline of the Authority of Judicial Decisions in Indonesia' in Lindsey (Ed.), *Indonesia: Law and Society*, p. 359.

([124]) Lindsey and Santosa, ch. 1 in Lindsey (Ed.), *Indonesia: Law and Society*, p. 21.

([125]) Paul Mah, 'Indonesia Makes Progress on its Ambitious Biometrics National ID Card Project' (TechRepublic, 2 October 2012), no longer available online.

([126]) Mah, 'Indonesia Makes Progress on its Ambitious Biometrics National ID Card Project'.

([127]) 'Indonesian Christian politician: remove religion from national ID cards' (Catholic World News, 6 January 2014), <https://www.catholicculture.org/news/headlines/index.cfm?storyid=20104>.

([128]) Including the family card number, date of birth; description of physical disability and or mental disability; personal information of mother and father (art. 84.1).

([129]) These have included Government Regulation No. 37/2007 and Presidential Regulation No. 35/2010. The Law on Population Administration (Law No. 23 Year 2006) is also relevant.

([130]) Privacy International, *Indonesia Report* (PI, 22 October 2012), <https://www.privacyinternational.org/reports/indonesia/>, section 'II Legal Framework: Constitutional protection for privacy'.

([131]) PI Indonesia Report, 'I Background: Civil Society'.

([132]) This section is derived, with permission, from Sinta Dewi, *Balancing Privacy Rights and Legal Enforcement: Indonesia Practices* (2012) 5 *International Journal of Liability and Scientific Enquiry*, pp. 238–9.

([133]) Case Number 5/PUU/2010.

([134]) Case no. 006/PUU-I/2003.

([135]) Case no. 012-016-019/PUU-IV/2006.

([136]) Law No. 39 of 1999 concerning Human Rights (UU 39/1999).

([137]) Human Rights Law 1999 (Indonesia), art. 30 provides: '(1) No one shall be subject to arbitrary interference with his home. (2) No one shall set foot in or enter the enclosure of a house or enter a house without the permission of the person who lives there, except for reasons provided for under prevailing legislation.' Article 31 provides: 'No one shall be subject to arbitrary interference with his correspondence, including electronic communications, except upon the order of a court or other legitimate authority according to prevailing legislation.'

([138]) UU 39/1999 establishes the Commission (art. 75), gives it a function to mediate human rights issues (art. 76), and authorizes it to arbitrate and mediate (art. 89), with procedures for complaints and mediation (arts. 90–96), including legally binding mediation settlements (art. 96). The Law also provides for establishment of a Human Rights Tribunal in cases of 'gross violations of human rights' (art. 104), but it has not yet been established.

([139]) By-Law No. 12 of 2005.

([140]) See also UU39/1999, art. 67: 'Everyone within the territory of the Republic of Indonesia is required to comply with Indonesian legislation and Indonesian Law, including unwritten law and international law concerning human rights ratified by Indonesia.' Article 71: 'The government shall respect, protect, uphold and promote human rights as laid down in this Act, other legislation, and international law concerning human rights ratified by the Republic of Indonesia.' Article 72: 'The duties and responsibilities of the government as referred to in Article 71, include measures towards effective implementation in law, politics, economics, social and cultural aspects, state security, and other areas.'

([141]) Human Rights Law 1999 (Indonesia), art. 89(3)(b).

([142]) Human Rights Law 1999 (Indonesia), art. 96. See Jeff Herbert, ch. 21 'The Legal Framework of Human Rights in Indonesia' in Lindsey (Ed.), *Indonesia: Law and Society*, pp. 460–3.

([143]) Human Rights Court Act (No. 26/2000).

([144]) Herbert, ch. 21 in Lindsey (Ed.), *Indonesia: Law and Society*, pp. 466–7.

([145]) PI Indonesia Report, 'I: Background'.

([146]) Public Information Disclosure Law (No 14 of 2008) (World Bank, 2014) <http://publicofficialsfinancialdisclosure.worldbank.org/?keyword=indonesia&submit=Search#searchlibrary>.

([147]) Public Information Disclosure Law (Indonesia), art. 4(2).

([148]) Public Information Disclosure Law (Indonesia), art. 4(3).

([149]) Public Information Disclosure Law (Indonesia), art. 4(4).

([150]) Public Information Disclosure Law (Indonesia), art. 1.

([151]) Public Information Disclosure Law (Indonesia), art. 1.

([152]) Public Information Disclosure Law (Indonesia), arts. 6(1) and 6(3)(c).

([153]) These include: '(g) Information that, if disclosed, may reveal the contents of an authentic personal deed and the last will or testament of an individual; (i) The memorandum or letters between the public agencies or among the public agencies that, based on their nature are confidential, except the decision of the Information Committee or the court; (j) Information that may not be disclosed under the law.'

([154]) Public Information Disclosure Law (Indonesia), art. 18(2).

([155]) Public Information Disclosure Law (Indonesia), art. 23.

([156]) Public Information Disclosure Law (Indonesia), arts. 24, 25.

([157]) Public Information Disclosure Law (Indonesia), art. 26(2)(b).

([158]) Public Information Disclosure Law (Indonesia), art. 47.

([159]) Public Information Disclosure Law (Indonesia), art. 50.

([160]) Public Information Disclosure Law (Indonesia), art. 51.

([161]) Public Information Disclosure Law (Indonesia), art. 52.

([162]) Public Information Disclosure Law (Indonesia), art. 53.

([163]) Public Information Disclosure Law (Indonesia), art. 61.

([164]) M.H. Napu, 'Towards a Better Regulation of Indonesia's Public Access to Information' (Master's Thesis, Tilburg University, December 2011) <http://arno.uvt.nl/show.cgi?fid=121581>.

([165]) Public Information Disclosure Law (Indonesia), art. 59.

([166]) Napu, 'Towards a Better Regulation of Indonesia's Public Access to Information', p. 24, citing a decision involving the Ministry of Health, two other agencies, and a university.

([167]) PI Indonesia Report, 'IV Privacy Issues'.

([168]) This section is based in part on Graham Greenleaf and Sinta Dewi Rosadi, 'Indonesia's Data Protection Regulation 2012: A Brief Code with Data Breach Notification' (2013) 122 *Privacy Laws &*

Business International Report, pp. 24–7.

([169]) 'Regulation of the Government of the Republic of Indonesia Number 82 of 2012 Concerning Electronic System and Transaction Operation' unofficial government English translation, <http://rulebook-jica.ekon.go.id/english/4902_PP_82_2012_e.html>.

([170]) In addition to data protection, it governs (i) the provision of electronic systems, (ii) electronic agent organizers/operator, (iii) provision of electronic transactions, (iv) electronic signature, (v) provision of electronic certification organization, (vi) trust mark certification body, and (vii) management of domain name.

([171]) See Bell, ch. 8 in Black and Bell (Eds.), *Law and Legal Institutions of Asia*, p. 275.

([172]) Widyawan & Partners, 'Indonesia' (Linklaters 'Data Protected') <https://clientsites.linklaters.com/Clients/dataprotected/Pages/Indonesia.aspx>.

([173]) Unofficial government translation of *Elucidation of Law of the Republic of Indonesia Number 11 of 2008 Concerning Electronic Information and Transactions*, <http://www.flevin.com/id/lgso/translations/JICA%20Mirror/english/4846_UU_11_2008_e_Eluc.html>.

([174]) Electronic Transactions Regulations 2012, arts. 15, 2.

([175]) The following paraphrase of art. 15 is based on the translation by Sinta Dewi, and differs in some terms from the unofficial government translation above, to give more clarity.

([176]) The wording in the unofficial government translation of Regulation is 'in accordance with the purpose of being delivered to the owner of Personal Data on the data acquisition'.

([177]) Electronic Transactions Regulations 2012, art. 1.27.

([178]) The unofficial government translation is 'Personal Data is specific individual data are stored, treated, and keep on the truth and confidentiality is protected'. Widyawan & Partners, 'Indonesia data protection commentary' provides a different translation: 'Article 1.27 of GR 82 defines personal data as the data of individuals that is stored and maintained, the truthfulness of which is maintained and the secrecy of which is protected.'

([179]) 2013 BSA Global Cloud Computing Scorecard 'Country Report and Scorecard for Indonesia' (Business Software Alliance, 2013) <http://cloudscorecard.bsa.org/2013/assets/.../Country_Report_Indonesia.pdf>.

([180]) Electronic Transactions Regulations 2012, art. 1.4.

([181]) Unofficial government translation of Regulation. An alternative translation of the definition as 'any person, state official, business entity or society that provides, manages and/or operates, jointly or singly, an electronic system for the users of the electronic system for the operator's interest and/or others' is from Widyawan & Partners 'Indonesia data protection commentary'.

([182]) Electronic Transactions Regulations 2012, art. 84.

([183]) Electronic Transactions Regulations 2012, art. 84.5.

([184]) Widyawan & Partners, 'Indonesia data protection commentary' <http://www.wnplaw.com/english/pubs/articles.htm>; see also Widyawan & Partners, 'Indonesia' in

Data Protected (Linklaters) <https://clientsites.linklaters.com/Clients/dataprotected/Pages/Indonesia.aspx>.

([185]) Electronic Transactions Regulations 2012, art. 16.

([186]) Electronic Transactions Regulations 2012, art. 18.

([187]) Electronic Transactions Regulations 2012, art. 20.

([188]) Electronic Transactions Regulations 2012, art. 22.

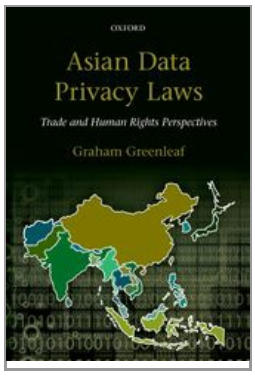
([189]) Electronic Transactions Regulations 2012, art. 17.

([190]) Electronic Transactions Regulations 2012, art. 68.

([191]) Sinta Dewi, 'Indonesia's Plans for Privacy Law' (2009) 92 *Privacy Laws & Business International Newsletter*, p. 17.

([192]) Law on the Procedures to Draft Regulations, Law 12 year 2011.

([193]) H.E. Palupi, 'Privacy and Data Protection: Indonesia Legal Framework' (Thesis, University of Tilburg, 2011), p. 40.



Asian Data Privacy Laws: Trade & Human Rights Perspectives
Graham Greenleaf

Print publication date: 2014
Print ISBN-13: 9780199679669
Published to Oxford Scholarship Online: December 2014
DOI: 10.1093/acprof:oso/9780199679669.001.0001

Privacy in the Other Five Southeast Asian (ASEAN) States

Graham Greenleaf

DOI:10.1093/acprof:oso/9780199679669.003.0014

[–] Abstract and Keywords

This chapter explains the limited progress toward data privacy laws that has so far occurred in the ASEAN (South-East Asia) member countries of Myanmar, Cambodia, Laos, and Brunei, and in the ASEAN candidate member Timor Leste. In some of these countries there are constitutional or other privacy protections worth noting, such as e-commerce, human rights or ombudsman laws, or the early stages of proposals for data privacy legislation. The chapter outlines such privacy protections as do exist in these five countries, and provides a brief background to the political and legal systems of each country within which future data privacy developments will take place. There are occasional surprising developments, such as the specific constitutional protection of personal information in the Constitution of Timor Leste.

Keywords: data protection, privacy, Asia, Myanmar, Cambodia, Laos, Brunei, Timor Leste, ASEAN

1. Limited developments in the other five ASEAN countries

The three previous chapters have dealt with six Association of Southeast Asian Nations (ASEAN) member countries that have to some extent moved toward the development of data privacy laws, although in most cases only in relation to their private sectors. Singapore and Malaysia have legislated in relation to their private sectors and appointed a data protection authority (DPA); the Philippines has enacted legislation but not yet appointed a DPA to administer it; Vietnam and Indonesia have data privacy laws in their e-commerce sectors; and Thailand has an existing but incomplete and ineffective public sector law and a Bill before its legislature for the private sector. Only the as yet inoperative law in the Philippines applies a full set of privacy principles to the public sector.

No such major developments of data privacy laws have yet occurred in the remaining ASEAN member countries of Myanmar, Cambodia, Laos, or Brunei, or in the ASEAN candidate member Timor Leste. However, in some of these countries there are constitutional or other privacy protections worth noting, or the early stages of proposals for legislation. Whether there will be any significant developments by 2015, in line with the ASEAN goal of stronger privacy protection (see Chapter 2, section 2.1) seems unlikely. Of the five countries covered in this chapter, only Timor Leste is a full democracy, and it is unlikely that in the other countries concerned that any data privacy laws, when and if they are enacted, will extend to the public sector, given the precedents established in their **(p.390)** ASEAN neighbours Singapore, Malaysia, Vietnam, and (as yet) Indonesia. The

purpose of this chapter is therefore to outline such privacy protections as do exist in these five countries, and to provide brief background to the political and legal systems of each country within which future data privacy developments will take place.

2. Brunei

Brunei is one of the world's few remaining absolute monarchies. It was a protectorate of Great Britain from 1888, and in 1905 became a Residency, The Sultan was head of state but bound to take advice from the British Resident on all matters except those dealing with Islam, so 'for all practical purposes' it was a colony. Japanese occupation during World War II led to negotiations which gave Brunei self-rule from 1959, with Britain retaining control over defence, foreign affairs, and internal affairs. The Constitution was progressively amended until Brunei gained full independence in 1984.[1]

Brunei is an Islamic state, and since independence has an official ideology known as *Melayu Islam Beraja* (MIB), or Malay Islamic Monarchy. A Religious Council advises the Sultan on matters relating to Islam. MIB was described by the Sultan in 1984 as 'a concept which upholds Islamic principles and values based on the Quran and *Hadith* as the basis of all activities'.[2] Since then, the centrality of MIB in Brunei's history has resulted in Islamic legal institutions becoming more significant than common law institutions.[3] Although it has a small population of about 400,000, of whom Malays make up about 64 per cent, it has per capita income around US$27,000, the highest in Southeast Asia. This is because of huge oil and gas reserves under its land and territorial waters. The country now has a considerable educated middle class, but about 70 per cent of the workforce are state employees.[4]

2.1. Political and legal system of Brunei

Brunei's Constitution (1959, with significant amendments in 1971, 1984, and 2006) makes the Sultan the head of state, with full executive powers and the ability to legislate by decree. It gives the Sultan sole power to add to, or amend, the Constitution.[5] An appointed nine-member Council of Ministers, headed by the Sultan as Prime Minister, carries out the functions of government. The 1959 Constitution, when Brunei was still a British Protectorate, provided for an elected Legislative Council, but shortly after the only election yet held, the Council was dissolved by the Sultan. A pro-democratic party opposing the monarchy, and supporting Brunei's inclusion in the proposed Federation of Malaysia, had won the election. When its demands were rejected it staged a revolt which was suppressed by British Gurka troops. The Sultan declared a state of emergency, which is still theoretically in force. In 1970 the Council was changed to an appointed council, currently with 36 members, which only has consultative powers. In 2004 the Sultan announced that the next Legislative Council would have 15 elected members, but no elections have subsequently been held.[6] In addition to being a non-democratic state, Brunei has also abolished judicial review of administrative actions, the Sultan's powers of **(p.391)** appointment and dismissal are unfettered, and there are very restrictive laws concerning criticism of the royal family.[7]

Brunei has had a dual legal system since 1906 when English common law and equity were

introduced. English common law is still the predominant legal system, but with significant codification. The 1951 Application of Laws Act provided that English common law and equity, and statutes of general application, as at 1951, would apply in Brunei, but only to the extent appropriate to local circumstances. English precedents since 1951, while not binding on Brunei's courts, still hold highly persuasive authority, and decisions of courts in other common law jurisdictions are also cited regularly.[8]

A three-tiered legal system is headed by a High Court of three members, with two Intermediate Courts and, at the lowest rung, 10 Magistrates' Courts. A previous limited right of appeal to the UK Privy Council in civil cases has been removed.[9] Separate Shariah courts deal mainly in Muslim divorce, ancillary matters and related sexual offences, with their own final Court of Appeal from one level of lower courts. Islamic law in Brunei has incorporated elements of Malay *adat* (customary law), and so is distinctive from Islamic law in other regions. All judicial offices are appointed by the Sultan as Prime Minister.[10] Brunei's common law courts 'have maintained a high level of public confidence in respect of efficiency and judicial independence'.[11]

State surveillance and ID system in Brunei

Brunei has had an ID card since 1965, required by citizens, residents, and visitors of over three months. It is chip-based, must be produced as required by various officials, and includes a photo, fingerprints, and the person's blood type. A person's race must be provided at registration.[12]

2.2. No privacy rights or binding commitments

Brunei's Constitution does not recognize any constitutional rights of citizens, let alone a right of privacy. Such rights would be inconsistent with the Sultan's unrestricted right to legislate. Nor have Brunei's courts recognized a right of privacy at common law, or the extended meaning of 'breach of confidence' which protects information of a confidential nature per se. Neither of these approaches had been developed by UK courts in 1951, although it is still possible that Brunei's courts could do either. Since 1951 UK courts have rejected the former and embraced the latter, however, Brunei is not bound by their approach, and (for example) the courts of New Zealand have taken the opposite approach in both cases.

Brunei has no binding international commitments concerning privacy. It is not a party to the International Covenant on Civil and Political Rights 1966 (ICCPR). Brunei is a member of the Asia-Pacific Economic Cooperation (APEC) and ASEAN (since 1987) but those engagements do not result in any binding commitments concerning privacy. It has had some involvement in the APEC Privacy Framework developments since their inception in 2003, but has kept a low profile.

(p.392) Brunei's Computer Misuse Order 2000 (revised 2007) may provide some incidental data privacy protections for such matters as unauthorized access to, or modification of computer resources. It also enacted an Electronic Transactions Act in 2004 (revised 2008), and introduced a Consumer Protection (Fair Trading) Order 2011

(CPFTO), but neither deal directly with data privacy issues.[13]

2.3. Future possibilities

The 2013 UNCTAD report[14] on e-commerce in ASEAN is ambivalent about whether Brunei will develop data privacy legislation, but considers it a possibility:

> Brunei Darussalam has taken a very strong interest in the development of privacy legislation. A National Data Protection Policy has been drafted and is currently being reviewed by relevant stakeholders and this may in turn form the basis for the drafting of legislation.
>
> The concept of privacy is challenging in Brunei Darussalam. There is no omnibus legislation providing protection for privacy. Such legislation is found in industry specific laws such as the Banking Act and the Tabung Amanah Pekerja Act. The introduction of data protection on the premise of privacy protection therefore has its challenges. However, the Government has been studying models in Malaysia and Singapore, and will be monitoring carefully the implementation of similar laws in those jurisdictions.

The most likely influences toward Brunei enacting data privacy legislation are its ASEAN commitments, the fact that its neighbours (Malaysia, Singapore, the Philippines, and possibly Thailand) are doing so, and its involvement in APEC. There is a strong history of Brunei adopting Singapore an laws as drafts or templates, including in IT-related laws. Brunei reported to the January 2012 APEC privacy sub-group meeting that the government is considering development of data privacy legislation for both the public and private sectors. The inclusion of the public sector in a data privacy law would set Brunei's legislation apart from its Malaysian and Singaporean neighbours. How privacy rights against government can be reconciled with an absolute monarchy remains to be seen. There is also the possibility, as mentioned earlier, that its common law courts might adopt a tortious right of privacy or, more likely, might extend protection of personal information through the law of breach of confidence.

3. Cambodia

Cambodia has no significant data privacy protections at present, nor any under development.

3.1. Cambodia—historical and political context

After the great age of the Angkor kingdoms from the ninth to the fourteenth centuries, the kingdom of Cambodia was one of a number of competing Indo-Chinese states until the colonial era. The French, following their colonization of Saigon (Vietnam), saw the Mekong River which passes primarily through Cambodia as a key potential trade route, and established a protectorate relationship in 1863 with Cambodia, in return for defending **(p.393)** it from its neighbours. French colonialism did little to develop Cambodia from subsistence rice agriculture for almost a century.[15]

A brief account of Cambodia's tragic but complex post-World War II history is necessary

for an understanding of its current position.[16] In 1953 then King Sihanouk convinced France, at that time exhausted from the war in Vietnam, to grant independence to Cambodia. He subsequently abdicated and won the first post-independence election, probably unfairly. During his next two decades of autocratic rule, Cambodia remained economically stagnant, but secretly allowed the North Vietnamese and Viet Cong to establish a supply route through Cambodian territory. He was replaced by an American-allied government in 1970, but its losses to the Vietnamese and US bombing of the Cambodian countryside (with consequent resentment toward the cities) contributed to the catastrophe that followed. The Khmer Rouge ('red Khmer') insurgents from the countryside took power in 1975 and forcefully evacuated a significant proportion of the population from the cities. All Cambodians were required to become farmers on collectives, and money, trade, books, education, and Buddhism were all proscribed. 'Former upper- and middle-class people, former government employees, most professionals and most educated people were treated as expendable labour.'[17] An estimated 500,000 Cambodians had died during the 1970–1975 war, and a further one million died at the hands of the Khmer Rouge from 1975–1979. Vietnam invaded Cambodia, following provocations, in December 1978 and the Khmer Rouge retreated to the countryside. The Vietnamese troops installed a new Cambodian government mainly consisting of former Cambodian communists who had fled the purges. Vietnam withdrew its troops in 1989, and its client government, now led by Hun Sen, became the State of Cambodia (SOC), and espoused a market economy, as Vietnam and China were doing at the same time.

The new Cambodian regime was still excluded from many aspects of international affairs (ostensibly because of its establishment by Vietnam), but this was finally resolved by the 1991 Paris Conference by which a coalition government was established. The Sihanouk-supported FUNCINPEC was the main coalition partner, but it also including the Khmer Rouge. Elections supervised by UNTAC (United Nations Transitional Authority in Cambodia) followed in 1993, resulting in a continuation of coalition government. Subsequent elections resulting in victories for Hun Sen's Cambodian People's Party (CCP) in 1998, 2003, 2008, and 2013 have extended his rule beyond 28 years. Although these elections have been considered relatively free and fair, Hun Sen 'has been accused by human rights observers and opposition parties of supporting increased repression against protestors, critics and members of rival political parties'.[18] The 2013 official election results have resulted in mass protests and claims of election rigging. As a country which has never changed governments though elections, Cambodia can at best be considered a quasi-democracy.

Twenty-first-century Cambodia is still a post-conflict and post-totalitarian society within the memory of much of its population. Trials for crimes against humanity by the Khmer Rouge leaders have been continuing since 2001 in a fitful manner, and with few convictions resulting. Cambodia has had to recover from an extreme degree of destruction of its social institutions and human capital which occurred less than 40 years ago. Other **(p.394)** countries such as South Korea or Taiwan have been far more successful in recovering from authoritarian regimes, but those regimes, or the resulting

task of recovery, cannot be compared with the Khmer Rouge. The fragility of its current democratic institutions, combined with the extent of previous destruction of its social institutions, makes Cambodia an inhospitable location for development of legal rights such as data privacy.

State surveillance and ID systems in Cambodia

Cambodia has Khmer National Identity Cards, which have 10-year validity and are issued to persons over 18.[19] Since 1998 new plastic cards have been issued with storage sufficient for a photograph, fingerprints, and demographic data.[20]

3.2. Legal system of Cambodia

Cambodia's previous legal system, based largely on French civil law, was destroyed during the 1975–79 Khmer Rouge period, along with virtually all institutions including the courts. No laws were enacted, and few legal professionals survived. Re-establishment of Cambodia's legal system 'from scratch' since the 1980s has been a long process, which is still incomplete.[21] Cambodia is now a constitutional monarchy with the king as head of state. The government head is the Prime Minister, and legislative power is vested in a bicameral parliament, with five-yearly elections. Pre-1975 legislation remains valid, subject to consistency with the Constitution. There is a constitutional separation of executive, legislative, and judicial powers. The Constitutional Council is responsible for interpreting the Constitution, at the request of other branches of government. The judicial system consists of courts of first instance, the Appeal Court, and the Supreme Court. There is continuing internal and external criticism that the judicial system is periodically misused against political opponents of the government.[22]

3.3. Lack of existing privacy protections or international commitments

Cambodia is a member of ASEAN (since 1995) and the World Trade Organization (WTO) (since 2004), both of which have encouraged its development of e-commerce laws. It is not a member of APEC, and is therefore not participating in the development of APEC's Cross-Border Privacy Rules. Cambodia is a party to the ICCPR, and signed the ICCPR Optional Protocol in 2004, but has not ratified it, so Cambodian citizens cannot make complaints to the UN Human Rights Committee.

Cambodia's Constitution provides in article 40 that 'The right to privacy of residence and to the secrecy of correspondence by mail, telegram, fax, telex, and telephone shall be guaranteed [and] Any search of the house, material and body shall be in accordance with the law'. The Constitution does not expressly protect the right to information. In January 2013 Cambodia's National Assembly rejected without debate a draft law on freedom of **(p.395)** information proposed by the opposition party, the second time in three years that this has occurred.[23] The second draft of the law by the opposition in 2011 was analysed by the article 19 non-governmental organization (NGO)[24] and praised as a law 'which would make Cambodia the model throughout Southeast Asia'.[25] It has not progressed.

3.4. Future prospects for data privacy legislation

Cambodia does not yet have an e-commerce law but UNCTAD has been supporting the governments of both Cambodia and of the Lao PDR to prepare e-commerce laws and build capacity for them.[26] The 2013 UNCTAD review states that 'the proposed omnibus e-commerce law will include a section on confidentiality that might provide some limited online privacy protection'. In 2012 Cambodia established an independent Telecom Regulator of Cambodia which is expected to have a significant administrative role in any e-commerce law.[27] It seems that this is the highest extent of data privacy law likely to emerge in Cambodia in the near future.

4. Laos

The Lao People's Democratic Republic (Lao PDR) is a landlocked country of over 6 million people, sharing borders with China, Vietnam, Thailand, Burma, and Cambodia. Although the Lao kingdom of Lao Xang had considerable influence for 300 years from the fourteenth century, a further three centuries of domination followed, first by Siam (Thailand) and then France as a colonial power until 1949.[28] There followed three decades of internal political division between left and right forces, occasional coalition governments, and no single force in control of all areas of the country. In 1975, following the wars in Indo-China, the communist Pathet Lao took full control of the government and united the area of the current Lao PDR 'under one indigenous government for the first time in almost 300 years'.[29] They ended a six-century-old monarchy, and most of the royal family died while confined in the late 1980s.[30] The Pathet Lao instituted a doctrinaire socialist regime which was initially closely aligned with Vietnam. There has since been increasing economic liberalization, but not political liberalization, and it is still a one-party Communist state.

4.1. Laos—historical and legal context

The Lao economy is one of the least developed in ASEAN. During the first decade of strict socialist policies under Pathet Lao rule, and facing a Thai blockade, about one-tenth of the population fled to Thailand, including the majority of the country's educated and skilled **(p.396)** people. A gradual, limited return to private enterprise and the liberalization of foreign investment laws began in the mid-1980s. This has been an overall success, resulting in growth averaging 6 per cent per year from 1988–2008.[31] Foreign investment in energy and raw materials industries has been substantial, and infrastructure has improved, but over half the population is still engaged in subsistence farming, and half the population outside the capital lives below the poverty line.[32]

The Lao PDR is a one-party state (Lao People's Revolutionary Party) with other parties proscribed. There is a unicameral National Assembly elected by popular vote from a list of candidates selected by the Lao People's Revolutionary Party to serve five-year terms. The next election is due in 2016. The military still has a very strong influence in government. Little information is available on the extent or mechanisms of data surveillance by the Lao government.

The legal system is based on French civil law. The judges of the People's Supreme Court and lower courts are elected by the National Assembly and its Standing Committee. The

rule of law is still weak and 'Party diktat can override law and institutionalised procedures'.[33]

Internet penetration in Laos was 8.1 per cent of the population, whereas mobile phone penetration was 83 per cent, as at 2010.[34] The Lao PDR national ID card displays the religious affiliation of citizens.[35]

4.2. Lack of existing privacy protections

Existing privacy protections are minimal to non-existent, but this may change, at least in relation to the private sector. Given the nature of the Lao PDR political system, it is unlikely to change in the near future in relation to the state.

The Lao PDR has ratified the ICCPR, but not the Optional Protocol, so it is not possible for Lao citizens to take privacy complaints to the UN Human Rights Committee. Laos has been a member of ASEAN since 1997, but not of APEC, so its privacy developments are likely to be influenced by ASEAN's commitment to stronger privacy protection by 2015, but not by APEC's Cross-border Privacy Rules (CBPR) developments. In 2013 the Lao PDR became a member of the WTO.[36]

The Lao PDR Constitution of 2003 does not provide express or implied protection of privacy interests except for the statement that the 'right of Lao citizens in their bodies, dignities and residences are inviolable'.[37] There is no freedom of information law at the national level. Local government bodies (provincial, city, municipal, and district cabinets) have the obligation[38] 'to provide information'.[39]

(p.397) The Law on Electronic Transactions, developed with support from UNCTAD and other organizations, was enacted in December 2012,[40] but does not contain provisions directly relevant to data privacy. The Law on Telecommunications includes as offences 'using any telecommunication equipment, [or] telecommunication network of their own to connect into frequency waves or any telecommunication equipment or network operated by others to obstruct, interrupt, encroach [on], destroy, modify, erase, tap [into], intercept, steal or retrieve other person's data [and] information'.[41]

According to Lao PDR officials, 'A number of laws are being revised to be stronger and be in line with international standards. New laws need to be introduced to enable future trade initiatives like the electronic transactions law and data protection laws'.[42] Future data privacy protections, if they occur, are likely to be a result of trade initiatives, particularly ASEAN- or WTO-influenced developments. They are unlikely to apply to the Lao PDR government.

5. Myanmar/Burma

Until recently it would have been possible to simply state that there was no data privacy protection in Myanmar, and none likely in the near future under its authoritarian and isolated military government. However, events have moved rapidly since 2011 and are continuing to do so, in favour of democratization, an end to isolation, and rapid economic liberalization and growth. In this context, the development of data privacy laws is no

longer an unrealistic possibility in the medium term. Thus the context in which such a law might emerge requires consideration.

5.1. Myanmar—historical and legal context

The country has officially been known as Myanmar (Republic of the Union of Myanmar) since 1989, but many countries, and its opposition parties, still refer to it by its previous name, Burma. 'Myanmar' will be used here to refer to the current state.

History and political system of Myanmar

Although various kingdoms within the present borders of Myanmar were powerful states in previous centuries, from 1824 the British successively conquered and incorporated them into its colonial empire, culminating in the deposition of King Thibaw in Mandalay in 1886. From then until 1937, Burma (as it was then known) was ruled as a province of India, and from 1937 to independence as a self-governing (but not independent) colony within the British Empire, with a British Governor.[43] Japan invaded Burma shortly after its attack on Pearl Harbor, and was in control by early 1942. By the conclusion of the war in 1945 the position of Britain was sufficiently weakened, that a local leadership headed by Aung San demanded and achieved independence by 1948. His assassination shortly thereafter was **(p.398)** followed by unstable parliamentary democracy, during which Burma had a high international reputation under leaders such as U Thant and U Nu. Forty-five years of stultifying dictatorship commenced in 1962 when General Ne Win staged a military coup and effectively held power until 1988.[44]

Multi-party elections in 1990 resulted in a clear victory for the National League for Democracy (NLD), the main opposition party. However, the military refused to cede power and placed NLD leader Aung San Suu Kyi, daughter of the assassinated independence leader Aung San, under house arrest from 1989 to 2010, except for two periods amounting to six years. Renamed 'Myanmar', the country became an international outcast during that period, with many countries imposing economic sanctions. In 2008 the ruling military junta organized a constitutional referendum. Then in 2010 parliamentary elections under the new 2008 Constitution resulted in the election of the Union Solidarity and Development Party (USDP), dominated by ex-military officers and a government headed by President Thein Sein. In 2012 the NLD was able to contest by-elections, and Aung San Suu Kyi was elected to the legislature. Release of some political prisoners and some further economic and social reforms have resulted in relaxation or lifting of sanctions, and Myanmar's international rehabilitation has continued since 2011 at a rapid pace.[45] Only a few years ago it could be said that '[t]he Burmese civil war is the longest-running armed conflict in the world and has continued, in one form or another, from independence to the present day'.[46] In 2012 some forms of peace agreements were reached with almost all the armed dissident ethnic groups, for the first time.

Myanmar has therefore become much more like many of its Asian neighbours, both internally and in terms of its international relations, during the last few years. Data privacy laws are therefore more likely, both for reasons of trade and for the protection of human

rights.

Legal system of Myanmar

Myanmar was an absolute monarchy, with a legal system dating back to 849, prior to the British colonial occupation being completed.[47] The British established courts from 1886, with the common law as the basis of the legal system, but supplemented by Burmese customary law. Various Indian colonial laws were also in force in Burma.[48] Legislative authority is now vested in the bicameral Pyidaungsu Hluttaw (National Parliament) comprised of the Pyithu Hluttaw (People's Assembly or House of Representatives) and the Amyotha Hluttaw (National Assembly or Senate).[49] The two houses are partly democratically elected and partly appointed from defence personnel.[50]

Following independence from Britain in 1948, it is said that 'Myanmar continues to apply the common law legal system as its basis',[51] and further that:[52]

> **(p.399)** Sources of law in Myanmar comprise of constitutions, legislations, customary law and English common law. English common law rules, developed and adopted in Myanmar case law during the British occupation, are applied where there is absence of local legislation governing a particular matter before the Courts. Moreover, judges are granted discretionary power to decide the matter in accordance with justice, equity and good conscience in the absence of any applicable law.

However, another perspective is that, partly because the courts of Myanmar progressively discontinued the publication of their decisions in English from 1948 to 1968, Myanmar has departed from the common law far more than other countries in Asia with a British colonial history, and has not participated in the development of a shared body of common law principles.[53] Partly as a result 'publications on modern Burmese law have been rare'.[54] The extent to which Myanmar law resembles the law of other common law jurisdictions (in areas not governed by legislation) is therefore difficult to assess.

The post-1948 judicial system, largely inherited from the British, was replaced by a more 'socialist' judicial system in 1962, further reformed in 1974, 1988, and 2000. In 2010 the Union Judiciary Law was enacted to create the current judicial system under the 2008 Constitution.[55] It now consists of a Constitutional Tribunal, the Supreme Court of the Union, High Courts of each Region and State, and a variety of other courts.[56] The nine-member Constitutional Tribunal is appointed in equal parts by the President and the speakers of each house.

The rule of law is still in a state of flux in Myanmar. This was exemplified by the resignation of all judges of the Constitutional Tribunal in September 2012 after they were threatened with impeachment by the legislature over a dispute concerning the Tribunal's ability to limit the powers of the legislature to question Ministers.[57] This resulted in a law of dubious constitutional validity empowering the legislature to overturn some decisions of the Tribunal.[58]

International engagements

Myanmar is a member of ASEAN, and its chair in 2014,[59] a position which is significant for its re-emergence into international respectability, particularly as it involves hosting the annual East Asia summit of leaders from 18 nations.

5.2. Minimal existing data privacy protections

The UNCTAD *Review* (2013) states succinctly that there 'is no privacy law in Myanmar at this time',[60] and while that is correct in relation to a specific data privacy law, there are **(p.400)** some cybercrime provisions in its electronic transactions law which are relevant to privacy protection, but which are also dangerous to freedom of speech.

Myanmar is not a party to the ICCPR, and is unusual in not having even signed it. However, in June 2013, Myanmar's National Human Rights Commission, which is close to the government, recommended that the government ratify the ICCPR and the International Covenant on Economic, Social and Cultural Rights (ICESCR), the two most significant international human rights treaties.[61]

Myanmar's 2008 Constitution[62] in Chapter VIII ('Citizen, Fundamental Rights and Duties of the Citizens'), includes guarantees of numerous civil and economic rights, including that 'every citizen shall be at liberty in the exercise of the…rights' of freedom of expression, assembly, and association, but only subject to such laws as exist,[63] and that:[64]

> The Union shall protect the privacy and security of home, property, correspondence and other communications of citizens under the law subject to the provisions of this Constitution.

These constitutional rights are supposed to be justiciable by application to the Supreme Court,[65] which is able to issue a number of writs for their enforcement.[66] Reform of the Constitution is a principal electoral aim of Burma's opposition party.

Burma's Electronic Transactions Law 2004[67] has been described as 'a solid framework upon which E-commerce and E-government can be built in the future'[68] but also as the law most frequently used to jail critics of the regime.[69] The law deals primarily with electronic signatures, and the licensing of certification authorities. It does not deal directly with data privacy issues, nor with the protection of consumers in e-commerce. The Act's computer crime provision[70] contains elements relevant to data privacy, including offences carrying potential jail terms of up to five years for 'hacking' or tampering with hardware or software, interception of communications, using 'any fact in any communication without permission of the originator and the addressee', using other people's passwords or security numbers, and creating or altering information so as to be detrimental to any person or organization. Such provisions could be used to protect personal information but, instead, they have been used for Internet censorship and to prosecute bloggers and other activists. They are clearly dangerously broader than the usual provisions providing reasonable protection to data privacy, and do not include any defences to help protect against misuse. The inclusion of an offence for 'using or giving

access to any person of any fact in any communication without permission of the originator and the addressee' is clearly open to such abuse.[71] The deputy communications minister stated in parliament in February 2013 that a new Electronic **(p.401)** Transactions Law was being drafted and that 'sections of the [existing] law used in the past to lock up activists will be repealed while the new legislation is being written'.[72] Amendments to replace prison sentences with fines have been approved by the legislature.[73] A Communications Law introduced into the National Assembly but not yet passed[74] requires licensing of all types of electronic communications systems.

In summary, there seems to be nothing in current Myanmar law which is of practical value for the protection of privacy other than some largely theoretical constitutional protection.

6. Timor Leste

Timor Leste (East Timor) is one of the world's youngest nations. Only Kosovo and South Sudan are more recent. It has been independent since 2002, after 400 years as a Portuguese colony, and nearly 30 years of Indonesian occupation after 1975. Timor Leste's application to become a full ASEAN member is still underway, following its signing of the ASEAN Treaty of Amity and Cooperation in 2006. The membership bid is supported by Indonesia, but some members have been sceptical that Timor Leste has yet developed the capacity to fully participate in ASEAN, including its hundreds of meetings each year, because it has an economy less than 20 per cent of that of the next smallest ASEAN member (Laos). Full membership is unlikely before 2015 at the earliest, but all member states are reported to now support its membership.[75] ASEAN membership would be likely to accelerate the development of data privacy laws in Timor Leste, as part of ASEAN's steps toward economic integration.

6.1. Timor Leste—historical, economic, and legal context

The development of data privacy protections in Timor Leste will take place in the context of a multiparty democracy, but in one of the least developed countries in the ASEAN region, and one of the smallest, with a population of less than 1.2 million.

History and politics of Timor Leste

Indonesia's departure from Timor Leste, after a pro-independence referendum in 1999, was accompanied by bloody reprisals by pro-Indonesian militias backed by some Indonesian generals, which caused over 2,000 deaths and considerable destruction of infrastructure. A UN-supervised multinational peacekeeping force (UNTAET) restored order until formal independence in 2002.[76] Despite this initial violence, Indonesia and Timor Leste have since developed a positive political relationship. The first decade of independent Timor Leste was fractured by an unsuccessful mutiny attempt by part of the army (leading to a further UN-sponsored peacekeeping force), and unsuccessful assassination attempts on both the **(p.402)** President and the Prime Minister. Despite these setbacks the country held peaceful Parliamentary and Presidential elections in 2007 and 2012, with results including changes of government and President. Timor Leste does seem to have consolidated a multiparty democracy.

Timor Leste—social and economic context

Timor Leste is one of the poorest countries in the ASEAN region. Over 40 per cent of its population of 1.1 million lives under the poverty line. Over 50 per cent are illiterate. There is high urban unemployment. Over 90 per cent of the population is rural, mainly subsistence farmers.[77] Tetum and Portuguese are the official languages.[78] 'East Timor's main source of income, for what is expected to be decades, will be oil and gas revenue, much of it from the joint development of vast oil and gas fields underlying the Timor Sea.'[79] Data privacy issues are likely to be a low priority until economic and social conditions have improved very substantially.

Legal and government systems of Timor Leste

Timor Leste's Constitution establishes what has been called a semi-presidential system, with an elected President who has various specific powers, including to veto legislation, dissolve Parliament, make appointments, and conduct foreign relations, but who does not otherwise participate in government. The Prime Minister is chosen by a parliamentary majority and leads the government.[80] Timor Leste has a unicameral Parliament.

The legal system, including the operation of the courts, is based on Portuguese law and is therefore a civil law system. Customary law is also recognized where consistent with statutory law and the Constitution.[81] Legislation, and most court proceedings are in Portuguese, which provides challenges for many participants:[82]

> The judiciary faces a number of other challenges. They have to apply UNTAET laws that are not always translated into their preferred language of Indonesian. They must also access new Timorese Government laws which are not always widely circulated and are written in Portuguese, a language most judges, in common with the vast majority of the population, do not read.

State surveillance in Timor Leste

Data surveillance in Timor Leste seems to be low in comparison with many other Asian countries. The US State Department reported in 2011 that there were 'no government restrictions on access to the Internet or credible reports that the government monitored e-mail or Internet chat rooms. Individuals and groups could engage in the peaceful **(p.403)** expression of views via the Internet, including by e-mail'.[83] Timor Leste is developing an ID card, first issued to government officials in 2011.[84]

6.2. Constitutional and treaty protections

Timor Leste's Constitution includes in its statement of fundamental principles that it is a state based on 'the respect for the dignity of the human person'.[85] Part II of the Constitution then spells out a comprehensive set of 'fundamental rights, duties, freedoms and guarantees', among which three provisions are particularly relevant to data privacy. It provides that '[e]very individual has the right to honour, good name and reputation, protection of his or her public image and privacy of his or her personal and family life',[86] and provides strong protections for the 'inviolability' of the home, correspondence, and other means of private communication, except under judicial warrant.[87] The US State

Department reported in 2011 that 'the government generally respected these prohibitions in practice'.[88]

The surprising constitutional inclusion is section 38 ('Protection of personal data') which provides that:

> (1) Every citizen has the right to access personal data stored in a computer system or entered into mechanical or manual records regarding him or her, and he or she shall have the right to demand the purpose of such data.
>
> (2) The law shall determine the concept of personal data, as well as the conditions applicable to the processing thereof.
>
> (3) The processing of personal data on private life, political and philosophical convictions, religious faith, party or trade union membership and ethnical origin, without the consent of the interested person, is prohibited.

This constitutional provision therefore provides a right of access to personal data, and protection against any processing without consent, of particular classes of sensitive personal data. Each apply against both the public and private sectors. The Constitution also requires that legislation be enacted to define legitimate processing of personal data, but this has not yet occurred. If Timor Leste does legislate on data privacy, its legislation will be likely to be influenced by the other lusophone (Portuguese-speaking) jurisdictions with data protection laws, such as Portugal, Macau, or Angola.

It is incumbent upon the government to guarantee the exercise of the fundamental rights and freedoms of citizens,[89] including by submitting legislation. It is possible for the failure of the government to legislate to protect constitutional rights to be brought before the **(p.404)** Supreme Court.[90] Provisions of international treaties to which Timor Leste is a party, including ICCPR Article 17, are part of Timor Leste's domestic law.[91] However, it is not a party to the Optional Protocol to the ICCPR, so its citizens cannot take matters to the UN Human Rights Committee. Any laws, or government actions, which are inconsistent with either the constitutional protections, or the privacy protection in ICCPR Article 17, can therefore be contested in the courts of Timor Leste.

6.3. Other data privacy protections

The Office of the Ombudsman (Provedor) for Human Rights and Justice has the Constitutional function to investigate citizens' complaints against public bodies, but can only make recommendations.[92] It is 'responsible for the promotion of human rights and good governance and has its own budget and dedicated staff. It has the power to investigate and monitor human rights abuses and governance standards, and to make recommendations to the relevant authorities'.[93] It has offices in four provincial centres in addition to the capital, and cooperates with a network of 10 NGOs, the Human Rights Monitoring Network. It is also a full member of the Asia-Pacific Forum of National Human Rights Institutions.[94]

Although Timor Leste's Constitution includes a right to 'be informed', it has not yet resulted in a right to information (or freedom of information) law. Article 19 has recommended that Timor Leste should adopt a comprehensive law in line with international principles.[95] Such a law would provide individuals with a right to access their own files held by public bodies, and protection against their personal information being unreasonably disclosed to others.

Notes:

([1]) E. Ann Black, ch. 9 'Brunei Darussalam: Ideology and Law in a Malay Sultanate' in E. Ann Black and Gary F. Bell (Eds.), *Law and Legal Institutions of Asia* (Cambridge, 2011), p. 302.

([2]) From the titah (royal speech) on independence, 1984.

([3]) Black, 'Brunei Darussalam', p. 327.

([4]) Peter Church, ch. 1 'Brunei' in *A Short History of South-East Asia* (5th Edn., Wiley, 2009), p. 2.

([5]) Black, 'Brunei Darussalam', p. 305.

([6]) Church, *A Short History of South-East Asia*, ch. 1.

([7]) Black, 'Brunei Darussalam', pp. 321–3.

([8]) Black, 'Brunei Darussalam', p. 305.

([9]) Black, 'Brunei Darussalam', p. 327.

([10]) Black, 'Brunei Darussalam', p. 317.

([11]) Black, 'Brunei Darussalam', p. 327.

([12]) National Registration Regulations, 2002 (Brunei), (CommonLII) <http://www.commonlii.org/bn/legis/nra19nrr657/>.

([13]) United Nations Conference on Trade and Development (UNCTAD), *Review of e-commerce legislation harmonization in the Association of Southeast Asian Nations, United Nations* (2013), p. 18, at <http://www.galexia.com/public/research/assets/unctad_asean_ecommerce_review_2013/> (hereinafter 'UNCTAD *Review* (2013)').

([14]) UNCTAD *Review* (2013), p. 18.

([15]) During WWII the French gave Japanese troops free right of passage, and Thailand seized some Cambodian territory, later returned.

([16]) This account, and the previous paragraph, are derived largely from Church, ch. 2

'Cambodia' in *A Short History of South-East Asia*. For a more detailed account see Francis Pike, *Empires at War: A Short History of Modern Asia Since World War II* (I B Tauris, 2010), chs. 37 and 42, and p. 724.

([17]) Church, *A Short History of South-East Asia*, p. 26.

([18]) Church, *A Short History of South-East Asia*, p. 30.

([19]) Sub-decree on Khmer Nationality Identity Cards, 1996 (Royal Government of Cambodia, No 36 ANK/BK/JULY 26, 1996).

([20]) 'Cambodia National ID' (Datastrip.com, 2014) <http://www1.btwebworld.com/datastrip/casestudies/pr-cambodia.htm>.

([21]) This section is based substantially on Jennifer Holligan and Tarik Abdulhak, 'UPDATE: Overview of the Cambodian History, Governance and Legal Sources' (GlobaLex, December 2013) <http://www.nyulawglobal.org/globalex/cambodia1.htm>.

([22]) Holligan and Abdulhak, 'UPDATE: Overview of the Cambodian History, Governance and Legal Sources', section 2.5 'Judicial Branch'.

([23]) K. Menghun and C. Meyn, 'Freedom of Information Draft Law Rejected' (*The Cambodia Daily*, 27 January 2013) <http://www.cambodiadaily.com/archive/freedom-of-information-draft-law-rejected-8311/>.

([24]) Article 19 NGO, 'Cambodia Draft Law on Access to Information – Legal Analysis' (Article 19, September 2011) <http://www.article19.org/data/files/medialibrary/2739/11-09-20-Cambodia.pdf>.

([25]) Article 19 NGO, 'Asia Pacific: Free expression and law in 201' (Article 19, 5 April 2012) <http://www.unhcr.org/refworld/docid/4fa790e62.html>.

([26]) UNCTAD 'UNCTAD and ASEAN review harmonization of e-commerce laws' (UNCTAD, 2 November 2012) <http://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=344>.

([27]) UNCTAD, *Review* (2013), p. 22.

([28]) During World War II, this included French acceptance of free passage of Japanese troops, and Thai occupation of some Lao territory.

([29]) Church, ch. 5 'Lao PDR' in *A Short History of South-East Asia*, p. 66.

([30]) Christopher Kremmer, *Stalking the Elephant Kings: In Search of Laos* (Silkworm Books, Chiang Mai, 1997) particularly ch. 8.

([31]) Central Intelligence Agency 'CIA World Factbook: Laos: Economy' <https://www.cia.gov/library/publications/the-world-factbook/geos/la.html>.

([32]) Church, ch. 5 'Lao PDR' in *A Short History of South-East Asia*.

([33]) Church, *A Short History of South-East Asia*, p. 77.

([34]) Cited in P. Douangboupha, 'Lao PDR Country Report', *ITU-ASEAN Forum on Promoting Effective and Secure Social Media* (ITU, Kuala Lumpur, 18 July 2012) <http://www.itu.int/ITU-D/asp/CMS/Events/2012/socialmedia/S6.4_Laos.pdf>.

([35]) 'Global Survey of Group Classification on National ID Cards' (Prevent Genocide International, circa 2001), 'Laos' section <http://www.preventgenocide.org/prevent/removing-facilitating-factors/IDcards/survey/>.

([36]) 'Member information: Lao People's Democratic Republic and the WTO' (WTO, 2013) <http://www.wto.org/english/thewto_e/countries_e/lao_e.htm>.

([37]) Amended Constitution of the Lao People's Democratic Republic 2003 <http://www.asianlii.org/la/legis/const/2003/1.html#C004>.

([38]) World Bank 'Public Accountability Mechanisms: Lao PDR' (World Bank, 2013) <https://www.agidata.org/pam/ProfileIndicator.aspx?c=110&i=9949>.

([39]) Articles 9, 22, and 35 of the Law on Local Administration 2003 <http://www.asianlii.org/la/legis/laws/lola2003250/>.

([40]) UNCTAD, *Review* (2013), p. 28.

([41]) Law on Telecommunications 2001 (Myanmar), art. 29.

([42]) Director-General Koun Southammakot of the Department of Import and Export, quoted by The World Bank, 'Lao PDR: New Online Platform to Boost Trade Transparency' (World Bank, July 9 2012) <http://www.worldbank.org/en/news/feature/2012/07/09/lao-pdr-new-online-platform-to-boost-trade-transparency>.

([43]) For a very readable history of events pre-1990, see Myint-U Thant, *The River of Lost Footsteps: A Personal History of Burma* (Faber and Faber 2007). Another account of Burma's post-war history is Pike's *Empires at War*, chs. 15 and 52. See also Church, ch. 7 'Myanmar' in *A Short History of South-East Asia*, for events to 2009.

([44]) Thant, *The River of Lost Footsteps*, chs. 10–12.

([45]) Thant *The River of Lost Footsteps*, chs. 10–12; Central Intelligence Agency 'CIA World Factbook: Burma'<https://www.cia.gov/library/publications/the-world-factbook/geos/bm.html>.

([46]) Thant, *The River of Lost Footsteps*, p. 258.

([47]) K.H. Win and E. Karim, 'The Legal System of the Republic of the Union of Myanmar in a Nutshell' (GlobaLex, September 2013) <http://www.nyulawglobal.org/globalex/Myanmar.htm> (hereinafter 'Win and Karim, "Myanmar legal system"').

([48]) Win and Karim, 'Myanmar legal system'. These laws included the Indian Penal Code (1860), the Criminal Procedure Code (1862), the Indian Evidence Act (1872), and the Civil Procedure Code (1859).

([49]) Constitution (Myanmar) 2008, art. 74.

([50]) Win and Karim, 'Myanmar legal system', pt. 4.

([51]) Win and Karim, 'Myanmar legal system', pt. 4.

([52]) Win and Karim, 'Myanmar legal system', pt. 6 'Sources of law'.

([53]) M. Zan, 'A Comparison of the First and Fiftieth Year of Independent Burma's Law Reports' (2004) 35 VUWLR 385, 387.

([54]) Zan 'A Comparison of the First and Fiftieth Year of Independent Burma's Law Reports', p. 389. For an exception see A. Huxley, 'The Last Fifty Years of Burmese Law: E Maung and Maung Maung' (1988) *Lawasia: Journal of the Law Association of East Asia and the West Pacific* pp. 9–20.

([55]) Win and Karim, 'Myanmar legal system'.

([56]) Win and Karim, 'Myanmar legal system', pt. 5 'Judiciary'.

([57]) Sarah Posner, 'Myanmar Constitutional Court Justices Resign Following Impeachment Vote' (*JURIST*, 7 September 2012) <http://jurist.org/paperchase/2012/09/myanmar-constitutional-court-justices-resign-following-impeachment-vote.php>.

([58]) H. Hindstrom, 'President Bows to Parliament on Controversial New Law' (*DVB*, 22 January 2013) <http://www.dvb.no/news/president-bows-to-parliament-on-controversial-new-law/25940>.

([59]) R. Severino, 'ASEAN's chairmanship in 2013 and 2014' (*East Asia Forum*, 2 April 2013) <http://www.eastasiaforum.org/2013/04/02/aseans-chairmanship-in-2013-and-2014/>.

([60]) UNCTAD *Review* (2013), p. 33.

([61]) Article 19 NGO, 'Myanmar: National Human Rights Commission recommends ratifying key human rights treaties' (Article 19 NGO, Press Release, 22 June 2013).

([62]) Constitution of the Republic of the Union of Myanmar (2008, Printing & Publishing

Enterprise, Ministry of Information) <http://www.burmalibrary.org/docs5/Myanmar_Constitution-2008-en.pdf>.

([63]) Constitution (Myanmar), art. 354.

([64]) Constitution (Myanmar), art. 377.

([65]) Constitution (Myanmar), art. 377: 'In order to obtain a right given by this Chapter, application shall be made in accord with the stipulations, to the Supreme Court of the Union.'

([66]) Constitution (Myanmar), art. 378 lists Writs of Habeas Corpus, Mandamus, Prohibition, Quo Warranto and Certiorari.

([67]) Electronic Transactions Law 2004 (Myanmar) (unofficial English translation) <http://www.burmalibrary.org/docs/Electronic-transactions.htm>.

([68]) S.E. Blythe, 'Rangoon Enters the Digital Age: Burma's Electronic Transactions Law as a Sign of Hope for a Troubled Nation' (CCSE International Business Research, 2010, originally on ccsenet.org) <http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan046159.pdf>.

([69]) W.N. Toe, and Z.M. Win, 'Myanmar's Parliament Considers Amending Draconian Law' (*Radio Free Asia*, 22 August 2013) <http://www.rfa.org/english/news/myanmar/electronic-transactions-law-08212013155853.html>.

([70]) Electronic Transactions Law 2004 (Myanmar), s. 34.

([71]) Electronic Transactions Law 2004 (Myanmar), s. 34(b).

([72]) S.T. Lynn, 'Government to Redraft "Outdated" Electronic Transactions Law' (*Myanmar Times*, 4 February 2013) <http://www.mmtimes.com/index.php/national-news/3977-govertment-to-redraft-outdated-electronic-transactions-law.html>.

([73]) 'Lower House Approves Amendments to Electronics Act' (DVB, 23 October 2013) <https://www.dvb.no/news/lower-house-approves-amendments-to-electronics-act-burma-myanmar/33786>.

([74]) Alternative Asean Network on Burma (ALTSEAN-BURMA) <http://www.altsean.org/>.

([75]) Ismira Lutfia Tisnadibrata, 'Timor-Leste Poised to Win ASEAN Membership' (Khabar Southeast Asia, 13 May 2013) <http://khabarsoutheastasia.com/en_GB/articles/apwi/articles/features/2013/05/16/feature-03>.

([76]) Church, ch. 3 'East Timor' in *A Short History of South-East Asia*, p. 34.

([77]) Church, *A Short History of South-East Asia*, p. 36.

([78]) Constitution (Timor-Leste), s. 13.

([79]) Editorial, 'East Timor Must Chart a Course out of Poverty' (*Sydney Morning Herald*, 22 January 2013).

([80]) Timor-Leste Legal Education Project, *An introduction to constitutional law in Timor Leste* (Timor-Leste Legal Education Project (TLLEP)) <http://www.stanford.edu/group/tllep/cgi-bin/wordpress/wp-content/uploads/2012/09/Constitutional-Law-in-Timor-Leste.pdf>.

([81]) 'The State shall recognise and value the norms and customs of East Timor that are not contrary to the Constitution and to any legislation dealing specifically with customary law': Constitution (Timor-Leste) s. 2(4).

([82]) Article 19 NGO and Internews, *Freedom of Information and the Media in Timor-Leste* (Baseline Studies, 2005) <http://www.article19.org/data/files/pdfs/publications/timor-leste-baseline-study.pdf>.

([83]) United States Department of State, *2011 Country Reports on Human Rights Practices—Timor-Leste* (24 May 2012) <http://www.unhcr.org/refworld/docid/4fc75a5673.html> (hereinafter US State Department *Timor Leste Country Report* (2012)).

([84]) 'Official launch of the first issue of the Identity Card of RDTL' (Government of Timor Leste, 6 November 2011) <http://timor-leste.gov.tl/?p=3198&lang=en>.

([85]) Constitution (Timor-Leste), s. 1.

([86]) Constitution (Timor-Leste), s. 36.

([87]) Constitution (Timor-Leste), s. 37: '(1) Any person's home and the privacy of his or her correspondence and other means of private communication are inviolable, except in cases provided for by law as a result of criminal proceedings. (2) A person's home shall not be entered against his or her will, except under the written order of a competent judicial authority and in the cases and manner prescribed by law. (3) Entry into any person's home at night against his or her will is clearly prohibited, except in case of serious threat to life or physical integrity of somebody inside the home.'

([88]) US State Department, *Timor Leste Country Report* (2012).

([89]) Constitution (Timor-Leste), s. 115.

([90]) Constitution (Timor-Leste), s. 151: 'The President of the Republic, the Prosecutor-General and the Ombudsman may request the Supreme Court of Justice to review the unconstitutionality by omission of any legislative measures deemed necessary to enable the implementation of the constitutional provisions.'

([91]) Constitution (Timor-Leste), s. 9: '(2) Rules provided for in international conventions, treaties and agreements shall apply in the internal legal system of East Timor following their approval, ratification or accession by the respective competent organs and after publication in the official gazette. (3) All rules that are contrary to the provisions of international conventions, treaties and agreements applied in the internal legal system of East Timor shall be invalid.'

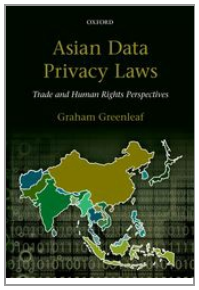
([92]) Constitution (Timor-Leste), s. 27.

([93]) US State Department, *Timor Leste Country Report* (2012).

([94]) A Byrnes, A Durbach, and C Renshaw, 'Joining the Club: The Asia Pacific Forum of National Human Rights Institutions, the Paris Principles, and the Advancement of Human Rights Protection in the Region' (2008) 14(1) *Australian Journal of Human Rights*, pp. 63–98 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1397466>.

([95]) Article 19 and Internews, *Freedom of Information and the Media in Timor-Leste*, pp. 100–1.

University Press Scholarship Online
Oxford Scholarship Online



Asian Data Privacy Laws: Trade & Human Rights Perspectives
Graham Greenleaf

Print publication date: 2014
Print ISBN-13: 9780199679669
Published to Oxford Scholarship Online: December 2014
DOI: 10.1093/acprof:oso/9780199679669.001.0001

India—Confusion Raj, with Outsourcing

Graham Greenleaf

DOI:10.1093/acprof:oso/9780199679669.003.0015

[–] Abstract and Keywords

India, the world's most populous democracy, has failed to develop significant data privacy laws, limiting the human rights protection of its citizens, and impeding its trade with Europe. After surveying the promising but as yet limited constitutional protection of privacy in India this chapter examines in detail the data privacy Rules made under section 43A of the Information Technology Act (IT Act) of 2000. It concludes that these Rules superficially resemble a data protection law, but they have crippling deficiencies and ambiguities. In addition, the enforcement system for the Rules is currently not functioning. However, there is more to the IT Act than section 43A: its Rules, and its other aspects relevant to privacy protection, are discussed. There are at least three current proposals for development of a comprehensive data privacy law for India, and these are outlined, although none have yet obtained clear government approval.

Keywords: data protection, privacy, Asia, India, SAARC, EU adequacy, s43A Rules

(p.406)

1. Contexts of information privacy in India

India is the world's most populous democracy, with an estimated 1.2 billion citizens. The Indian economy, previously very state dominant, has developed an energetic private sector in the last two decades. It is one of the fastest growing major economies with growth of more than 7 per cent per year since 1997.[1] Its GDP is one of the five largest in the world on a purchasing power parity basis.

India's service industry accounts for around 55 per cent of the country's GDP,[2] and a significant part of this is the international outsourcing of processing of personal information (business processing outsourcing),[3] through telecommunications call centres, transcription of medical consultation notes, and in many other areas. Statistics concerning outsourcing have high volatility as trade patterns change, and often low reliability. Nevertheless, despite other countries increasingly challenging India's dominance in particular business processing outsourcing sectors, India remains one of the world's largest outsourcing destinations, with the USA and Europe being its two largest sources of incoming work.

India has failed to develop significant data privacy laws. As well as its implications for Indian citizens, this is impeding India's very significant economic relationship with Europe.[4] Protracted negotiations between the European Union (EU) and India for a comprehensive Free Trade Agreement started in June 2007 and are far from concluded.[5] This chapter focuses on both the domestic and international implications for India of the development of data privacy laws.

1.1. India—historical and political context

India's history is both well known and well served by excellent histories both of sweeping scope[6] and with a focus on the period since independence from British colonialism.[7] The British colonial period from the late eighteenth century was the last of many periods of foreign rule in India. The end of the colonial administration was marked by the partition of India and Pakistan (and vast loss of life), the incorporation of the 'princely states' into India, and the birth of an optimistic and socialist-leaning democracy. Democracy survived and strengthened, despite the aberration of Mrs Gandhi's 'emergency' in the 1970s. However, India's version of socialism had ceased to produce benefits for many people by the 1970s, and although the governments of both Indira and Rajiv Gandhi had started to reduce the 'licence Raj' that stifled initiative, it was the government of Narasimha Rao from 1991 that started the rescue of the

Indian economy through opening up to foreign investment, and the end of state monopolies in many sectors. After 1994, the India economy **(p.407)** exceeded seven per cent annual growth in most years. A different society is now emerging, with a rapidly expanding middle class and a largely free market economy.[8]

India has a multiparty bicameral parliamentary system at the national level. It is a unitary state (not a federation) but has 35 regional governments (28 states and 7 union territories). The national government has strong powers, and is often referred to as 'the Centre'. India is a republic within the Commonwealth, independent of Britain since 1947. All states, and the two union territories of Puducherry and the National Capital Territory of Delhi, have elected legislatures. The other five union territories are directly ruled by the Centre through appointed administrators. Government is patterned on the Westminster model, although with a written constitution including guarantees of rights, and with many innovations which have led to it being described as the pioneer of a new form of 'monitory democracy'.[9] Significant data privacy laws have not been developed in India except by the Centre government, but laws could be developed by regional governments, or they may be involved in administration of a future national law. Despite various institutions which assist transparency, the Indian government still has very considerable problems with corruption, as do some of its private sector institutions.

1.2. Legal system of India

India's legal system is complex and different from its British origins.[10] India's Constitution is an extraordinary document, developed by an inclusive process headed by Motilal Nehru for 20 years before Indian independence, including both Directive principles aimed at future legislation for social justice, and Fundamental Rights giving protection against state action (and in some case private sector action).[11] These constitutional principles create the basis of India's interventionist Supreme Court, which has had significant implications for protection of privacy (for example, the Right to Information Act, see section 7.1 of this chapter), and may continue to do so in future. In addition to legislation passed by the Centre or state legislatures, there are a variety of other sources of legislation. Regulations made under Acts may be disallowed by the relevant legislatures. The executive may make Ordinances while a legislature is not in session, but which will lapse six weeks after it resumes in session.[12] The executive may also legislate, by a variety of instruments (including 'Press Notes', see section 3.2 point (ix) of this chapter) in areas in which the legislature has not legislated in such as way as to 'cover the field'. Such executive legislation may prevent executive actions or directions from being *ultra vires* in many instances. It is therefore necessary to be aware of a wide range of possible legal instruments which may affect privacy issues.

India inherited a legal system based on the common law from the UK upon independence, and with some modifications this has continued. Indian common law and equity is part of the family of common law systems, with a case law system of precedent cases as elsewhere. India's Supreme Court is the apex court of India's legal system, and is also the highest constitutional court, although other courts are also entitled to interpret the Constitution and declare legislation unconstitutional (and often do so), subject to appeals to **(p.408)** higher courts. Decisions of the Supreme Court are binding on lower courts but not on the Supreme Court itself. There are High Courts at state level with their own precedent hierarchies.[13] Decisions of foreign courts (other than the Privy Council prior to independence) are of persuasive value only.

1.3. State surveillance in India

The need for stronger data privacy laws in India is apparent from even a brief account of some key aspects of India's growing array of surveillance institutions and surveillance powers. The rapid recent development of surveillance powers and institutions has also made the incomplete development of data privacy laws in India a highly political topic. India has been a frequent target of terrorist attacks, so there is a constant temptation to extend every form of surveillance. India's private sector has not yet embraced systemic data surveillance techniques for commercial purposes, except in the credit industry. The Credit Information Companies (Regulation) Act 2005 is a blueprint for a comprehensive credit surveillance system, but on the other hand the information it collects will be largely restricted to the credit industry.[14] However, the Indian state itself is not yet involved in pervasive surveillance of its population, or even major segments of it. Furthermore the tendencies toward increased surveillance are tempered by the activism of the somewhat slow-moving Indian judiciary which administers the rule of law in ways that are sensitive to issues of civil liberties, including privacy.

However, there are substantial increases in surveillance capacities under development in both sectors, through measures such as those discussed in the following section. In particular, the development of the Unique Identification Authority of India (UIDAI) system has major data protection implications, but it is unknown whether the legislation under which it will operate (when enacted) will bring it within the established protections of Indian democracy and civil liberties. Whether those protections will be sufficient, in light of all the developments sketched below and the fact that some of them are already occurring without any legislative basis, remains to be seen. Some

critics claim the surveillance situation is worsening rapidly, arguing that the convergence of the developments in this section carries great risks for Indian society and democracy.[15]

ID systems

Since 2009, India's Congress party national government has aggressively pursued the development of an ID system, the Unique Identification Number (UID number or 'aadhaar'), with the ostensible aim of increasing social inclusion by providing a verifiable means of identification to the large proportion of India's population that lacks it. The UIDAI was established by Executive Order in 2009. The UIDAI aims to issue a biometric-based unique **(p.409)** ID number to all of India's estimated 1.2 billion population, and claims to have issued about 450 million UIDs. The UIDAI claimed from the outset that obtaining a UID number was not compulsory, that it did not involve the issue of a card, and that it was not an indication of 'citizenship' because it was available to any resident of India. However, by a variety of means, possession of a UID (or at least one of a variety of 'official' documents stating it) has become compulsory, in some states in India, for people to obtain various essential services such as LPG gas allocations. This is very contentious for various reasons, including the delays and difficulties that many people experience in obtaining UIDs, and because of privacy concerns. Also, some governments in states which are not Congress-led, such as West Bengal, see no reason to promote a key Congress party political initiative which is of dubious legality.[16]

The Congress government introduced the UIDAI Bill 2010 into the Lok Sabha in 2010 to give the UID a legislative basis, but its passage has been blocked, including on the grounds of its privacy deficiencies, and that it is not accompanied by a national data privacy Bill. An amended UIDAI Bill has not been tabled despite announcements. The need for enabling legislation became acute in September 2013, when the Supreme Court's interim ruling in *Puttaswamy v Union of India*[17] held that (in the absence of enabling legislation) it was unconstitutional for possession of a UID to be made compulsory for any person to obtain essential services from the government, such as LPG gas allocations. It was also unconstitutional, in the absence of enabling legislation, for UIDs to be issued to persons who were not Indian citizens, as evidence suggested had been the practice. In October 2013, a full Supreme Court bench continued the previous prohibition orders, but has not yet issued its final judgment on unconstitutionality. Conflict has continued, with some government agencies continuing to ignore the Supreme Court orders and require UIDs as a condition of service. On the other hand, the Madras High Court has directed public sector oil companies to await the Supreme Court's final decision before requiring an Aadhaar-linked bank account before remitting LPG subsidies.[18] In March 2014, the final decision by the Supreme Court in *Puttaswamy* upheld the interim decisions, and ordered the central government to withdraw any orders making the ID number mandatory for any government services.[19] In a related action, the Court also prohibited the UIDAI from providing any data it holds to any government agency without data subject consent, in response to attempts by a court in Goa to obtain biometric data to aid identification in a criminal case.[20] Some opposition parliamentarians have stated that if the opposition wins the 2014 elections, the new government will scrap the ID number, so its future is uncertain.

There are numerous other identification systems developing or existing in parallel with the UID, at both state and Centre levels,[21] including the National Population Register **(p.410)** (NPR) which is intended to eventually lead to the issue of a national ID card. The proliferation of ID systems is chaotic and political.

Government surveillance powers

The Information Technology Act 2000 includes extensive provisions for data interception and surveillance. New expansions to the data surveillance capacity of the Indian government arise from the 2008 amendments to the Act, providing the government with powers to intercept data, access stored data, require retention of data and control encryption in a broad range of circumstances. Many departments have extensive powers to demand personal data, and systemic methods of collection, including the Reserve Bank of India and the taxation authorities.[22] The National Intelligence Grid (NATGRID) is intended to link together 21 government departments and agencies, and private sector bodies. It is under development with a very large budget, but without any legislative control or announcement of relevant legislation.[23]

2. Constitutional and common law protections of privacy in India

Non-statutory protections of privacy in India are of uncertain scope but may become significant.

2.1. International obligations in relation to privacy

India is a signatory to the International Covenant on Civil and Political Rights 1966 (ICCPR), Article 17 of which includes protection of privacy. Treaties are not enforceable under Indian law until they are incorporated into domestic law.[24] However, article 21 of the Indian Constitution (discussed later in relation to privacy) has to be interpreted consistently with international law.[25] India is not a signatory to the 1st Optional Protocol to the ICCPR, so it is not possible for Indian citizens to make complaints to the UN concerning failures to fully implement Article 17.

India is not a party to any of the other significant international data protection agreements. It is not a member of the OECD or of the Asia-Pacific Economic Cooperation (APEC). The South Asian Association for Regional Cooperation (SAARC), the regional organization of which India is the largest member, does not list human rights or privacy among its seven current areas of cooperation (see Chapter 2, section 2.2).

2.2. Constitutional basis of privacy protection

The Constitution of India provides in article 21 that '[n]o person shall be deprived of his life or personal liberty except according to procedure established by law', interpreted by the Supreme Court to include implied protection of privacy as 'an essential ingredient of **(p.411)** personal liberty'.[26] Privacy was also held in that case to be protected by the rights to freedom of speech and expression, and the right of freedom of movement.[27] The phrase 'procedure established by law' has been held to have a meaning similar to 'due process of law' in the US Constitution.[28] Article 14 guarantees 'equality before the law or the equal protection of the laws' and is also significant because of its interaction with article 21. Against the constitutional right of privacy must be balanced the guarantees of 'freedom of speech and expression'.[29] Article 21 rights are available to all persons, whether or not they are citizens of India. The Supreme Court has insisted that authorities relying on the 'procedure established by law' exception to article 21 'must strictly and scrupulously observe the forms and rules of the law'.[30] Case law has repeatedly taken a 'persons and not places' emphasis in interpreting the right of privacy, rejecting views that privacy is tied to property interests.[31] This is consistent with the Indian Supreme Court developing article 21 in the direction of data protection principles, although this has not occurred as yet: almost all cases on article 21 are about search and seizure or telecommunications surveillance.

The most significant development outside search and surveillance issues was the decision of the High Court of Delhi in the *Naz Foundation, Case*,[32] but four years later it was reversed on appeal by the Supreme Court. This was public interest litigation brought by the non-governmental organization (NGO), Naz Foundation to challenge the constitutional validity of section 377 of the Indian Penal Code, 1860, which criminally penalizes what is described by the section heading as 'unnatural offences' including, in the Court's interpretation, homosexual sexual acts. The Delhi High Court initially dismissed the application as an 'academic challenge', but was required by the Supreme Court in 2004 to re-examine the matter. The Delhi Court found that section 377 breached the right of privacy and rejected the claim that this invasion of privacy was justified within the 'procedure established by law' exception to article 21. It found that the state cannot invade the privacy of citizens based solely on considerations of 'public morals' but requires a 'compelling state interest' as justification. Section 377 was also held to violate article 14 (equality before the law) and its more particular expression in article 15 (prohibiting discrimination on the grounds of sex).[33] In the *Naz Foundation Case* the Delhi High Court took the protection of privacy under the Indian Constitution beyond issues of search and surveillance. The broadest statement of the Delhi High Court's approach, following its review of Indian case law on protection of privacy, was that '[t]he right to privacy thus has been held to protect a "private space in which man may become and remain himself". The ability to do so is exercised in accordance with individual autonomy'.[34]

However, the Supreme Court held on appeal[35] that distinctions made between different forms of intercourse cannot be categorized as arbitrary or irrational, and therefore **(p.412)** section 377 was not *ultra vires* articles 14 or 15. In interpreting article 21, it accepted that for a law to be valid it must 'not only be competently legislated but must also be just, fair and reasonable', taking into account 'notions of legitimate state interest and the principle of proportionality'. It did not find that any of these considerations indicated that section 377 was unconstitutional, and that evidence that the section had been misused by authorities 'is not a reflection of the vires of the section'. The decision contributes little to clarification of the boundaries of the implied right of privacy.

There have been other recent significant cases reiterating the constitutional right to privacy[36] in areas such as compulsory medical tests,[37] the use of 'silent observer' surveillance technology in hospital ultra-sound equipment,[38] display of a photograph of a person by the police,[39] and various aspects of telecommunications surveillance. These cases have primarily dealt with the balances between privacy rights and other public interests that must be met by public authorities, and have not dealt with the key question (for this chapter) of whether there the constitutional right of privacy will be expanded in the direction of protecting data privacy interests. Nor does the Supreme Court's decision in the *Naz Foundation Case* give any indication of whether this is likely.

Some unusual factors are relevant to the constitutional protection of privacy in India. Breaches of the constitutional rights by public authorities can result in court orders for compensation.[40] Indian courts have given some constitutional rights[41] a 'direct horizontal effect', allowing constitutional rights to be asserted against non-state actors, including directly by litigation. The implied right to privacy protection is unlikely to be one of these rights, according to both academic opinion,[42] and dicta in one of the few privacy decisions dealing with a claim against a

private party.[43] Most unusual, is that if the legislature has failed to enact protections required by the Constitution, the Supreme Court can make binding rules which will operate until laws are made by the legislature and found by the Court to be sufficient. This occurred when the Supreme Court required enactment of a right of access to public information, in the absence of which its own draft statute would apply. This led ultimately to national enactment of provisions providing this right in the Right to Information Act 2005.[44]

(p.413) 2.3. Common law protection of privacy—tort and breach of confidence

A tort of invasion of privacy has not been established in Indian law, though there is some slight judicial support for it.[45] The distinction between a common law right and a constitutional right is still important in India, both because the scope of the two rights may differ, and because (as discussed earlier) Indian courts are unlikely to allow horizontal enforcement of the constitutional implied right of privacy. Nor have Indian courts yet adopted the extension of the law of breach of confidence to protect privacy interests as has occurred in the UK over the past decade,[46] although there are only limited dicta to that effect.[47] Supreme Court decisions are needed to clarify both matters.

3. Information Technology Act 2000 and Rules under section 43A

Such statutory protection of privacy as can be found in India is scattered across a number of statutes. The Information Technology Act 2000 (IT Act), as amended by the Information Technology (Amendment) Act 2008 (ITAA), has the broadest scope. The IT Act 2000 includes the most significant Indian statutory provisions dealing with data privacy issues, but only in a small number of sections, particularly sections 43 and 43A. It also deals with electronic transactions and digital signatures[48] and cyber-security issues. The ITAA came into force on 27 October 2009.[49] There has been little judicial interpretation of the privacy or personal information aspects of the Act and no Supreme Court decisions.

India did not have any general data protection legislation until 2011, when a set of Rules (delegated legislation) made under section 43A of the IT Act purported to create a whole data privacy regime, but only by delegated legislation, not by primary legislation. These Rules superficially resemble a data protection law, but they have crippling deficiencies and ambiguities, only some of which can be mentioned here: they may be *ultra vires*; half of the Rules only apply to a very restrictive definition of 'sensitive personal data', and not to other personal data; half of them do not impose obligations in relation to data subjects per se, but only to 'the provider of the information'; and it is questionable whether and when consumers (data subjects) are given a right of civil action. No consumer has exercised any rights under these Rules, and after three and a half years they have had no visible effect. In addition, the enforcement system for the Rules is currently not functioning (see section 7 of this chapter). Under these circumstances, only limited discussion of the Rules is justified in the rest of this section of this chapter, although a full discussion is available elsewhere.[50] However, there is more to the IT Act than section 43A and its Rules (see section 5, this chapter).

(p.414) 3.1. Section 43A and the 2011 Rules—civil liability relating to personal data

Section 43A of the IT Act, inserted by the ITAA in 2008, provides:

> Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

There is no limitation imposed on the compensation that can be awarded. At first glance this looks like a useful data protection provision dealing with data security: organizations controlling personal data that fail to implement reasonable security procedures will be liable to pay compensatory damages to 'the person so affected' for resulting 'wrongful loss'. Data leaks and other data security breaches could, it seems, result in compensation to the data subjects so harmed. Foreign companies dealing with Indian outsourcing organizations could also have a statutory basis for compensation, as could Indian companies outsourcing some of their processing. However, the Act allows rules to be made concerning 'the reasonable security practices and procedures and sensitive data or information under section 43A'.[51] In April 2011 the Department of Information Technology within the Ministry of Communications and Information Technology made the Information Technology (Reasonable security practices and procedures and sensitive personal information) Rules, 2011 (the 'Rules').[52] The Rules are the closest that India has to a general data protection regime, but the ambiguous wording of both section 43A and of the Rules makes them complex to interpret. There are no court or tribunal decisions concerning the Rules, so no judicial guidance is available.

3.2. The uncertain scope of section 43A and the Rules

Before considering the substantive data protection content of the Rules, consideration of the exact scope of the both section 43A and the Rules, and their legal validity, is required.[53]

(i) Limitation to 'body corporate' and 'commercial or professional activities'. Section 43A only applies to a 'body corporate', which 'means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities'. Although there are some public sector bodies which come within this, such as state-owned corporations, there is very limited coverage of the public sector. Religious and social organizations, including charities, whose activities are not classified as 'commercial' will also be a substantial exclusion from the scope of the law.
(ii) Exclusion of non-automated data. 'Data' is defined as data 'in any form' 'which is intended to be processed, is being processed, or has been processed in a computer system or computer network'.[54] While this resembles the limitation found in other laws such as the EU Data Protection Directive and the Macau legislation, it is in fact far more limited because these other laws include organized manual filing systems.
(p.415) *(iii) Is the extension of scope beyond 'security'* ultra vires? Section 43A does not purport to regulate anything other than 'negligen[ce] in implementing and maintaining reasonable security practices and procedures'. How broadly can the Rules regulate aspects of personal data processing other than 'security' (in its ordinary meaning), before they go beyond what is authorized by section 43A and become *ultra vires*? There is incompatibility between rule 8 and the other Rules which can only be resolved by interpreting rule 8 as leaving the other Rules intact, if they are to be *intra vires*.[55] There is therefore considerable doubt as to whether all or most of the Rules are *intra vires*, or of any substantive effect. This whole edifice therefore rests on very shaky foundations.
(iv) Distinction between 'personal' data and 'sensitive' data (rules 2 and 3). 'Personal information' is defined in rule 2(i) in a conventional way, to mean 'any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person'. 'Sensitive personal data or information' is then defined by rule 3 as follows:

> Sensitive personal data or information of a person means such personal information which consists of information relating to: (i) password; (ii) financial information such as Bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) Biometric information; (vii) any detail relating to the above clauses as provided to body corporate for providing service; (viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:

This rule 3 definition of 'sensitive personal data' is a very narrow definition both in comparison with 'personal information' in the Rules, and with many other definitions of sensitive information, including that in the EU Data Protection Directive. Other than 'data concerning health or sex life', it gives additional protection to none of the categories of personal information that European law considers requires extra protection. The narrowness of the meaning of 'sensitive' information is one of the key limitations of the Rules. Half of the Rules only apply to this narrow category of 'sensitive' personal data, and do not apply to the broader category of 'personal information'. It is also much narrower than the definition of 'sensitive personal data' in the published draft of the Rules, reported to be because the Indian government requested advice on this definition from the Data Security Council of India (DSCI), which recommended a very narrow definition (and expanded it to a small extent later).[56] Six rules and sub-rules apply only to sensitive data,[57] which means that for all 'non-sensitive' 'personal information', there are no rules at all concerning **(p.416)** disclosure or data exports, and possibly collection, because those rules only apply to 'sensitive personal data'. This defect calls into question whether this law should be described as a 'data privacy law' at all.
(v) Some rules do not apply directly to data subjects, only to 'providers' of data. A further source of complexity is that half of the Rules[58] do not impose obligations in relation to data subjects per se, but only to 'the provider of the information'. In the case of outsourced processing, this may only mean that the controller, not the processer, is liable, which is not uncommon in data privacy laws, provided the data subject has someone against whom to take action.[59] However, it also means that where the data subject is not the 'provider' of the information to the data controller (all collection of personal data from third parties, and all collection by observation or from documentary sources), none of these data protection rules will apply. This also calls into question whether this law should be described as a 'data privacy law' at all.
(vi) Section 43A obligations only apply to companies processing sensitive personal data. Neither section 43A nor the Rules apply to a company that is not involved in processing some 'sensitive personal data', but is only processing other types of personal information.[60] Many companies that clearly do process personal data will therefore fall outside section 43A, denying all remedies to data subjects.

(vii) Can 'agreement between the parties' affect the Rules? The definition of 'reasonable security practices and procedures' requires that section 43A applies to those practices and procedures 'as may be specified in an agreement between the parties or as may be specified in any law for the time being in force'. This is ambiguous, but the better answer may be that the section 43A Rules are 'a law' and will apply, and agreements between the parties are irrelevant.
(viii) Do data subjects have any right of action? Another problem with the reference to 'an agreement between the parties' is that it could give rise to an argument that section 43A is only intended to benefit parties who have contracted to have data processing done for them (data exporters), and not consumers (data subjects) who do not have a contractual relationship with the processor. All that can be said with confidence is that the circumstances under which consumers (data subjects) may be able to rely on section 43A is ambiguous, and awaits court interpretation. The rest of this discussion proceeds on the assumption that data subjects can rely on section 43A, while noting its uncertainty. If this deficiency can be overcome, then section 43A might allow compensation to affected data subjects, despite the lack of application of some of these Rules directly to data subjects. Section 43A states that breaches of the section may result in payment of compensation 'to the person so affected'. It is therefore arguable that this could give data subjects the basis of a right of action despite the rule only applying to 'providers'.
(p.417) *(ix) The Press Note's uncertain effect.* In August 2011 India's Department of Information Technology issued what it called a 'Press Note',[61] a purported executive order which may be *ultra vires*. Whether it has any legal validity is questionable, but it has no substantive effect on the position otherwise described here.[62]

We can therefore summarize the scope (and validity) of the Rules and section 43A in the following propositions:

- Only commercial private sector entities are covered, with few exceptions. Only automated information systems are covered.
- To the extent that the Rules cover more than 'security' some or all of them may be *ultra vires*, or alternatively all except rule 8 could be made ineffective.
- If the Rules are 'a law' (which is probable) then they cannot be nullified by 'agreement between the parties'.
- At least six of the 12 rules and sub-rules apply only to 'sensitive personal data' (which has a very narrow definition) and do not apply to all 'personal information'.
- Half of the 12 rules do not apply directly to data subjects, only to 'providers' of data, and therefore might not be able to be enforced by consumers (data subjects) in many situations, depending on who 'provided' the data in question.
- Unless a company processes some sensitive personal data, it will have not liability at all under the Rules, even if it does process other 'personal information'.

These problems of scope and validity also make the Rules and section 43A incoherent and close to impossible to understand. Nevertheless, businesses operating in India will have to comply with some of them, some of the time, if they can work out which ones and when.

From the perspective of an Indian data subject (consumer), there is an extremely small probability that a relevant rule would apply to a specific transaction in which they encounter a problem, or that they could obtain any remedy, These Rules are largely irrelevant as substantive data protection for consumers. This will be even more apparent when the non-functioning enforcement structure under which the Rules are currently operating is considered later in this chapter. Taking all the deficiencies into account, the Rules do not qualify as a data privacy law.

3.3. The content of the Rules under section 43A

Each of the Rules is now examined in relation to their data protection content, subject to the general limitations discussed in the previous section. However, given the previous discussion, less space will be spent analysing the substantive rules than might otherwise have been the case.

Data protection principles generally (rule 5)

Rule 5 sets out briefly a set of data protection principles, covering collection (consent, lawful use, etc.), notice, retention, internal use, access, correction, security, and handling of grievances. Each is paraphrased briefly below. The paraphrases below simply refer to **(p.418)** 'information', and the scope (all personal data or only sensitive data or ambiguous scope of data), plus the relevant rule number, is included at the end of the paraphrase. The fatal deficiencies of these principles because of their multiple limitations of scope have been set out in the previous section.

The DSCI issued a 'White paper' in 2012, in which it claims at various points that these rule 5 provisions satisfy the EU's requirements of adequacy (and by implication provide a reasonable standard of data protection).[63] However, it does not at any point explicitly address these issues arising from non-applicability of the Rules to all personal data, the non-applicability to all data subjects, and the non-applicability to data received from sources other than the data subject. DSCI's claims must therefore be discounted or ignored.

Each of the sub-rules of rule 5 are now addressed in turn.

(1) Consent and purpose limitation (rule 5(1)). Companies must obtain, before collection, written consent from the provider of the information 'regarding purpose, means and modes of uses' (sensitive information only). This does not apply to all data subjects, only to the 'provider of the information'. Within its limited scope, if Indian data controllers are dealing directly with data subjects to collect sensitive personal information, this is strong protection.
(2) Lawful purpose and minimal collection (rule 5(2)). The collector must ensure that 'the information is collected for a lawful purpose connected with a function or activity of the agency'; and 'the collection of the information is necessary for that purpose' (sensitive information only). There is no specific requirement that data be 'accurate and where necessary, kept up to date', a deficiency in comparison with international standards.
(3) Notice and purpose limitation (rule 5(3)). Companies 'collecting information directly from the individual concerned' (but not otherwise), 'shall take such steps as are, in the circumstances, reasonable to ensure that the individual concerned is aware of' the fact of collection, the purpose, the intended recipients, and the contact information for the collector and the party that will hold the data. Because of the broad definition of 'information' in rule 2((1)(f), this should apply to all 'personal information'. Data subjects are not entitled to any notice when their personal data is collected from third parties.
(4) Retention (rule 5(4)) Companies may not retain information beyond when it may lawfully be used (sensitive information only). This is not the same as when the purpose of collection has expired, and is a low standard of protection. It applies to processors as well as controllers.
(5) Use (rule 5(5)). 'The information collected shall be used for the purpose for which it has been collected' (sensitive information only—implied by context). This applies to processors as well as controllers.
(6) Subject access and correction (rule 5(6)). Companies must 'permit the providers of information, as and when requested by them, to review the information they had provided and ensure that any personal information or sensitive personal data, or information found to be inaccurate or deficient, shall be corrected or amended as feasible'. However, this will only apply to those data subjects who are the 'provider of the information', and not to all data subjects.
(p.419) *(7) Options to refuse or withdraw consent (rule 5(7)).* Companies must provide 'an option to the provider of the information to not to [*sic*] provide the data or information sought to be collected', and later 'to withdraw its consent given earlier'. The body corporate can then refuse to provide goods or services. This applies to all personal information.
(8) Security (rule 5(8)). Companies must 'keep the information secure'. The scope of this rule is ambiguous, but it probably applies to all personal information, on the same reasoning as applied to rule 5(3).
(9) Complaint handling (rule 5(9)). Companies do not have any obligation to address and respond to any complaints by data subjects (no matter what the other rules say), unless they are complaints by 'their provider of the information'.

Disclosure limitations and exceptions (rule 6)

Companies disclosing 'sensitive personal data or information' to any third party require prior permission from the provider of the personal data who has provided such information under lawful contract or otherwise to the body corporate. Disclosures agreed by contract between the provider of the information, or necessary for compliance with a legal obligation, are also allowed. Companies must not 'publish' sensitive personal information (presumably meaning they must not make it generally available to the public). Third parties receiving sensitive personal data under this Rule 'shall not disclose it further'. A proviso to rule 6(1) provides an exception for disclosure where the information is 'shared' 'with Government agencies mandated under the law to obtain information including sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences'. From a data subject perspective, these limitations are valuable (and the exceptions not unusual) where they have provided their data directly to a controller, but rule 6 imposes no limitations on disclosures by controllers of any personal information they have collected from other sources. Normal data protection laws impose restrictions on disclosure of any personal information—but this is not such a law.

'Reasonable security' defined (rule 8)—'accountability' for security

The IT Act makes the meaning of 'reasonable security practices and procedures' depend on the existence of regulations. Rule 8(1) provides such a definition:

> A body corporate or a person on its behalf shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business. In the event of an information security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies.

On its face, rule 8 requires the company to 'have implemented' such a security programme, not merely to pay lip service to one. Presumably, negligent failure[64] to implement such a **(p.420)** programme, if proven to cause the requisite damage, will constitute a breach of section 43A.[65] Those who comply with either implementation approach allowed,[66] 'shall be deemed to have complied with reasonable security practices and procedures', provided they also comply with specifically stated independent audit requirements.[67] Companies are therefore required to both have and to implement such a security programme and be able to demonstrate their compliance—one meaning of 'accountability'.

Privacy policies required (rule 4)

Under rule 4, a company or person acting on its behalf who 'collects, receives, possess[es], stores, deals or handle[s] [personal information] shall provide a privacy policy for handling of or dealing in user information including sensitive personal information and ensure that the same are available for view by such providers of information who has provided such information under lawful contract'.[68] The policy, to be published on a website, is not required to be accessible to data subjects per se, but only to providers of data under contract. Data subjects only have a right to seek a privacy policy from a party to which they provided their personal data.

Data export restrictions (rule 7)

It seems that, as in most data privacy laws, the exporter has to comply with both the disclosure principle (rule 6) and this data export principle (rule 7). Rule 7 imposes two conditions for a transfer of sensitive personal data (only—i.e. not all personal data) by a company in India to any body corporate or person 'located in any other country':

> (i) The recipient 'ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules'.
> (ii) The transfer (a) 'is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information', or (b) 'where such person has consented to data transfer' (presumably the provider).

Condition (i) is ambiguous about whether it is the country to which the data is exported that must ensure the same level of data protection, or whether the recipient company alone can provide such assurance, and if so, how it is required to do so. Also, since the whole of the Rules are so ambiguous (as explained in the preceding sections), it is an open question what 'the same level of data protection' means: if India's protection is very low, then rule 7 only requires a low standard. The value of rule 7 as data protection is also crippled by the fact that it only applies to sensitive personal data and not to all personal data. As well as **(p.421)** being largely useless to data subjects, it does not meet the 'restrictions on onward transfers' requirement of the EU Data Protection Directive's adequacy requirements because that requires application to all personal information. The only exceptions allowed are those in line with Article 26 of the Directive, and a restriction to sensitive personal data is not such an exception.

Condition (ii) means nothing except that there must be a lawful contract for export. The consent of the data subject is not required, only that of the data exporter, the 'provider of information'.

4. International data transfers from India

In addition to the limited impact of rule 7, there are other factors relevant to international personal data transfers and India. Indian law provides no significant protection against the personal data of Indian citizens being transferred overseas (except for 'sensitive' data). There are no general restrictions applying to all private sector personal data, nor any applying to all public sector personal data.

4.1. Extraterritorial application (sections 75(1) and 1(2))

The IT Act asserts in section 1(2) that it has unlimited territorial jurisdiction and 'applies…to any offence or contravention [under the Act] committed outside India by any person', save as otherwise provided in the Act. The substance of this provision is repeated in section 75(1) but section 75(2) limits this to where 'the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India'.[69] Given the proviso to section 1(2), it seems likely that section 75(2) also limits the scope of section 1(2), unless section 1(2) deals with the person and section 75(2) deals with the cause of action arising in India. It would be entirely sensible for an extraterritoriality provision to require computers in India to be used before India asserted jurisdiction, but for this to apply irrespective of the location outside India from which the person controlled the computer.

4.2. Indian contract law—privity, choice of law, and outsourcing

The Indian Contract Act 1872, and Indian contract law in general, does not specifically recognize the concept of a 'third party beneficiary', which allows a third party to sue for enforcement of a contract made for its benefit.[70] This is sometimes referred to as the requirement of 'privity of contract'. Indian courts have unevenly applied the doctrine of privity, but usually uphold it,[71] with exceptions not very relevant to privacy protection. Calls for reform have not been followed.[72] Where a contract between an overseas data controller and an Indian processor creates data protection obligations on the Indian outsourcer, data subjects cannot enforce those obligations if the Indian company breaches the data protection obligations, under a contract made under Indian law. If the law of the **(p.422)** contract is the law of the UK or any other country that protects 'third party beneficiaries', it may be that the data subject can enforce those rights in the courts of the foreign country concerned, or in an Indian court which is willing to enforce the contract applying the law of the foreign country as a matter of private international law. The position is similar when personal data of an Indian data subject is exported for overseas processing.

5. Other privacy provisions in the Information Technology Act

There are a number of other provisions in the IT Act (as amended by the ITAA 2008) relevant to privacy, other than section 43A and the Rules made under it.

5.1. Disclosure restrictions—private and public sectors (IT Act sections 43(b) and (g) and 66)

Section 43(b) provides for a civil action for compensation payable to a data subject when a person, without permission of a computer system owner or operator, 'downloads, copies or extracts any data' so that harm to the data subject results. It is available to data subjects where unauthorized access to any extraction of personal data occurs, against the person who accessed the data. The same action is available against any other person who improperly assists a person to obtain access to a computer system, etc.[73] The computer system in question may be owned or operated by either a private sector or public sector body (unlike the restriction of section 43A to a 'body corporate'). Section 66 adds a criminal offence punishable by imprisonment or a Rs 500,000 (US$8,000) fine (or both) wherever a person 'dishonestly or fraudulently' breaches section 43.

5.2. Disclosure restrictions—private sector (IT Act sections 72A and 72)

It is an offence, subject to any other legislation in force, where 'any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person'.[74] So a disclosure may be an offence even if it is not in breach of the contract, provided (i) it is without the consent of the data subject, and (ii) it is made with the requisite intent. It is punishable by up to three years' imprisonment or a fine of up to five lakh rupees (US$8,000), or both. Complaints are often made to police under this section, but the outcomes are unknown.[75]

The section is potentially quite broad. The condition that the offender is a person 'providing services under the terms of lawful contract' would include (i) a business located in India (whether locally owned or an overseas 'captive' business) providing any form of services to its customers (whether local or overseas customers) pursuant to an express or implied contract with them; and (ii) an Indian business providing processing services (i.e. an intermediary) for an overseas data controller under an outsourcing contract. The broad **(p.423)** definition of 'intermediary' further extends the scope of the section. Any disclosure of personal information about data subjects without their consent, is therefore potentially a criminal offence if the act of disclosure occurs while the services are being provided by them. This would not criminalize further disclosures by third parties who subsequently received the data, only disclosures by the data controller or intermediary/data processor. It will rarely apply to public bodies because they do not usually obtain people's personal information 'while providing services under the terms of a lawful contract'.

However, there are important limiting factors to this offence. The relevant intent is to cause 'wrongful loss or wrongful gain'. The wrongfulness of either the loss or the gain may be difficult to prove in cases where personal information has been disclosed, for example, only so that it can be used for an otherwise legitimate commercial purpose such as direct marketing, rather than for some more obviously wrongful purpose such as credit card fraud. Whether direct marketing may be construed as wrongful gain because it arises from uses other than under the lawful contract, is uncertain but is arguable. The lack of any significant restrictions on what personal information can be collected in India also means that it is more difficult to argue that disclosures for the purpose of someone else's collection is in itself causing 'wrongful loss' to the data subject. The offence also only occurs if there is disclosure of the information, as distinct from use of it for a wrongful purpose by the party securing access to it—so it is a wrongful disclosure offence, not a wrongful use offence. It is unlikely that there would be data subject consent, at least in circumstances where the requisite ('wrongful') intent was also present. However, if the data subject had given a broad consent to further commercial use of personal information at the time the information was collected, consent could exist (in which case the gain would not be 'wrongful' in any event). 'Consent' is not defined in the IT Act.

5.3. Protection against third party access to or alteration etc. of data (IT Act section 43)

Section 43 also creates a civil action which allows a data subject (as well as a system owner or operator) to take action against any third party who acts without permission to access data, or do a wide range of things which could cause alterations to personal data, or otherwise interfere with the utility of that personal data, including the following:[76]

(i) 'accesses, downloads, copies or extracts data';
(ii) 'damages' the personal data, where 'damage' is defined to mean 'to destroy, alter, delete, add, modify or rearrange any computer resource by any means';
(iii) any form of 'damaging' or 'disrupting' any computer resources, or causing access to them to be denied, or introducing viruses (broadly defined);
(iv) causing one person to be charged for services 'availed of' by another person.

Almost any unauthorized actions affecting a computer system which would affect the value of a person's personal data, or result in other harm to the person, can result in a section 43 compensation action, assuming that the person responsible can be identified. Such a third party is liable to pay compensatory damages not exceeding Rs 10,000,000 (US$200,000) 'to the person so affected'. The relevant damage will be different depending on whether a system operator or a data subject utilizes the provision. In one section 43 case the Delhi High Court awarded significant damages for injuries that seemed to include interference **(p.424)** with privacy, resulting from theft of a computer.[77] Section 66 adds a criminal offence punishable by imprisonment or a Rs 500,000 (US$8,000) fine (or both) wherever a person 'dishonestly or fraudulently' breaches section 43. These protections apply in relation to both public sector and private sector computer systems.

5.4. Criminal offences by third parties in relation to personal data (IT Act sections 66, 66B)

The IT Act provides in section 66 for an offence where a person dishonestly or fraudulently does any act referred to in section 43 (as discussed earlier). A new criminal offence is created by the 2008 Amendments where a person 'dishonestly received or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen'.[78] Those involved in dealing with unlawfully obtained personal data, or even data resulting from data leaks, could be prosecuted under this section. Sections 66 and 66B are therefore also complementary: section 66 deals with those who breach system security, and section 66B deals with those who subsequently attempt to profit from data. Valuable though these provisions are, they are not directly relevant to the question of implementation of the security principle, which is concerned with the obligations of data controllers and service providers.

5.5. Identity offences (IT Act sections 66C and 66D)

Identification frauds of various types are becoming one of the most significant threats to the integrity and 'quality' of a person's personal data. The ITAA 2008 creates new offences concerning misuse of identity information, carrying penalties of up to three years' imprisonment or a fine of up to one lakh rupee (US$2,120), or both. One offence is where a person 'fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person'.[79] This is an 'identity misuse' provision which should have a wide ambit to deal with misuse of credit card numbers, driver's licence numbers and the like due to the breadth of 'any other unique identification feature'. It is probably broad enough to deal with the combination of a person's name and address. The other covers other forms of 'identity misuse' wherever a person 'by means for any communication device or computer resource cheats by personating'.[80] Logging into a person's account by use of any information

such as usernames and passwords would be covered by this, even if the information used could not be said to constitute a 'unique identification feature'.

6. Enforcement under the IT Act in India

The enforcement structure of the IT Act (as amended by the ITAA) is largely the same for both civil remedies (compensation) and for offences and penalties, and applies to section 43A and its Rules, as well as to section 43 and other provisions under the IT Act discussed in the previous section. This section first considers the four-tiered enforcement structure established by the IT Act: company 'Grievance Officers'; state Adjudicating Officers (AOs); the Cyber Appellate Tribunal (CAT); and appeals and removals to the courts. It then **(p.425)** considers the civil remedies and offences under the Act, and how they apply in relation to data protection.

6.1. Grievance Officers in companies (IT Act section 43A and rule 5(9))

Any company in India that deals with 'sensitive personal information' must 'address any discrepancies and grievances of their provider of the information with respect to processing of information in a time bound manner', and must appoint 'a Grievance Officer who shall redress the grievances…within one month'.[81] A Grievance Officer is therefore the first tier of complaint handling in this system, one element of the role of a Data Protection Officer in proposals currently under consideration in the EU. There are limitations on the scope of the obligation: it applies only to companies that deal with 'sensitive personal data', not any personal information; data subjects can only use the provision where they have provided the information to the company; and Grievance Officers need not deal with them in relation to personal information obtained from other sources.

6.2. Adjudicating Officers (AOs) under the IT Act

Contraventions of any provisions of the Act, 'or of any rule, regulation, direction or order made thereunder which renders him liable to pay compensation', are to be heard by an Adjudicating Officer (AO) to be appointed by the Central Government, which must hold an inquiry in a manner to be prescribed.[82] AOs must have 'experience in the field of Information Technology and legal or judicial experience'.[83] AOs have the same powers of a civil court conferred on the CAT, and proceedings before an AO are deemed to be judicial proceedings and to be before a civil court.[84] The Indian government did not make appointments of either AOs or CATs for over two years, only doing so in 2003 after being ordered to do so by the Mumbai High Court in 2002.[85]

The Rules for eligibility for appointment as an AO require appointees to hold a position 'not below the rank of Director' in the central government or equivalent in a state government, and to have other appropriate academic or professional qualifications.[86] The Secretary of the Department of Information Technology of each state and union territory was appointed as an AO and required to provide the necessary infrastructure.[87] There are therefore 35 AOs so appointed. 'Enquiry Rules' govern the procedures that AOs are to follow,[88] but these have not yet been used in relation to any data privacy issues.[89] After nearly a decade of operation of the AO system, with an average of about 13 decisions being made per year across India (a total of 125) by 35 AOs, there are only four of these **(p.426)** decisions readily available, and none are on privacy issues, as documented elsewhere,[90] and as noted by other analyses.[91] It is exceptionally difficult for anyone to assess the operation of the AO system under the IT Act, or the likely consequences of breaching its provisions. It is therefore a complaint system almost completely lacking in transparency.

6.3. The CAT and appeals to the courts

Anyone aggrieved by an order of an AO may appeal to a Cyber Appellate Tribunal (CAT),[92] which comprises a chairperson, with qualifications as a High Court judge, and other members as appointed, with information and communications technology (ICT) and legal qualifications.[93] Tribunals are not to be bound by civil procedure laws 'but shall be guided by the principles of natural justice',[94] and with the same powers as are vested in a civil court.[95] The CAT does not have any original jurisdiction,[96] but only hears appeals against decisions of AOs. Rules for the procedure of the Cyber Appellate Tribunal[97] have been made.[98] There is a right of appeal to the High Court from CAT decisions.[99]

Only one CAT has been appointed, located in Delhi. The CAT is in practice defunct, as at December 2013. It has not delivered any decisions, and seems not to have heard any new matters, since 30 June 2011.[100] A bench of the CAT cannot hear a matter without the chairman as part of that bench.[101] The CAT has not had a chairperson since 30 June 2011, and has therefore been unable to hear any matters.[102] It is claimed that this is because the Chief Justice refuses to consent to the Union Law Minister's nominee for chairman, and the minister refuses to nominate an alternative candidate.[103] The lack of a CAT chairperson means that the Indian data privacy system under section 43A and the Rules, and under other sections of the IT Act, has been largely non-functional for at least two and a half years, from approximately the time that the section 43A Rules came into effect. The CAT may at some point become

functional again. This makes the value of the whole structure under the IT Act questionable, because any company that is aware of the situation will know that, even within the exceptionally limited scope that data subjects have to exercise any rights, they cannot do so effectively.

6.4. Civil remedies under the IT Act—compensation for breaches

Actions for compensation for breaches of data privacy by data subjects can arise not only under section 43 (concerning actions by third parties) and section 43A (concerning actions by data controllers/processors) but also under section 45, a residuary provision providing that any contraventions of the Act or Rules for which 'no penalty has been separately **(p.427)** provided' may result in compensation or a penalty not exceeding Rs 25,000 (US$456). Neither section 43 nor section 43A place a limit on the amount of compensation that may be ordered, but section 46(1A) provides that AOs only have jurisdiction to hear matters where the claim for compensation does not exceed 5 crore rupees (just over US$1 million). Where damages claimed exceeds that, only a competent court has jurisdiction. Realistically, most claims for privacy breaches will fall within the jurisdictional limit of the AO.

6.5. Offences and penalties under the IT Act

As discussed in section 5.3 of this chapter, a broad range of actions done 'dishonestly or fraudulently' in breach of section 43, can be criminal offences under section 66 and punishable by very significant fines or imprisonment. AOs can only provide compensation, and cannot convict respondents for offences. Where an AO is 'convinced that the scope of the case extends to [offences]…needing appropriate punishment instead of mere financial penalty' he or she is to 'transfer case to the Magistrate having jurisdiction to try the case, through Presiding Officer'.[104] Such referrals do occur,[105] but is difficult to obtain details of investigation and prosecution of offences under the IT Act.[106] There is no equivalent provision criminalizing breaches of section 43A or the Rules.

7. Other legislation relevant to data protection in India

No other Indian legislation is of major significance to the protection of privacy, but there are a variety of Acts of some significance and effectiveness in particular areas, on which more details are available elsewhere.[107]

7.1. The Right to Information Act 2005—a much used law

India's 'right to information' legislation resulted from a broad popular campaign, prompted by evidence that funds meant for village development were being routinely misappropriated. From 1996 a national network of journalists, lawyers, bureaucrats, and NGO activists advocated the removal of the Official Secrets Act 1923 and for access to official information to be made possible. As the PI Report puts it:[108]

> India has had the good fortune of being home to a number of very resilient civil society movements which have over the years tenaciously fought for and achieved transparency. It was owing to the efforts of one of these movement spearheaded by the Mazdoor Kisan Shakti Sanghatan (MKSS), and joined by various organizations across the nation, that India finally passed the Right to Information Act in 2005, which has ushered in an unprecedented era of openness in government affairs.

(p.428) A number of states enacted access to information Acts from 1997 to 2004,[109] covering what is elsewhere called 'freedom of information', in relation to the public sector. In 2004 India's Supreme Court conclusively interpreted article 19(1)(a) of the Constitution of India to impliedly include the right to information in the constitutional guarantees of freedom of speech and expression (*People's Union for Civil Liberties v Union of India*),[110] five years before a similar conclusion was reached in Europe.[111] National legislation was then enacted by the Centre as the Right to Information Act 2005 (RITA).

The Indian legislation only provides a right of access to personal information, not a right of correction. It also provides protection against disclosure of personal information of third parties when right to information (RTI) requests are made. The 'right to information' provided by the 2005 national legislation has a broad scope, covering 'information held by or under the control of any public authority'.[112] 'Public authority' includes any body established under the Constitution, or Centre or state law, or under delegated legislation, and includes bodies owned or controlled by government or directly or indirectly substantially financed by government (even if they are NGOs).[113] The reach of the legislation is therefore to all tiers of government and somewhat beyond that.

The Central Information Commission (CIC) is clearly an activist and independent[114] organization administering a very heavily used piece of legislation. Its website[115] contains an exceptionally broad and informative collection of information about administration of the Act, including standards for administration of penalties. By October 2012 the CIC had already published 89,336 reasoned decisions since 2006,[116] more than 12,000 per year, and of those over 700 referred to privacy.[117] The RTI commissions are significant because these tribunals could possibly play a role in

a future general Indian data privacy law. Their track record of successful operation in the related field of access to information could prove invaluable. The CIC has the attributes that would be looked for in an appeals tribunal from a data protection authority, but with very limited powers of complaint investigation. At present it only operates in the limited area of rights of access in the public sector.

7.2. Credit Information Companies (Regulation) Act 2005—an ignored law

In contrast, the Credit Information Companies (Regulation) Act 2005 (CICRA), operational since 2006,[118] is the only Indian legislation, other than the IT Act, to provide a comprehensive data protection code. Despite the complexity of the Act, Regulations, and those Rules already published, none of them have any specific provisions for consumers to **(p.429)** make complaints, receive assistance, or have remedies awarded in their favour. There are provisions for penalties. There are no Reserve Bank of India (RBI) Circulars, Press Releases, or Master Circulars dealing with the consumer aspects of credit reporting,[119] other than some vague promises.[120] There is nothing on the RBI website about credit reporting dispute resolution. It seems therefore that the RBI takes a very passive role (put charitably) in relation to the Act. Similarly, the websites of Indian credit bureaus do not mention the Act or dispute resolution procedures. In all, credit reporting law is a disreputable aspect of the Indian system. A supervisory system is needed to deal with many thousands of complaints and disputes each year—perhaps hundreds of thousands, given India's population—if the credit reporting data protection system is to have any substance. Some aspects of CICRA could have provided a model for a more general data protection law for India, but it is not so. Although CICRA has been in force for over seven years, there is no evidence that it is effectively operational except as a tool for the RBI to require Indian financial institutions to participate in a credit surveillance system. The RBI has a conflict of interest in both promoting and (supposedly) regulating this surveillance system.[121] Another regulator is needed.

7.3. The Protection of Human Rights Act 1993

The Protection of Human Rights Act 1993 (PHRA) defines 'human rights' by reference to India's obligations under its Constitution and international commitments, and is therefore broad enough to include ICCPR Article 17 concerning privacy.[122] It establishes the National Human Rights Commission (NHRC)[123] which has the power to investigate alleged violations[124] and can recommend that the government or authorities pay compensation, commence prosecutions, and approach courts for directions, orders, or writs. It has no independent powers to take remedial actions. Complaints can also be made to state Human Rights Commissions. The NHRC has not had any major involvement in data privacy issues, other than making submissions on the ID number, but it has had a very significant involvement in Supreme Court decisions concerning compulsory DNA testing, lie detector tests, and related matters, with its guidelines having been adopted by the Supreme Court.[125] No privacy issues are included in the hundreds of cases heard by it and summarized on its website since 1993.[126] Its focus has been, and is, on wrongful deaths and other extreme violations.

7.4. The National Consumer Disputes Redressal Commission

The National Consumer Disputes Redressal Commission (NCDRC) was established under the Consumer Protection Act 1986 to promote and protect the rights of consumers, and to enable 'ordinary consumers to secure less expensive and often speedy redressal of their grievances'.[127] Complaints may be made by consumers in relation to an 'unfair trade **(p.430)** practice' which is defined broadly enough to cover many types of complaints about misuse of personal data. There is a very decentralized system of District Forums with appeals to State Commissions and thence to the National Commission in Delhi. Decisions from all three levels of the CDRC (national, state, and district) are published on the Internet.[128] A simple search (e.g. for 'privacy') confirms that the tribunals at the different levels do make decisions (with short, reasoned judgments) concerning many consumer disputes involving privacy issues such as unsolicited issuing of credit cards, privacy rights of hospital patients as consumers, and failure to observe direct marketing restrictions.

In the *Nivedita Sharma Case*[129] the Delhi State Commission held that both a mobile telephone service provider (Bhari) and two financial services companies (ICICI and Amex) were in breach of the provisions in the Act in relation to unfair trade practices and defective provision of services because of the provision by Bhari of personal details of its telecommunications customers to the two financial services providers, contradicting the statement in Bhari's terms of service that it 'does not disclose your personal information' to others. Kapoor J held both sides of the transaction in breach for 'deficiency in service and unfair trade practice'. Viswanathan[130] considers that such large-scale trafficking in personal data was a 'fairly common practice' of Indian mobile phone operators in 2006, as indeed the CDRC seemed to assume. On appeal, the main privacy protection aspects of the judgment were not challenged.[131] The Delhi CDRC ordered the Cellular Operators Association of India, a party to the case on behalf of its members, to inform all its members to cease using for telemarking or any other purposes, any such list of subscribers and their mobile telephone numbers provided to them by banks, financial companies, etc. It also

ordered the Telecommunications Regulatory Authority of India to establish a 'Do Not Call' Registry, which it has done. The case illustrates the breadth of orders that Indian courts and tribunals are accustomed to making, and how this has the potential for data protection developments to be initiated by the judiciary.

7.5. State laws and other sectoral laws

The union territory of Chandigarh, a 'city state', has become the first Indian state or territory to implement a data privacy law. The administration of the Chandigarh union territory sought comments from the police before communicating its consent to the Ministry of Home Affairs on the Right to Privacy Bill, 2011. According to press reports, the new law will bar collection of personal information by any agency by unlawful means, as well as using or disclosing information on a person's private affairs. Spying on or following someone in a manner likely to harass him or her or photographing someone while he or she is in their private premises is also covered.

Apart from the non-functioning credit reporting legislation, there is little sectoral law. The Public Financial Institutions Act 1993 codifies banking confidentiality. Under telecommunications legislation, the Telecom Regulatory Authority of India has developed the Common Charter of Telecom Services[132] which provides that 'All Service Providers assure **(p.431)** that the privacy of their subscribers (not affecting the national security) shall be scrupulously guarded'; however, the Charter is non-justiciable.

7.6. Non-legislative protections—self-regulation, trustmarks, etc.

There has been no significant development in India of self-regulation aimed at providing protection to data subjects. The main concern of industry bodies such the DSCI is self-regulation of the relationship between the overseas data controllers providing personal data for processing in India and Indian processors. DSCI's current proposals are contained in the DSCI Framework for Data Protection[133] and DSCI Security Framework.[134] DSCI claims that its Privacy Framework does 'address consumer privacy protection',[135] but this statement is incorrect. A more accurate statement is that 'The DSCI Framework is specially aimed at data protection practices for companies engaged in outsourcing, with a view to assure controllers of information from outside of India, that Indian companies are familiar with basic processor practice requirements and have developed model practices to ensure security and appropriate data use'.[136] 'Organisations are also required to remedy problems arising out of a failure to comply with the Principles',[137] but the only apparent sanction is suspension of DSCI membership. There are no provisions for data subjects to request a remedy. There is little evidence of take up of the Privacy Framework by DSCI members. The Framework may have some indirect benefits for consumers, but that is not its purpose.

Privacy seals or 'trustmarks' are also not important in India. Some Indian companies are members of the TRUSTe privacy seal programme. No Indian privacy seal or certification programmes are known.

8. Proposals for comprehensive legislation in India

Indian government spokespersons have at various times since 2003[138] stated that data protection Bills have been drafted, but none have ever been introduced into the legislature. Since 2011 there have been three significant steps toward such legislation: (i) a draft 'The Right to Privacy Bill', 2011 drafted by the Department of Personnel and Training and considered (largely favourably) by the Committee of Secretaries (2011); (ii) recommendations for a Bill from a report by a government-appointed 'Group of Experts' chaired by former Justice A.P. Shah (2012),[139] and (iii) a non-official Bill developed in 2013 by a civil society organization, the Centre for Internet & Society, Bangalore.[140] In February 2014 a revised and strengthened version of the 2011 'The Right to Privacy Bill', **(p.432)** which takes into account the Shah Committee recommendations, became available unofficially.[141]

While these four Bills have their differences, their many similarities include coverage of both public and private sectors, a data protection authority (DPA), a conventional definition of 'personal information', and privacy principles generally up to 'minimum' OECD standards. They differ somewhat on the range of enforcement methods and whether individuals would have court actions available. Modest improvements could bring any of them to an international standard. None of these draft Bills have yet been adopted as government proposals. By and large, they are all proposing 'normal' data privacy laws such as are found in most of the more than 100 countries with such laws. These Bills and proposals would fit somewhere on the spectrum from 'weak' to 'moderately strong'. The most likely future for data privacy in India is that it will go down this path. Detailed comparisons are not included here as they are only proposals and as yet not introduced to Parliament.

9. Conclusions and future directions

The future shape of data privacy in India is unlikely to be based on the incoherent Rules under section 43A of the IT Act, and its moribund enforcement vehicle, the CAT. In their current form they provide only a smokescreen or illusion of protection. They were a knee-jerk attempt to provide data protection via delegated legislation in a political

environment where legislative gridlock meant legislation was impossible. As data protection legislation they are a failure. Until India's 2014 election is held and a new government formed, future directions will remain unclear.

9.1. Trade and adequacy

India's outsourcing industry is of considerable national economic importance, but is facing strong economic challenge from countries such as the Philippines. It also faces legal impediments, because of the European Union's restrictions on exports of personal data from EU member states to countries which have not been held to provide 'adequate' data protection at least to the standards of the 1995 EU Data Privacy Directive. India's laws were not found to be 'adequate' in a previous EU study in 2010.[142] A further expert report was obtained by the EU in 2013, and according to the DSCI:[143]

> India and EU have appointed an Expert Group comprising experts from both the sides to discuss the findings of the EU Data Adequacy report on Indian data protection regime. With representation from DSCI and NASSCOM, the group will also review the periodic progress made by EU and India on the implementing the recommendations of the Expert Group with the ultimate objective of exploring the possibility of provisional adequacy and specific arrangements for IT/BPM sector. First meeting is proposed in Feb 2014 in Brussels.

India has tried to link what it calls 'data secure status' to its negotiations for a proposed EU-India Free Trade Agreement, but EU representatives have stated that adequacy status is not **(p.433)** a matter that can be included in trade negotiations,[144] which seems to be clear from the Directive. The Free Trade Agreement negotiations are reported to be 'in suspended animation' at least until the 2014 Indian elections are held.[145]

9.2. Trade-offs between privacy and surveillance

At the end of 2013, India has conflict at every level over privacy issues: between Parliament and Executive, the Courts and Executive, over the ID card; between the EU and India over adequacy; and within and outside the Executive over the shape of a comprehensive law. A common solution in other countries to such impasses (other than a complete change of the political landscape) has been political compromises resulting in a 'package' of legislation to legitimate an ID system, accompanied by something like a 'normal' data privacy law including a DPA and at least the minimum set of principles. This might also assist India to secure the trade benefits of an 'adequacy' determination by the EU. No one in India is yet proposing such a package, but it is not uncommon for privacy laws to be the trade-off for laws increasing surveillance. Potential trade benefits would increase the attraction to some business and political groups. Whether consumers would benefit overall would depend on the details of the compromise. However, the Supreme Court's findings of unconstitutionality of the current ID number operation, and the claims by opposition politicians that it may be scrapped after the election, mean that the ID number might not be any part of India's future development of data privacy. The position continues to be 'confusion rules'.

Notes:

([1]) *CIA World Factbook*, 'India' <https://www.cia.gov/library/publications/the-world-factbook/geos/in.html>.

([2]) *CIA World Factbook*, 'India', states fifth largest GDP and 56 per cent; Wikipedia, 'Economy of India' entry, 2009, and references cited therein, state fourth largest by GDP at 54 per cent in 2009.

([3]) See generally, A. Viswanathan, *Outsourcing to India: Cross-Border Legal Issues* (LexisNexis Butterworths, 2008).

([4]) The value of EU–India trade grew from US$40 billion in 2003 to US$56 billion in 2011, and trade in commercial services tripled during the same time period, reaching US$25 billion by 2010.

([5]) EU–India trade statistics on Europa <http://ec.europa.eu/trade/creating-opportunities/bilateral-relations/countries/india/>.

([6]) For on overall introduction to Indian history, see John Keay, *India: A History* (HarperPress, 2000, updated edn. 2010).

([7]) For post-colonial history see Bipan Chandra, Mridula Mukherjee, and Aditya Mukherjee, *India Since Independence* (Penguin, 2008); John Pike, *Empires at War: A Short History of Modern Asia Since World War II* (I B Tauris, 2010), chs. 5, 23, 29, 53, and 56; and Y.K. Malik et al., *Government and Politics in South Asia* (Westview Press, 2009), pp. 11–146.

([8]) Pike, *Empires at War*, pp. 651–9, Chandra, Mukherjee, and Mukherjee, *India Since Independence*, pp. 475–89.

([9]) John Keane, *The Life and Death of Democracy* (Pocket Books, 2009), pp. 585–647.

([10]) For surveys of the Indian legal system, see V. Ramakrishnan, 'Guide to Indian Laws' (GlobaLex, January 2006) <http://www.nyulawglobal.org/globalex/india.htm>; K.N.C. Pillai (Ed.), *Indian Legal System* (2nd Edn., Indian Law Institute, 2006); Chandra et al., *India Since Independence*, chs. 4 and 5.

([11]) Chandra et al., *India Since Independence*, pp. 41–59.

([12]) Ramakrishnan, 'Guide to Indian Laws', section 'Primary sources'.

([13]) 'The judgments of a State High Court are binding on itself and on all subordinate courts and tribunals in the State. However a numerically larger bench of the High Court can overrule a decision of a numerically smaller bench. Judgments of a High Court are not binding on another High Court or on courts subordinate to another High Court, but are of great persuasive value': Ramakrishnan, 'Guide to Indian Laws', section 'Secondary sources'.

([14]) See section 7.2 of this chapter. For details of the surveillance aspects see Graham Greenleaf, 'Promises and Illusions of Data Protection in Indian Law' (2011) 1(1) *International Data Privacy Law*, pp. 47–69, at pt. 3.2 'Credit Information Companies (Regulation) Act 2005' <http://ssrn.com/abstract=2133915>.

([15]) Sunil Abraham and Elonnai Hickok, 'Government Access to Private Sector Data in India' (2012) 2(4) *International Data Privacy Law*, pp. 302–15 <http://idpl.oxfordjournals.org/content/2/4/302.full>; Privacy International, *India—Country Report 2012* (Privacy International, London, 2012) <https://www.privacyinternational.org/reports/india-0>; R. Gupta, 'A Gathering Storm—How UID Will Transform India into a Police State' (*Desicritics.org*, 2010) <http://bourgeoisinspirations.wordpress.com/2010/03/22/how-uid-will-transform-india-into-a-police-state/>.

([16]) Ursula Rao and Graham Greenleaf, 'Subverting ID from above and below: The Uncertain Shaping of India's New Instrument of E-governance' (2013) 11(3) *Surveillance & Society* <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2350631>; Graham Greenleaf, 'India's National ID System: Danger Grows in a Privacy Vacuum',(2010) 26(5) *Computer Law & Security Review*, pp. 479–91 <http://ssrn.com/abstract=1964046>.

([17]) *Justice K.S. Puttaswamy (Retd) v Union of India & Ors*, WP (c) 494/2012. The Court's order is available, but no written judgment was provided.

([18]) 'Await SC Verdict on Linking Aadhaar Card, Bank account' (New Indian Express, 24 January 2014) <http://www.newindianexpress.com/states/tamil_nadu/Await-SC-Verdict-on-Linking-Aadhaar-Card-Bank-account/2014/01/24/article2016973.ece>.

([19]) Supreme Court decision 24 March 2014, three-judge bench headed by Justice B.S. Chauhan (report not yet available).

([20]) 'Withdraw orders making Aadhaar mandatory for any service: Supreme Court tells Centre' (India Today, 24 March 2014) <http://indiatoday.intoday.in/story/data-collected-for-aadhar-confidential-supreme-court-centre/1/350993.html>.

([21]) Privacy International, *India—Country Report 2012*, section 'Identity documents'.

([22]) Abraham and Hickok, 'Government access to private sector data in India'.

([23]) H. Gupta, 'Chidambaram has his way as National Intelligence Grid gets PM's okay' (Daily News & Analysis (DNA), 12 May 2010) <http://www.dnaindia.com/dnaprint910.php?newsid=1382016>.

([24]) CRID, University of Namur (with Indian expert consultants), 'First Analysis of the Personal Data protection Law in India' (Report to the Directorate General, Justice, Freedom and Security, European Commission (CRID, 2005)) <http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/final_report_india_en.pdf>, p. 21. The central government has legislative power to implement treaty provisions in domestic law (Constitution (India), art. 253).

([25]) *People's Union for Civil Liberties (PUCL) v The Union of India & Anr* [1996] INSC 1637 per Kuldip Singh, J.

([26]) *Kharak Singh v The State of U. P.* [1962] INSC 377; 1963 AIR 1295 (per Subba Rao and Shah, JJ).

([27]) Constitution (India), arts. 19(1)(a) and 19(1)(d) respectively.

([28]) *Maneka Gandhi v Union of India* (1978) AIR 1978 SC 597.

([29]) Constitution (India), art. 19(1)(a); art. 19(2) also permits the state to impose reasonable restrictions on the exercise of the rights conferred by art. 19(1).

([30]) *Ram Narain v State of Bombay* (1952) SCR 652.

([31]) *District Registrar and Collector, Hyderabad & Anr v Canara Bank & Ors* (2005) 1 SCC 496.

([32]) *Naz Foundation v Government of NCT of Delhi* [2009] INDLHC 2450; WP(C) No.7455/2001 (High Court of Delhi, 2 July 2009) <http://www.liiofindia.org/cgi-bin/disp.pl/in/cases/dl/INDLHC/2009/2450.html>.

([33]) For more detail of this and earlier cases, see Graham Greenleaf, 'The Naz Foundation Case: Delhi High Court Ruling Expands India's Constitutional Privacy Rights' (2009) 100 *Privacy Laws & Business International Newsletter*, Issue 100, pp. 24–5 <http://ssrn.com/abstract=2027877>.

([34]) *Naz Foundation Case* (High Court of Delhi), para. 40.

([35]) *Koushal v Naz Foundation* (2013) Civil Appeal No.10972 of 2013 and other matters (Supreme Court of India, 11 December, 2013) <http://indiankanoon.org/doc/58730926/>.

([36]) Details of some cases noted in this and the next paragraph were provided by Mr Vakul Sharma.

([37]) *Bhabani Prasad Jena v Convenor Secretary, Orissa State Commission for Women & Anr*, AIR 2010 SC 2851; *Shri Rohit Shekhar v Shri Narayan Dutt Tiwari & Anr*, Delhi High Court, CS (OS) 700/2008, decided 23 December 2010.

([38]) *Radiological and Imaging Association v Union of India* 2011(113) BomLR 3107.

([39]) *G. Raman Alias Ramachandran vs The Superintendent of Police*, Madras High Court, 17 September 2012 <http://www.indiankanoon.org/doc/30170031/>.

([40]) See *Alarmelu Mangai v The Secretary to the Government of Tamil Nadu* where the Madras High Court ordered payment of Rs 5,00,000 (US$9,150) compensation for the public humiliation suffered by a woman as a result of an unjustified police raid on private premises and the resulting questioning at a police station.

([41]) M. Singh, ch. 6 'India—Protection of Human Rights against State and Non-State Action' in D. Oliver and J. Fedke (Eds.), *Human Rights and the Private Sphere: A Comparative Study* (Routledge, 2007), p. 182 consider that rights primarily available against private parties, or equally against them as against the state, include those in arts. 15(2), 17, 23, 24, 25, 26, 29(1), and 30(1).

([42]) Singh, 'India—Protection of Human Rights against State and Non-State Action', p. 180: 'it may be inferred that they involve state action and therefore are protections against the state'. Viswanathan, *Outsourcing to India*, p. 309: 'A right to privacy per se would give the wronged party a right to damages against another private party, unlike a constitutional right to privacy, which only gives rights to the State.'

([43]) *Petronet Lng Ltd v Indian Petro Group and Another* (13 April 2009) High Court of Delhi (Bhat J) <http://indiankanoon.org/doc/874488/>.

([44]) *P.U.C.L. v Union of India* [2003] INSC 173; 2003(3) SCALE 263: JT 2003 (2) SC 528.

([45]) For cases, see Greenleaf, 'Promises and Illusions of Data Protection in Indian Law', at p. 50, 'Tort law' <http://ssrn.com/abstract=2133915>.

([46]) In summary, breach of confidence may lie where there is public disclosure of personal information about which the data subject has a reasonable expectation of privacy irrespective of whether the data subject has imparted the information in circumstances importing an obligation of confidence on the recipient.

([47]) For cases, see Greenleaf, 'Promises and Illusions of Data Protection in Indian Law', pp. 50–1 'Breach of confidence law'.

([48]) See generally V. Sharma, *Information Technology Law and Practice* (3rd Edn., Universal Law Publishing, 2011);

Pavan Duggal, *Cyberlaw—The Indian Perspective* (2nd Edn., Saakshar Law Publishers, New Delhi, 2004).

([49]) Notice under s. 1(2) ITAA (India), *The Gazette of India*, 27 October 2009.

([50]) For a more detailed discussion see Graham Greenleaf, 'Illusions Squared: India's Failed Data Privacy Rules' (SSRN, 16 March 2014) <http://ssrn.com/abstract=2409736>.

([51]) IT Act (India), s. 87(2)(ob), as inserted by the ITAA.

([52]) GSR 313(E) dated 11 April 2011: Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (DEITY, 2011) <http://www.mit.gov.in/content/notifications>. They came into force on the date of their publication in the Official Gazette on 11 April 2011.

([53]) See Greenleaf, 'Illusions Squared: India's Failed Data Privacy Rules'.

([54]) IT Act (India), s. 2(1)(o).

([55]) 'Reasonable security practices and procedures' is defined in s. 43A to mean 'security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment'. This can be interpreted to mean that all of the Rules dealing with 'access, damage, use, modification, disclosure or impairment' are properly made under s. 43A. However, this broad approach is not consistent with the proviso in r. 8 that a body corporate or a person on its behalf, shall be considered to have complied with reasonable security practices and procedures if they have implemented certain 'security practices and standards'. If they have satisfied r. 8, then it would seem that they cannot be 'negligent' in relation to their obligations under s. 43A (the sole basis of liability under s. 43A). This would make all of the other Rules irrelevant because it would be impossible to breach them.

([56]) For details of the definitional change, see Greenleaf, 'Illusions Squared: India's Failed Data Privacy Rules'.

([57]) The Rules applying only to sensitive data are: consent to collection (r. 5(1)); lawful purpose of collection (r. 5(2)); (possibly) notice when collecting directly from the person (r. 5(3)); retention after expiry of purpose (r. 5(4)); disclosure (r. 6); and data exports (r. 7). Five rules and sub-rules apply (or possibly apply) to all personal information: privacy policies (r. 4); (possibly) use only for purpose of collection (r. 5(5)); access and correction (r. 5(6)); refusal or withdrawal of consent to processing (r. 5(7); (possibly) security (r. 5(8)) and r. 8 which applies to all 'information assets' including all personal information.

([58]) The Rules applying only to 'providers' of personal data are: privacy policies required (r. 4); consent (r. 5(1)); subject access and correction (r. 5(6)); options to withhold or withdraw consent (r. 5(7)); responding to complaints (r. 5(9)); use and disclosure limitations (r. 6).

([59]) These Rules (rr. 4, 5(1), 5(6), 5(7), and 5(9), and 6) will not apply to the data subject in any situation of outsourced processing, where the 'provider' is the data controller (located either in India or overseas), and there is a processor in India. This complexity is not necessarily a problem, because it may be reasonable that processors should not be liable for compliance with some data protection obligations, but only the data controller should be liable for such compliance. Put in its simplest form, the question becomes 'If a data protection principle (or Rule) is not adhered to, is there always at least one appropriate party (data controller or processor) against whom the data subject is able to take action to enforce his/her rights?' If the answer is 'yes', then the substantive goal of providing enforceable data protection rights will have been achieved. This requires an examination of each Rule.

([60]) If a company is involved in processing at least one form of 'sensitive personal data' then some of the Rules will apply to other personal information that it processes. But if it is not doing so, then it is difficult to see how even the rules that apply to 'personal information' can be enforced against that company.

([61]) 'Clarification on Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 under Section 43A of the Information Technology Act, 2000' (DEITY, 2011) <http://deity.gov.in/sites/upload_files/dit/files/PressNote_25811.pdf>.

([62]) On the unusual role of press notices in Indian law, see Greenleaf, 'Illusions Squared: India's Failed Data Privacy Rules'.

([63]) Data Security Council of India, *White Paper on EU Adequacy Assessment of India* (DSCI, 2012)

<http://www.dsci.in/taxonomy/term/713>, at pts. 7.1, 7.2, 7.3, 7.4, and 7.8.

([64]) There is no reference to negligent failure to implement in r. 8(1), the latter part of which requires companies 'to demonstrate' that they 'have implemented' the required standard. It is, however, hard to see how this Rule can override the requirement of negligence stated in s. 43A, and the requirement 'to demonstrate' should best be considered as a separate obligation relating to security, not as a reversal of the onus of proof.

([65]) There are already cases on s. 43 (not s. 43A) where courts have found that failure to maintain sufficient security on computer systems has resulted in a liability to compensate for financial loss due to fraudulent actions by third parties.

([66]) Rule 8(2) allows either compliance with IS/ISO/IEC 27001, or 'Any industry association or an entity formed by such an association, whose members are self-regulating by following other…codes of best practices for data protection as per [rule 8(1)] shall get its codes of best practices duly approved and notified by the Central Government'.

([67]) Rule 8(4).

([68]) Rule 4 requires that it must provide for: '(i) Type of personal or sensitive information collected under sub-rule (ii) of rule 3; (ii) Purpose, means and modes of usage of such information; (iii) Disclosure of information as provided in rule 6; and (iv) reasonable security practices and procedures as provided under rule 8.'

([69]) IT Act (India), s. 75(2). This is unusual in that it does not exclude where such equipment is merely used for the transit of data through India (compare e.g. art. 4(1)(c) of the EU Data Protection Directive).

([70]) B. Vagadia, *Outsourcing to India—A Legal Handbook* (Springer, 2007).

([71]) Prashant Iyengar assisted in obtaining this information on the current status of the doctrine of privity in India.

([72]) The Indian Law Commission in its 13th Report (1952) recommended the Indian Contract Act be amended to allow named third party beneficiaries to sue upon a contract, but no such amendments have been enacted.

([73]) IT Act (India), s. 43(g).

([74]) IT Act (India), s. 72A.

([75]) According to the Ministry (DEITY), in 2012 there were 46 'privacy related' 'cases registered by the Central Bureau of Investigation' under s. 72A, and 22 arrests; however, the number of prosecutions, or convictions, or the issues involved, were not given. See Standing Committee on Information Technology, *Cyber-crime, cyber-security and right to privacy* (52nd Report, 15th Lok Sabha, 2013–14), p. 11 <http://164.100.47.134/lsscommittee/Information%20Technology/15_Information_Technology_52.pdf>.

([76]) Respectively, IT Act (India), ss. 43(b), 43(d) and (v), 43(c)–(f), and 43(h).

([77]) *Shashank Shekhar Mishra v Ajay Gupta—CS(OS) 1144/2011* [2011] INDLHC 4294 (5 September 2011) <http://www.liiofindia.org/in/cases/dl/INDLHC/2011/4294.html>.

([78]) IT Act (India), s. 66B.

([79]) IT Act (India), s. 66C.

([80]) IT Act (India), s. 66D.

([81]) Rule 5(9): 'Body corporate shall address any discrepancies and grievances of their provider of the information with respect to processing of information in a time bound manner. For this purpose, the body corporate shall designate a Grievance Officer and publish his name and contact details on its website. The Grievance Officer shall redress the grievances or provider of information expeditiously but within one month from the date of receipt of grievance.'

([82]) IT Act (India), ch. IX (penalties, compensation, and adjudication), s. 46(1).

([83]) IT Act (India), s. 46(3).

([84]) IT Act (India), s. 46(5).

([85]) See website of Asian School of Cyberlaws at <http://www.cyberlawdb.com/gcld/category/asia/india-asia/>.

([86]) Rule 3, *Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003*, made 17 March 2003.

([87]) IT Act Notification NO 240, G.S.R.240(E) New Delhi, 25 March 2003 ('Order', no other title), available at <http://www.mit.gov.in/content/it-act-notification-no-240>; Appointments were made on 25 March 2003.

([88]) Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003, made on 17 March 2003; full copy not available on DEITY website but available at <http://www.naavi.org/importantlaws/it_rules_compendium/adj_off_notification_goi.pdf>.

([89]) Greenleaf, 'Illusions Squared: India's Failed Data Privacy Rules'.

([90]) Greenleaf, 'Illusions Squared: India's Failed Data Privacy Rules'.

([91]) PI Report 2012, p. 14: 'Although the powers of the AO under the Act are very extensive, they have been used very sparingly in the 11 years since the passage of the IT Act. No compilation of the orders of AOs of various states exists either online or offline and they are only sparingly reported in newspapers.'

([92]) IT Act (India), s. 57(1).

([93]) IT Act (India), ss. 49–50.

([94]) IT Act (India), s. 58.

([95]) IT Act (India), s. 58(2).

([96]) IT Act (India), s. 57.

([97]) Prior to the 2008 Amendments, called the Cyber Appellate Regulations Tribunal.

([98]) Notification of rules for Cyber Regulations Appellate Tribunal (Procedure), 17 October 2000.

([99]) IT Act (India), s. 62.

([100]) There are no published decisions of the Tribunal on its website since 30 June 2011. Cyber Appellate Tribunal <http://www.catindia.gov.in/>.

([101]) IT Act (India), s. 49.

([102]) Vijayashankar Na, 'Cyber Appellate Tribunal Chairman-Status' (Naavi blog, 5 June 2013) <http://www.naavi.org/wp/?p=1474>.

([103]) Vijayashankar Na, '13th Anniversary of the Indian "Digital Society Day"' (Naavi blog, 17 October 2013) <http://www.naavi.org/wp/?cat=34>.

([104]) Enquiry Rules (India) 2003, r. 4(l).

([105]) Standing Committee on Information Technology, *Seventeenth Report*, 2011 <http://164.100.40.18/parliament/standing_reports/loksabha15/17th%20Report%20-%20English.pdf>.

([106]) For examples of investigations and prosecutions (none directly relevant to privacy issues), see Justice Rajesh Tandon, Chairperson, Cyber Appellate Tribunal, 'Cyber Law and Adjudication Issues in India', Lecture in the Workshop on Cyber Law, Asian School of Cyber Laws, Pune, held in New Delhi on 28 August 2010 <http://catindia.gov.in/writereaddata/ln_bgKMZv1_17_2012.pdf>.

([107]) Greenleaf, 'Promises and Illusions of Data Protection in Indian Law', pp. 51–5 provides more detail on some of the bodies discussed in this section.

([108]) Privacy International, *India* (Report under the 'Privacy in the Developing World' project, PI, 14 November,

2012), p. 17 <https://www.privacyinternational.org/reports/india-0> (hereinafter 'PI Report, 2012').

([109]) Tamil Nadu Right to Information Act 1997; Goa Right to Information Act 1997; Rajasthan Right to Information Act 2000; Delhi Right to Information Act 2001; Maharashtra Right to Information Act 2002; Assam Right to Information Act 2002; Madhya Pradesh Right to Information Act 2003; Jammu & Kashmir Right to Information Act 2004.

([110]) (2004) AIR 2004 SC 1442.

([111]) The European Court of Human Rights in 2009 reached a similar conclusion in relation to the European Convention on Human Rights. See *Társaság a Szabadságjogokért v Hungary*, judgment of 14 April 2009 regarding application no. 37374/05.

([112]) RTIA (India), s. 2(j) refers to 'any authority or body or institution of self government established or constituted' under such laws.

([113]) RTIA (India), s. 2(h).

([114]) The independence of the RTI panels has been questioned by a Supreme Court which suggested that appeal panels should have at least one judicial member.

([115]) Central Information Commission <http://cic.gov.in/>.

([116]) CIC decisions on LII of India at <http://www.liiofindia.org/in/cases/cen/INCIComm/>.

([117]) PI Report, 2012, p. 18.

([118]) The Act was notified in the Gazette on 23 June 2005, and came into force by Notification on 14 December 2006. The rules and regulations were notified on the same day, making the Act operational.

([119]) See RBI, 'For Common Person' web pages <http://www.rbi.org.in/commonman/English/scripts/home.aspx> under 'Useful Information / RBI Regulations'.

([120]) RBI, 'Code of Bank's Commitment to Customers', 1 July 2006 at <http://www.rbi.org.in/commonman/English/Scripts/CustomerServiceGuidelines.aspx#pri5>.

([121]) Greenleaf, 'Promises and Illusions of Data Protection in Indian Law'.

([122]) Protection of Human Rights Act (India)1993, s. 1(d).

([123]) PHRA (India), s. 3.

([124]) PHRA (India), s. 12(a).

([125]) In *Selvi vs. State of Karnataka* (2010) 7 SCC 263 at <http://indiankanoon.org/doc/338008/>. See PI Report 2012, p. 82.

([126]) NHRC website <http://nhrc.nic.in/>. See 'Human Rights Cases' and 'Suo-Motu Cases'.

([127]) NCDRC website <http://ncdrc.nic.in/>.

([128]) Judgments Search <http://cms.nic.in/ncdrcrep/>.

([129]) *Nivedita Sharma v Bharti Tele Ventures, ICICI Bank Ltd, American Express Bank* (Complaint Case No. CC-09/2006) CDRC State Commission: Delhi, 26 December 2006 <http://cms.nic.in/ncdrcrep/judgement/80NIVEDITA%20SHARMA%20VS%20BHARTI%20TELE%20VENTURES.htm>.

([130]) Viswanathan, *Outsourcing to India*, p. 303.

([131]) Some aspects of the compensation ordered were successfully challenged as beyond the powers of the CDRC: *Cellular Operators Ass.O.I. & Ors v Nivedita Sharma & Ors* (2010) High Court of Delhi, 15 January 2010, available at <http://indiankanoon.org/doc/1179078/>.

([132]) Common Charter of Telecom Services <http://www.trai.gov.in/Content/CCharter.aspx>.

([133]) Data Security Council of India, *DSCI Privacy Framework* (DSCI, 2010) <http://www.dsci.in/dsci-privacy-framework>.

([134]) Data Security Council of India, 'DSCI Security Framework' (November 2009) <http://www.dsci.in/taxonomypage/63>.

([135]) DSCI, 'DSCI Privacy Framework—Best Practice' (November 2009), p. 3 <http://www.dsci.in/dsci-privacy-framework>.

([136]) DSCI, 'DSCI Privacy Framework—Best Practice', p. 4.

([137]) DSCI, 'DSCI Privacy Framework—Best Practice', p. 25.

([138]) In 2003 the head of the Department of Information Technology said 'We are ready with the draft of the Data Protection Act. It might be possible to enact it in the winter session of Parliament'.

([139]) Report of the Group of Experts on Privacy, Planning Commission, Delhi, 16 October 2012 <http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf>.

([140]) For the background to this Bill, see CIS, 'The National Privacy Roundtable Meetings (CIS, 19 September 2013) <http://cis-india.org/internet-governance/blog/national-privacy-roundtable-meetings#fn13>.

([141]) Summarized in Graham Greenleaf, 'India's Draft The Right to Privacy Bill 2014—Will the BJP Enact It?' (2014) 129 *Privacy Laws & Business International Report*, pp. 21–4.

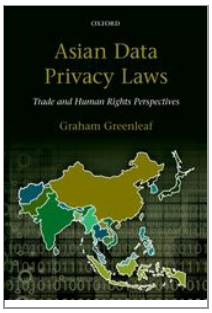
([142]) Nayanima Basu, 'Data adequacy grant to India non-negotiable, says EU envoy' (Business Standard (India), 17 May 2013) <http://www.business-standard.com/article/economy-policy/data-adequacy-grant-to-india-non-negotiable-says-eu-envoy-113051700013_1.html>.

([143]) (2013) 4(7) *DSCI News*, p. 2 (Nov/Dec 2013).

([144]) Basu, 'Data adequacy grant to India non-negotiable'.

([145]) Rajat Pandit, 'Free Trade Agreement with EU in suspended animation till new govt takes over' (Times of India, 8 December 2013) <http://timesofindia.indiatimes.com/business/india-business/Free-Trade-Agreement-with-EU-in-suspended-animation-till-new-govt-takes-over/articleshow/27043726.cms>.

University Press Scholarship Online
Oxford Scholarship Online



Asian Data Privacy Laws: Trade & Human Rights Perspectives
Graham Greenleaf

Print publication date: 2014
Print ISBN-13: 9780199679669
Published to Oxford Scholarship Online: December 2014
DOI: 10.1093/acprof:oso/9780199679669.001.0001

Privacy in the Other Seven South Asian (SAARC) States

Graham Greenleaf

DOI:10.1093/acprof:oso/9780199679669.003.0016

[–] Abstract and Keywords

In this chapter the limited privacy developments in each of the seven South Asian countries (other than India) are detailed, including constitutional, general law and statutory protection. None of the South Asian countries of Pakistan, Bangladesh, Sri Lanka, Nepal, the Maldives, Bhutan, and Afghanistan have data privacy laws for their private sectors, nor does it seem likely that any will be put in place in the near future. However, there are lesser but still significant data privacy developments in most of these countries. They include a near-comprehensive data privacy regime in Nepal's public sector; a Right to Information (RTI) Act with some data privacy extensions in Bangladesh; computer crime and compensation provisions in Sri Lanka, Bangladesh, and Pakistan; and constitutional protections (at least in theory) in most. RTI initiatives, which can be stepping stones to full data privacy legislation, have been commenced, but remain incomplete, in most of these countries.

Keywords: data protection, privacy, SAARC, Pakistan, Bangladesh, Sri Lanka, Nepal, Maldives, Bhutan, Afghanistan

1. The South Asian (SAARC) countries

With the exception of India, none of the other South Asian countries, namely Pakistan, Bangladesh, Sri Lanka, Nepal, the Maldives, Bhutan, and Afghanistan, have comprehensive data privacy laws even for their private sectors, nor does it seem likely that any will be enacted in the near future. However, there are lesser but still significant data privacy developments in most of these seven countries. They include a near-comprehensive data privacy regime in Nepal's public sector; a right to information (RTI) Act with some data privacy extensions in Bangladesh; computer crime and compensation provisions in Sri Lanka, Bangladesh, and Pakistan; and constitutional protections (at least in theory) in most **(p.436)** of the countries. RTI initiatives have been commenced in all South Asian countries, but remain incomplete in most. They are important because, although they only apply to the public sector, they are sometimes stepping stones to full data privacy legislation.

In this chapter these privacy developments in each of the seven South Asian countries (other than India) are detailed, including constitutional, general law, and statutory protection. The context for future data protection developments is also set out, covering the political and economic context, government and legal systems, and the surveillance context (including national ID systems). Regional data privacy harmonization is not yet on the agenda of the South Asian Association for Regional Cooperation (SAARC), but this may change, as it has in the Association of Southeast Asian Nations (ASEAN) (as discussed in Chapter 2). In future, it is also possible that developments in India may spark changes in its neighbours as well, for various reasons—because they compete with India for outsourcing work, because of the influence of Indian examples, or because India's new law may prevent exports of personal data to these countries.

1.1. Impediments to data privacy in South Asia

In the past two decades and continuing, South Asia has had a higher incidence of political instability, civil war, and terrorism than has Northeast Asia or ASEAN. Under these circumstances, the development of privacy protections and data privacy laws are far less likely to occur, and that has been the case until the recent developments in India. Such circumstances also make it far more likely that national security considerations will result in considerable legally sanctioned inroads into privacy, and the increased adoption of surveillance

technologies by governments. Partly as a result of these factors, South Asia is, in general, at a lower stage of economic development than Northeast Asia or ASEAN, where data protection laws, usually of international standard, have now been adopted in most countries as part of economic and social modernization.

The development of national ID systems is occurring in almost all South Asian countries without any limits on the uses that either the private sector or the public sector can make of ID cards and ID numbers. In the public sector this raises the risk of unrestrained data matching between agencies, and in the private sector it is an invitation to private sector organizations to require national ID cards as the sole form of acceptable identification, to build their own information systems around the ID numbers, and in the longer run to develop much larger-scale interconnections with public sector databases than is the case at present. India's and Pakistan's ID systems are influential.

2. Nepal

More than any other country in South Asia, Nepal has legislation which (at least on paper) is closest to a data privacy law, although it is primarily a Right to Information Act.

2.1. Nepal—political, economic, and social context

Nepal is a landlocked state of nearly 30 million people to the north of India, also sharing a border with China. Its population is around 80 per cent Hindu, with Buddhist and Muslim minorities. It is regarded as 'among the poorest and least developed countries in the world, with about one-third of its population living below the poverty line', and with agriculture and the processing of agricultural products accounting for most of its economy. Transparency **(p.437)** International's Corruption Perception Index for 2013 ranks Nepal 116th (of 177 countries) for overall public sector corruption, with a score of 31/100.[1]

Nepal was never a colony.[2] Rule by hereditary Rana premiers since 1846 was overthrown in 1951 by popular pressure (with support from newly independent India), and was replaced by the monarchy which assumed power with a cabinet system of government. Subsequent constitutions declared Nepal a 'Hindu kingdom'. Reforms in 1990 established a multiparty democracy and constitutional monarchy, but after the massacre of the entire royal family in 2001,[3] the new King (the surviving brother of his predecessor) dismissed the elected government in 2002 and assumed absolute power in 2005. An insurgency led by Maoists commenced in 1996, initiating a decade-long civil war between insurgents and government forces. Mass protests in 2006 resulted in peace negotiations and an accord between the Maoists and government officials, and an interim constitution in 2007. A Constituent Assembly elected in 2008 declared Nepal a federal democratic republic, abolished the monarchy, and elected the country's first president. There have since been four different coalition governments, led twice by the Maoist party (which received a plurality of election votes), and twice by the Marxist-Leninist party.

In May 2012 the assembly elected in 2008 lapsed without completing the task of replacing the 2007 Interim Constitution, creating a political impasse.[4] The Maoist-led coalition government continued to govern until early 2013. A caretaker government under the Chief Justice supervised November 2013 elections where the Nepali Congress and the Marxist-Leninist party won the largest proportions of seats, but neither won a majority. In February 2014 the assembly elected Sushil Koirala, leader of the Nepali Congress and a long-time democracy activist, as Prime Minister. The Marxist-Leninist Party agreed to a constitution being completed within a year, and to support the government until then.[5]

Government and legal system of Nepal

Under the Interim Constitution, Nepal has a parliamentary system of government headed by a Prime Minister, with a largely ceremonial President as head of state. The legal system is based on a comprehensive civil and criminal code, the Muluki Ain (Country Code) which has been progressively amended since its introduction in 1883.[6] It was influenced by the English and French legal systems of the time, Hindu legal concepts, and legal developments in India, and has absorbed subsequent legal influences. The Supreme Court is the final court of appeal and also the constitutional court. The Chief Justice of the Supreme Court is **(p.438)** appointed by the President, on the recommendation of the Constitutional Council, and the Chief Justice appoints other judges on the recommendation of the Judicial Council.

Public attitudes and civil society in Nepal

The Citizens' Campaign for Right to Information (CCRI)[7] obtains funding from the Open Society Foundation, and has been operating RTI educational campaigns since 2008. The students in the RTI case against Tribhuvan University, discussed in section 2.4, were represented by lawyers provided by CCRI.

2.2. State surveillance in Nepal

After decades of political instability and violence by both insurgents and government forces, Nepal is slowly finding its way toward a balance between democracy and surveillance practices.

Interception and other surveillance

Telecommunications interception is unregulated and extensive, although there is a Bill before the Parliament which would impose some controls if enacted. A non-governmental organization (NGO) report summarizes:

> Wiretapping is one of the most sensitive areas relating to privacy rights in Nepal. Our research shows that the security forces, with the help of telecommunication companies, frequently intercept phone communications, both mobile and fixed line…At present, there is no law regulating nor specific judicial process for authorizing communications interception. Our research found that if the security forces wish to intercept communications, they approach the telecommunications companies, who agree to help. Some wiretaps are set in place directly by the security forces.[8]

According to the same report: 'Security forces can stop individuals anywhere at any time and search their body, belongings, and home. Although warrants or court orders are necessary for searching people's houses, the security forces do not bother to obtain the required authorization before conducting such searches.'[9] The Nepal government is planning to establish a DNA database to collect and store biological samples taken from prisoners.[10] Cyber-cafes are licensed and must 'maintain a record of users' login and logout time'.[11]

National ID system under development

The Nepal government has started development of a national ID card. In 2011 it established the National ID Management Center[12] under the Home Ministry of Nepal, and is **(p.439)** seeking international aid agency funding.[13] Draft legislation awaits approval from the Cabinet and then the Parliament.[14] The new system will be based on the Election Commission database, which contains fingerprint information as well as photographs and unique identification numbers, and is the basis for the ID cards it issues. The scope of the proposed ID system is unclear: it is reported to be intended to replace other identity documents including citizenship certificate, voter's card, driving licence, passport, and ATM cards, and even to include information about property ownership and criminal records.[15] The Election Commission database will be transferred to the National ID Card Centre to enable it to issue the cards. In April 2010 the pilot phase of a voter registration project was completed by compilation of a new voter list with photographs and fingerprints, and included all citizens between the ages of 16 and 18 whether or not entitled to vote. By April 2012 the Election Commission (EC) claims that 10.2 million people had been issued with a biometric voter's identity card.[16]

2.3. Existing privacy protections

Nepal has very limited privacy protections in relation to the private sector. Concerning public bodies, however, its Right to Information Act (RTI Act), while primarily concerned with 'freedom of information' issues, also has a number of unusual and potentially important data privacy protections.

International obligations

Nepal ratified the International Covenant on Civil and Political Rights 1966 (ICCPR), which under Nepalese law should mean that its provisions (including Article 17 protecting privacy) should prevail over Nepalese statutes.[17] It also ratified the Optional Protocol to the ICCPR in 1991, allowing 'communications' (complaints) to be made to the UN Human Rights Council concerning failures to uphold Article 17. Two such complaints have been brought, but neither concerned privacy. Nepal is a member of SAARC, but SAARC has not been active in relation to regional privacy standards.

Constitutional and statutory protections

In the Constitution of the Kingdom of Nepal 1990, the right to privacy and the right to information were both included for the first time. The right to privacy was retained in the 2007 Interim Constitution, still in force, which provides in article 28: 'Except in **(p.440)** circumstances as provided by law, the privacy of the person, residence, property, document, statistics, correspondence, and character of anyone is inviolable.' A more explicit privacy protection has been proposed during parliamentary committee discussions of the draft constitution.[18] It may be possible to use such constitutional protections as the basis for litigation.[19]

There are minor other scattered statutory provisions relating to privacy.[20] Complaints concerning violations of privacy may be made to the National Human Rights Commission (NHRC),[21] but no such complaints have yet been made.[22]

2.4. Right to Information (RTI) Act and National Information Commission

The Right to Information Act 2007[23] finally gave effect to a 1990 constitutional right to information, a development resulting largely from 15 years of grassroots advocacy.[24] The judiciary played a key role,[25] as it did a decade later in India, by requiring the government to enact legislation following a 1994 case.[26] The Act is supplemented by the Right to Information Regulation, 9 February 2009.[27]

The National Information Commission

The Act establishes an independent National Information Commission (NIC) comprising a Chief Information Commissioner and two other Information Commissioners,[28] to which complaints can be made of non-compliance with the Act. A complaint against refusal of access (or access in breach of section 3(3)) by a public body's information officer must first **(p.441)** be made to the 'chief' of the public body.[29] Appeals from an adverse decision may be made to the NIC, which then has 60 days to investigate and make its decision.[30] There is a right of appeal against NIC decisions to the Appellate Court.[31] The NIC's very general powers include 'to order concerned parties to fulfil liabilities in accordance with this Act' and 'to issue other appropriate orders regarding the protection, promotion and exercise of right to information'.[32] The NIC publishes on its website[33] its decisions on complaints and annual reports, in Nepali.

Scope of access rights

The RTI Act provides that every citizen shall have 'the right to information subject to this Act' and 'access to the information held in the public Bodies'.[34] 'Information' and 'right to information' are given generally broad definitions,[35] but the definition of 'information' limits it to 'information related to the functions, proceedings thereof or decisions of public importance made by the Public Bodies'. As the 'Article 19' freedom of information (FOI) NGO points out, most RTI Acts apply to all information held by public bodies, and this would be preferable, and would also cover information created by one public body but held by another.

The scope of the Act is broad, because 'public body' is defined to include every type of body established under the Constitution or an Act, of or by the government (or under its partial control), plus political parties, NGOs funded directly or indirectly by the government or by foreign governments or international organizations, and other bodies as may be prescribed.[36] For an example of a body within jurisdiction because of its funding, a finance company was required to disclose a Due Diligence Audit Report to an applicant.[37] Nepalese citizens therefore have a right of access to personal information held about them by a wide range of government and non-government bodies, but not by most parts of the private sector. There is a separate provision seemingly guaranteeing employees of public bodies access to data about themselves.[38]

The RTI Act is generating litigation to expand its boundaries. In 2011 the Supreme Court of Nepal upheld a decision by the NIC, ruling that every student has the right to see his or her exam answer sheet. Tribhuvan University (the oldest in Nepal) rejected the application, arguing that the exam results were secret and that showing them was against examination norms and principles. Both the NIC and the court rejected the argument, and ordered the university to comply.[39] This case has subsequently been used by the NIC to convince the Examination Controllers Office to change its procedures so that high school students can obtain their answer books (with examiners' names removed).[40]

The Act also requires what is described as 'proactive disclosure' by public bodies of a wide range of information about their structure, decision-making procedure, types of **(p.442)** data held by them, etc.[41] This encompasses what the OECD privacy Guidelines call the 'openness' principle.

Rates of complaints and decisions

Analysis of the published decisions shows that 407 complaints have been investigated since 2008, and 85 remain unsettled (as at 13 April 2013). The two most recent Annual Reports include a breakdown between requests on matters of public concern, and those of private concern (essentially, requests for personal information), indicating that while in 2010/11 there were nearly twice as many matters concerning personal information investigated as there were matters of public concern (31/16), in 2011/12 the position was reversed (44/92). Case numbers continue to rise, and it appears that cases concerning personal information are likely to amount to more than 40 per year. (See Table 16.1.)

No breakdown by government sector is available for cases concerning personal information, but analysis by sector of all complaints given in the 2010/11 and 2011/12 NIC Annual Reports shows that complaints are distributed across most parts of Nepal's public sector.

Fourteen appeals against NIC decisions have been taken to the Supreme Court, and five to the Appellate Court. No court decisions have yet resulted from these writs, with the exception of the case concerning exam scripts discussed earlier.

Correction rights

Persons may appeal to the chief of a public body if they believe 'that the information in Public Body on a particular subject is wrong', 'along with necessary evidences for the correction of the information'. After investigation, corrections must be made within seven

Table 16.1 Applications, complaints and appeals with NIC and settlement status (Fiscal Year 2008/09–2012/13)

Fiscal Year	Applications, complaints and appeals received by NIC			Settled			Not settled
	Overall	Public concern	Personal concern	Total	Ordered to provide information	Dismissed	
(1)	(2)=(5)+(8)	(3)	(4)	(5)=(6)+(7)	(6)	(7)	(8)
2008/09	12	NA	NA	11	NA	NA	1
2009/10	39	NA	NA	29	NA	NA	10
2010/11	47	16	31	22	NA	NA	25
2011/12	136	92	44	90	81	9	46
2012/13*	173	NA	NA	170†	NA	NA	3
Total	407			152			85

NA = Not available

(†) Initial actions have been completed.

(*) As of 13 April 2013.

Annual Reports, 2009/10, 2010/11, and 2011/12, National Information Commission, Kathmandu, Nepal, available from the NIC website (in Nepali). Extraction of information and table preparation by Mr Shalik Ram Sharma and Mr Rajan Sharma.

(p.443) days.[42] This is not restricted to personal information. There is no specific right of appeal to the NIC, but its general powers under section 19 may be sufficient for it to make orders concerning corrections. In any event, the right of compensation (discussed below) covers 'wrong information' so it is

clear that complainants can take issues of incorrect personal information to the NIC, even if there is no general right to appeal to have corrections made to any government-held information. The NIC Annual Reports do not indicate whether any correction orders have been made.

Protection of personal information against access

The exceptions to the right of access include an exception, among others, for information 'that interferes on individual privacy and security of body, life, property or health of a person',[43] in addition to other exceptions such as that concerning national security.[44] There is a pro-disclosure proviso that a 'Public Body shall not refrain from the responsibility of flowing information without appropriate and adequate reason not to flow information'. Information officers have the responsibility to redact such information as should not be provided, and provide the rest.[45]

Classification of information as privacy-sensitive

A Committee is established[46] to classify information in accordance with the categories in section 3(3), including the privacy-sensitive information in section 3(3)(e). The three-person Classification of Information Committee (CIC) consists of the Chief Secretary of the Government of Nepal as chairperson, the Secretary of the relevant Ministry, and an expert in the relevant subject assigned by the chairperson. The section 27 Committee has to make a decision 'determining the number of years the information should be kept confidential and method for the protection of information', and to inform the NIC of this.[47] However, members of the public can appeal to the NIC against such classifications.[48] The section 27 Committee can classify information as confidential for up to 30 years, but must review this every 10 years.[49] The NIC, when reviewing any appeal under the Act, can override the committee's classification and order the information to be made public.[50]

The operation of section 27 has proven to be controversial in practice.[51] The CIC made an initial classification of information on 22 December 2008, but the NIC found that the classification did not match the intent of the RTI Act, and requested the CIC to review and correct the classification. The re-classification by the CIC, in January 2012 was found by the NIC still to be deficient in not meeting the intent of the Act to provide a right to information. Civil society organizations, journalists, lawyers, and others protested against the classification, and the Journalist Federation called for a nationwide protests. A lawyers' organization filed a case in the Supreme Court against the implementation of the classification, and the Court issued an interim order against it on 31 January 2012. The Journalist Federation then suspended its national protest. Finally, the government withdrew its decision to implement the classification. The NIC commented that this example showed the Nepalese public how an active civil society can play a role in protecting people's rights in a democratic system.

(p.444) Protection of accessed personal information against misuse by third parties

An application for access must state the 'reason to receive such information',[52] but it does not appear that access can be refused on the basis of the reasons stated. However, section 31(1) ('Information not to be Misused') is a potentially important protection of personal data, providing that '[a]ny person who obtains any information from any public Body should not misuse the information by not using it for the purpose that was considered' as stated under section 7(1). Complaints concerning misuse may be made to the NIC.[53] This is a very unusual data privacy protection, because use of a person's personal information disclosed to a third party despite section 3(3) is still subject to the restricted use provided for in section 31(1). The NIC Annual Reports do not indicate that it has yet been used.

Restrictions on use and disclosure of personal information by public bodies

Further very broad data privacy provisions are in section 28 ('Protection of Information') which requires that a 'Public Body shall protect the information of personal nature held in for [sic] preventing unauthorized publication and broadcasting',[54] and that 'Personal information held in public Body…shall not be used without written consent of concerned person' except in very narrow defined circumstance, namely '(a) in case of preventing a serious threat to life and body of any person or public health or security; (b) if required to be disclosed in accordance with prevailing laws; [or] (c) if related to investigation of offence of corruption'.[55] This implies that public bodies in Nepal cannot use or disclose any personal information they hold except with express authorization under existing laws (including under RTI Act requests). The NIC

Annual Reports do not indicate that any decisions have yet been made under this provision.

Compensation and offences

A right to compensation is provided in section 33, and it is much wider than the equivalent provision in India's RTI Act because the privacy rights in Nepal's Act are so much broader:

> (1) If any person incur losses and damages due to not providing information, denying to provide information, providing partial or wrong information or destroy the information by the Chief or Information Officer of Public Body, such person may appeal before the Commission for compensation within three months from the date of not acquiring information, acquiring partial or wrong information or destroyed information.
>
> (2) If the application in accordance with Sub-Section (1) is found reasonable after the investigation, the Commission by considering the actual loses, may compensate the applicant from the concerned Body with reasonable amount.

This is in effect a 'data privacy tort', a right of action for compensation against a public body, for losses caused by refused or delayed access, providing incorrect information, or wrongly deleting information.

There are also offences which can be found by the NIC (not a court), with various 'punishments' of up to Rs 25,000 (about US$300) able to be imposed on Information Officers or Chiefs, for refused or delayed access, providing incorrect information, or wrongly deleting information, irrespective of whether a person suffers loss.[56] Similar fines may be imposed on **(p.445)** third parties who misuse personal information in breach of section 31, but it does not seem that an action for compensation is available. No compensation actions have yet been reported by the NIC in its Annual Reports. However, one of the writs before the Supreme Court claims compensation as part of the claim.

2.5. A public sector data privacy law?

Nepal's RTI Act has almost all of the minimum principles that could be expected in a data privacy Act for the public sector in relation to personal data (see Chapter 3, section 3): right of access; right of correction; protections against access by others; restrictions on use and disclosure by government agencies; restrictions on additional uses by third parties when they do obtain access; 'openness' of government practices concerning personal data; both offences and compensation provisions for breaches; an independent authority to investigate complaints and resolve disputes; and a right of appeal to the courts. Although there is no explicit provision in the Act concerning data security or data quality, actions can be taken before the NIC if data is wrongly destroyed. One element not addressed is an explicit restriction on when public bodies can collect personal information, and how much. However, the inclusion of all other standard elements is sufficient to justify regarding Nepal as a country with a public sector data privacy law.

This is not to suggest that Nepal is some Shangri La[57] for public sector privacy. While the article 19 NGO's 'overall assessment of the Act, on its enactment in 2008 was 'very positive',[58] the leading Nepalese NGO's view, after the Act had been in force for more than three years, was:

> Compared to India and Bangladesh, the implementation status is too poor. However, situation is not hopeless; it could be done in better stage if associated problems are addressed promptly and positively. Reports shows that very few information officers are appointed in public agencies and the status of proactive discloser is extremely at a low level.[59]

The RTI law is nevertheless a major step forward for data privacy in the public bodies which govern Nepal and provide many of its services. Although public use of the data privacy aspects of the law is limited, the NIC seems to be taking an active and reasonably transparent role in enforcement of the law.

Nepal's law is an example of the handful of RTI/FOI laws which are also public sector data privacy laws. It is worth remembering that, in many countries now considered to have comprehensive laws on data privacy, their laws initially only covered the public sector (for example, Australia, South Korea, and Japan). Public sector privacy laws can be a stepping stone to a comprehensive law. In South Asia the Nepalese law is

already innovative in applying privacy principles to the public sector. **(p.446)**

3. Bangladesh

The strongest aspect of data privacy protection in Bangladesh is its public sector right to information law, supplemented by some criminal provisions in its e-commerce law.

3.1. Bangladesh—political, economic, and social context

Bangladesh was part of British India as eastern Bengal, becoming the eastern part of Pakistan, following the partition of India and Pakistan in 1947.[60] East Pakistan split from West Pakistan in 1971, following a war between the two provinces, suppression of East Bengal by the Pakistan army, and intervention by the Indian army on the side of independence for the East. Pakistani armed forces are estimated to have killed between one and three million Bengalis during this period.[61] Bangladesh emerged as a separate country, initially with a democratic government. On three occasions since 1971 Bangladesh came under military rule, alternating with periods of return to civilian government. Since 1990 Bangladesh has had a continuous period as a parliamentary democracy, although punctuated by a state of emergency in 2007/8.[62] Two main political parties are dominant, the Bangladesh Nationalist Party (in office from 2001–08) and the Awami League, in office since 2009.

The population of Bangladesh is estimated to be over 160 million,[63] the eighth most populous country and with one of the world's highest population densities. About 90 per cent of the population are Muslims, the fourth largest Muslim population of any country (after Indonesia, India, and Pakistan). The Bangladesh economy has been increasingly successful over the last 20 years (5–6 per cent growth per annum since 1996), indicated by factors such as dependence on foreign aid falling, increase in foreign direct investment, the success of the micro-credit movement (invented in Bangladesh by Grameen Bank), and a slow rise in GDP (but still under US$2,000 per capita). The service industry accounts for over 50 per cent of the economy. The garment industry and repatriation of funds by overseas workers are two major sources of income. Over 30 per cent of the population lives below the poverty line. Transparency International's Corruption Perception Index for 2012 ranks Bangladesh 144th (of 176 countries) for overall government corruption, a very poor ranking. Bangladesh has had growing Internet connectivity since 1996, with an estimated 5.5 million (3.5 per cent population penetration) Internet connectivity as at December 2011. Users are almost entirely concentrated in the cities. Only about 80,000 people currently have mobile Internet connectivity.[64] It is also threatened by rising sea levels resulting from global warming.

(p.447) Government and legal system of Bangladesh

Bangladesh is a unitary state with an intermittent parliamentary democracy, with its most recent return to democracy being in 2008.[65] Its legal system is mainly English-derived common law with elements of Islamic law. Laws are enacted by the unicameral Parliament, but the President has a temporary veto power.[66] In November 2007, Bangladesh successfully separated the judiciary from the Executive. The judiciary consists of the Supreme Court as the apex court, with other courts subordinate to it, and no separate constitutional court.

Civil society organizations and public attitudes in Bangladesh

'Civil society in Bangladesh plays an important role particularly with respect to reaching the poor at the grassroots level…[but] does not play a strong role in advocacy or research.'[67] The main Bangladesh NGO involved in privacy issues (in cooperation with Privacy International) is VOICE,[68] an activist organization whose interests include rights in relation to information and communication.[69] It held a 'National Convention on Right to Privacy and Data Protection' in 2012[70] which called on the government 'to enact a privacy and data protection law to secure privacy rights and personal data'.

3.2. State surveillance in Bangladesh—interception and ID cards

As is the case in many Asian countries, telecommunications interception is not effectively regulated by law. Although the government's use of its telecommunications interception powers was challenged in the High Court in 2006, the case has not come to a hearing, and the government did not respond to questions issued by the court to the government.[71] In jurisdictions such as Indonesia, India, and Hong Kong, constitutional protections of privacy (such as are found in Bangladesh, as discussed in section 3.3 of this chapter) have

been used to force governments to pass legislation defining the limits of telecommunications surveillance.

Bangladesh has developed what is popularly known as a 'voter identity card' but is in fact the 'national identity card' established by the National Identity Registration Act 2010.[72] The Act empowers the Election Commission to register those eligible to be on the voting roll[73] for the issue of national identity cards and a 'National Identification Number' (NIN),[74] and fixes the validity of an ID card for 15 years from issuance.[75] There are offences in relation to fraud concerning card issue or use,[76] but there do not seem to be any restrictions on the use of, or demands for, the card or number, whether by government organizations or the private sector.

Seventy-five million people (a substantial portion of the electorate) are reported to have registered in the first phase to mid-2012, obtaining a card which carries the person's name, parents' names, date of birth, address, and the NIN. The Act does not specify what is to be **(p.448)** included on the card.[77] The introduction of the cards may have improved social inclusion in Bangladesh by providing an identity document to those who did not previously have one, and also fostering a sense of national inclusion: 'For most Bangladeshis, the card is required for accessing government and non-government services. It has become mandatory for opening a bank account or getting a new mobile phone connection.'[78] Use of the national ID card is expected to be mandatory for citizens to obtain any services from the government, its departments and institutions, or from any statutory offices, but legislation to make it mandatory had not been enacted as at mid-2013.[79] Twenty-two services are covered, including the issue of passports, driving licences, trade licences, tax and business ID numbers, and bank accounts. It will also be required in order to obtain government subsidy facilities, allowance and relief.[80] The intended functioning of Bangladesh's NIN therefore seems to be similar to that of India's unique identification number (UID) (see Chapter 15, section 1.3), except that it has legislative authority, including for the issue of a card, not only a number.

3.3. Constitutional, treaty, and general law protections of privacy

The Bangladesh Constitution recognizes the right of privacy of home and correspondence. Article 43 states: 'Every citizen shall have the right, subject to any reasonable restrictions imposed by law in the interests of the security of the State, public order, public morality or public health, to be secured in his home against entry, search and seizure; and to the privacy of his correspondence and other means of communication.' Article 11 also states that Bangladesh 'shall be a democracy in which fundamental human rights and freedoms and respect for the dignity and worth of the human person shall be guaranteed'. Bangladesh is a secular state and its constitution does not reflect strong Islamic influences, although nearly 90 per cent of the population are Muslims.[81]

Bangladesh is a member of the Commonwealth, of SAARC, and the World Trade Organization (WTO), but not of the Asia-Pacific Economic Cooperation (APEC). It is a party to the International Covenant on Civil and Political Rights 1966 (ICCPR), Article 17 of which is reflected in its constitutional provisions, but has not ratified the Optional Protocol. Bangladesh takes a monist approach to international law, so ICCPR Article 17 is part of its domestic law. No right of privacy has yet been recognized at common law in Bangladesh. This may be less relevant in light of the status of ICCPR Article 17.

3.4. Statutory privacy protections

Bangladesh does not have data protection legislation, but does have a number of pieces of legislation which may be relevant to the development of a data protection regime, and which provide some data protection rights.

(p.449) Right to Information Act and Information Commission

The Right to Information Act 2009 (RTI Act)[82] establishes a right of access to a person's own file held by public bodies, but no explicit right to correction. The scope of the Act goes well beyond the public sector, and is not limited to government administrative bodies. Section 2(b) defines 'authority' to include any private organizations 'run by government financing or with aid in grant from the government fund', or 'run by foreign aid in grant' or that 'undertakes public functions in accordance with any made on behalf of the Government or made with any public organisation or institution'. This broad scope is similar to India's RTI Act. There are the usual exemptions for specified institutions 'involved in state security and intelligence'.[83]

The right to information established by the Act[84] is subject to the usual range of exceptions in freedom of information laws, including any information 'that may, if disclosed, offend the privacy of the personal life of any individual'[85] or 'endanger the life or physical safety of any person',[86] and 'any secret information of a person which is protected by law'.[87] Restriction on disclosure established by the Official Secrets Act 1923, or any other law, are superseded by the RTI Act.[88] All authorities bound by the Act are required to appoint Designated Officers to administer it.[89] They must normally provide the information requested within 20 days.[90]

The Information Commission[91] (IC) is established to administer the Act, comprising a Chief Information Commissioner and two Commissioners (at least one female).[92] The IC has broad powers to investigate complaints of maladministration of the Act, including on its own initiative, and has the powers of a civil court to investigate, summon witnesses, etc.[93] It has numerous other powers and functions including advising government on law reform and international agreements relevant to RTI, and carrying out public education and research.[94] The procedures for appointment and removal of members are likely to create an IC with a significant degree of independence.[95] The IC hears appeals concerning refusal of access requests or failure to provide information within the required time,[96] and is supposed to deal with the matter within 45 days of receiving an appeal, or 75 days in special cases.[97] The IC has significant powers to administer fines for various failures of authorities to perform their RTI duties, as well as to initiate misconduct proceedings against officers.[98] It also has powers 'to give compensation for any loss or damage',[99] which are unusual in freedom of information legislation in Western countries, but often found in Asian RTI Acts.

The structure and powers of the IC are such that, if the words 'data protection' were substituted for 'right to information' (or added to them) throughout the Act, it would be a fully formed data protection authority. This is one path through which data protection laws could develop in Bangladesh. The Commission publishes Annual Reports with some **(p.450)** English translation.[100] It states that 'The foremost aim and objective of this Act is to reduce corruption and ensure good governance, transparency and accountability in all public and private organizations'.[101] As in India, 'RTI' is seen as a major popular instrument of reforming both government and many private organizations, and reducing corruption, giving this legislation a significance which is not often achieved by 'freedom of information' laws in Western countries. The 'root and branch' extent to which the Act's objectives are being pursued is indicated by the Information Commission's statement that 'More than 10,000 Designated Officers from various government/non-governmental organizations have been appointed till December, 2011 to provide information and their names and contact addresses have been uploaded in the Information Commission's website'.[102] In 2011 there were nearly 8,000 RTI applications across Bangladesh. Since the Commission was established it has received 104 complaints, of which it has discarded 44 as faulty, 'taken 44 complaints into account', and issued one fine.[103] Use of the Act could therefore be said to still be rather modest in so populous a country.

Privacy-related offences and Cyber Tribunals under the ICT Act

The Information and Communications Technology Act 2006 (ICT Act)[104] is an omnibus Act dealing with various issues of electronic commerce and cybercrime. It is substantially based on India's Information Technology Act 2000, prior to its 2008 amendments. Given the significance that Act is now assuming in data protection in India, future developments of the ICT Act may become relevant to data protection in Bangladesh.

The offences established by section 54 could be used to enforce privacy protection against third parties who interfere with computer systems, but not against the 'data controller', the owner or operator (which is the main concern of data protection laws). These offences are sufficiently broad that they will criminalize any unauthorized third party interference with a computer system which adversely affects personal data held on the system. Unlike the Indian legislation, which also creates a civil action in relation to such interference,[105] the Bangladesh legislation only creates a criminal offence.

The Act requires the establishment of one or more Cyber Tribunals to hear matters under the Act, to be headed by a Sessions Judge.[106] A Cyber Appellate Tribunal is to be established to hear appeals, headed by a Supreme Court judge,[107] but until established, appeals may be heard by the High Court Division.[108] For

enforcement of data protection laws, and particularly for criminal offences, Cyber Tribunals are an alternative model now **(p.451)** being developed in India, although poorly (see Chapter 15, section 6.3). The use of the Information Commission under the RTI Act is more suited to civil actions and compensation claims.

4. Pakistan

Pakistan has few data privacy protections beyond a very limited 'right to information law', and they operate within a state which is of fluctuating political stability, and increasingly engages in intensive surveillance activities.

4.1. Pakistan—historical and legal context

Since the 1947 partition of British India into India and the state of Pakistan (divided between West and East sections), Pakistan has alternated between democratic but corrupt governments and military regimes.[109] In 1971 East Pakistan become the separate nation of Bangladesh. Since elections in 2008, Pakistan has had an elected government with a legislature and President, but the possibility of regression to military government is ever-present. Pakistan is an almost entirely (95 per cent) Muslim country of over 190 million people,[110] and therefore the second most populous state in South Asia and one of the most populous in Asia.

Pakistan's international position has always been precarious: it has fought wars with India in 1947–48 and 1965 over the disputed Kashmir territory (still unresolved); a third war was triggered by its repression of East Bengal in 1971; nuclear weapons have been developed by both Pakistan and India; wars, insurgency, and terrorism have continued on its border with Afghanistan since at least 1978, and at various times within Pakistan itself in areas such as the Swat Valley. There is a continuing and severe terrorist threat from the Pakistani Taliban. Pakistan consequently has more security concerns than most states, coupled with an unstable democracy alternating with military regimes. One consequence is an increased likelihood of government surveillance; another is that it is less likely that human rights measures such as data privacy laws will be developed.

Government and legal system of Pakistan

The Islamic Republic of Pakistan is a federation, with four provinces, a federal territory, and a Pakistan-administered Kashmir. Its current constitution dates from 1973, following the separation of East Pakistan, and has been suspended three times since, and most recently restored in December 2007. Transparency International's Corruption Perception Index for 2013 ranks Pakistan 127th (of 177 countries) for overall governmental corruption, with a score of 28.

The lower house of the bicameral Parliament (Majlis-e-Shoora), the National Assembly, is elected by universal suffrage, with some seats reserved for religious minorities. The Senate has equal representation from each of the four Provinces, elected by their Provincial Assemblies, and some representatives of territories. The Prime Minister is nominated by **(p.452)** the lower house, and is usually the leader of the majority party or coalition. The President is elected for a five-year term by an electoral college comprising members of both federal houses and each provincial assembly. Pakistan has a semi-presidential system, with both President and Prime Minister actively participating in government.[111]

Pakistan's legal system is common law based, with Islamic law influence. Islam is the state religion.[112] It has a Supreme Court which also acts as a constitutional court, and a High Court in each Province. There is also a federal Shariat court which has power to declare legislation invalid as repugnant to the injunctions of Islam, and appellate jurisdiction in some issues involving sexual behaviour or intoxication. There are also numerous special courts and tribunals.[113] Pakistan is a member of SAARC, and the Commonwealth once again, following restoration of democratic institutions. It is not a member of APEC.

There are many civil society organizations in Pakistan, some of which have been active in relation to RTI laws, but few are involved in privacy issues.[114]

4.2. State surveillance in Pakistan—ID cards and telecommunications surveillance

Data protection developments in Pakistan take place in a state which has always engaged in intensive surveillance activities, more so in the last decade as domestic terrorist activities have increased. Government interception powers in the Telegraph Act 1885 have been described as unrestricted, and with no judicial oversight or intervention.[115] It is claimed by Pakistan NGO Bytes4All that in 2012 'the Pakistan Telecommunication Authority (PTA) commissioned a new wave of surveillance and censorship, whereby all emails, telephone calls and communications will be monitored'.[116] The government also announced plans in 2011 to ban the use of encryption.[117]

Pakistan's National Database and Registration Authority (NADRA)[118] is active in ID system development internationally, and is involved in projects in Sri Lanka and Nigeria as well as in Pakistan. It is a federal department of the Government of Pakistan which employs more than 11,000 staff in 400 domestic offices and five international offices. By 2010, NADRA announced that it had already issued nearly 80 million CNIC (Computerized **(p.453)** National Identity Card) numbers and cards,[119] covering 99 per cent of the eligible male population but only 77 per cent of the female population 'due to social inhibitions'.[120] NADRA claims significant achievements in Pakistan's very disrupted society, stating that successful cash disbursement, and rehabilitation of Internally Displaced People, in the aftermath of the Swat Valley army operation against the Taliban, was possible due to accurate data available about the population with NADRA; that banks in Pakistan are 'flourishing because they know the identity of all their account holders'; and that 'arrests have been made after tracing mobile phones that are issued after verification of the applicants' CNIC'.[121]

4.3. Limited privacy protections

Pakistan has no data protection law, only some weak constitutional protections, and some other scattered statutory provisions. It has ratified the International Covenant on Civil and Political Rights 1966 (ICCPR), but not the Optional Protocol. Because it is not a monist state concerning international legal obligations, Article 17 of the ICCPR is not part of the domestic law of Pakistan.

Constitutional protections

The current (1973) Constitution of Pakistan contains a number of articles relevant to privacy protection, although there is no express protection of privacy except in relation to the home. These include protections against interference with 'the life, liberty, body, reputation, or property of any person' except 'in accordance with the law',[122] that the 'dignity of man, subject to law, the privacy of home, shall be inviolable',[123] and guarantees of 'freedom of speech and expression'.[124] Article 8 provides that 'Any law, or any custom or usage having the force of law, in so far as it is inconsistent with the rights conferred by this chapter, shall, to the extent of such inconsistency, be void' and 'The state may not make any law which takes away or abridges the right so conferred and any law made in contravention of this clause will, to the extent of such contravention, be void'.

These constitutional provisions do sometimes result in protection of privacy. One instance concerned a circular from the State Bank of Pakistan 'requiring banks and financial institutions to supply to the Central Board of Revenue information regarding profit/return in excess of PKR10,000 paid to account holders/depositors along with their names, addresses, National Tax Numbers, and National Identity Card Numbers'.[125] The courts held this unconstitutional on privacy grounds:

> The Lahore High Court subsequently held that taking private information of ordinary people without any allegation of wrongdoing would affect their lives, making them potentially vulnerable and insecure, and that it represented an extraordinary invasion of their fundamental right to privacy. Such a direction in subordinate legislation was illegal, unreasonable, and discriminatory, **(p.454)** being ultra vires of Articles 4 and 25 of the Constitution. The High Court accepted a Constitutional petition and struck down the impugned Circular as being without lawful authority.[126]

Islamic injunctions and the Constitution

The 1973 Constitution article 227 specifically obliges the state to develop laws in accordance with Islamic teachings and forbids enactment of any law that does not conform to the teachings of the Quran and Sunnah.[127] Pakistani NGOs are attempting to find support in the Quran for privacy protection, supported by

these constitutional provisions:[128]

> When we speak about privacy, we find that the Quran and Sunnah have an inventory of references that can play a key role in clarifying our understanding of Privacy Rights as guaranteed in Islamic teachings. This enables us to develop a standard to gauge the application of Islamic Privacy principles in Pakistan and see for ourselves how thoroughly they have been entwined and observed.

The authors identify a variety of privacy-related injunctions found in the texts of Islamic law.[129] It is possible, given the constitutional provisions concerning consistency with the injunctions of Islam, that these texts could be used in court to assist arguments that legislation or common law legal practices are unconstitutional.

Right to information and ombudsman laws

The Federal Ombudsman (Wafhaqi Mohtasib) is empowered 'to diagnose, investigate, redress and rectify any injustice done to a person through maladministration on the part of a Federal Agency or a Federal Government official'. 'The Mohtasib is empowered to award compensation to an aggrieved person for any loss or damage suffered by that person due to maladministration.'[130] Misuse of personal information by government agencies in Pakistan could readily fit within the concept of maladministration. Article 19A of Pakistan's Constitution, which states a right to 'access to information in all matters of public importance', was inserted only in 2010, and is in conformance with the 1993 *Sharif Case*,[131] which held that article 19 includes a right of citizens to receive information. As with elsewhere in South Asia, the first concrete steps toward data protection laws in Pakistan are found in its RTI law which gives individuals the right to access their own personal information held by government agencies, and protections against others accessing their information. Commencing in 2002, Pakistan enacted its laws earlier than other South Asian countries, and uses the terminology 'freedom of information'. However, the Pakistani laws are more limited than elsewhere.

The Freedom of Information Ordinance 2002 (FIO),[132] is a Presidential promulgation of dubious validity,[133] but has been in operation for over a decade. It applies only to agencies **(p.455)** of the Federal government and bodies established under Federal laws,[134] not to the broader classes of institutions receiving public funding found in the RTI laws of India and Bangladesh. However, the scope of information covered by the Ordinance is ambiguous.[135] There is an apparently broad right of access, that 'subject to the provisions of this Ordinance, no requester shall be denied access to any official record other than exemptions as provided in section 15',[136] and 'record' is defined broadly,[137] although 'official record' is not defined. However, the Ordinance then allows access to 'public records', a narrow range of records involving property transactions, licences, and similar government grants, and 'final orders and decisions', which are 'declared to be [on] the public record',[138] and access is allowed to those records only. Whether the second definition of access limits the first is unclear, but given that the Ordinance also requires that it be 'interpreted so as…to facilitate and encourage, the disclosure of information',[139] it probably does not. There are then exemptions from access, *inter alia*, of records relating to the personal privacy of other individuals; records of information provided on express or implied conditions of confidentiality; and records of 'banking companies and financial institutions relating to the accounts of their customers'.[140] Where applicants are dissatisfied, the Federal Ombudsman can investigate complains, and make binding decisions. There is no dedicated FOI tribunal.

Pakistan's Senate formed a subcommittee in 2012 to consider reforms to the law.[141] Journalists complain about the rate of refusal of access requests,[142] but the extent of use by individuals to access their own files is unknown. There are NGOs active in supporting FOI in Pakistan, and working for reform.[143] There are also provincial laws relating to freedom of information in Baluchistan (2005) and Sindh (2006) 'that set similar boundaries with regards to individual privacy per the federal ordinance'.[144]

Criminal law and electronic transactions law

The Pakistan Penal Code (PPC), dating from 1860 with few amendments, was amended in 2010 by provisions intended to prevent actions 'intending to insult the modesty of any woman', including an action which 'intrudes upon the privacy of such woman'.[145] The Code also contains protections against trespass

but otherwise does not protect privacy.[146]

(p.456) The Electronic Transaction Ordinance 2002,[147] although primarily dealing with electronic evidence and digital signatures, is now[148] the principal law under which cybercrime is prosecuted in Pakistan through provisions which also giving protection to privacy. It creates offences by the following third parties (not data controllers):

> Any person who gains or attempts to gain access to any information system with or without intent to acquire the information contained therein or to gain knowledge of such information, whether or not he is aware of the nature or contents of such information, when he is not authorised to gain access, as aforesaid.[149]
>
> Any person who does or attempts to do any act with intent to alter, modify, delete, remove, generate, transmit or store any information through or in any information system knowingly that he is not authorised to do any of the foregoing.[150]
>
> Any person who does or attempts to do any act with intent to impair the operation of, or prevent or hinder access to, any information contained in any information system, knowingly that he is not authorised to do any of the foregoing.[151]

'Information system' is defined with sufficient generality to include all forms of computer systems and other electronic information systems, including those in use at home.[152] Conviction under either section can lead to a maximum of seven years in prison, or a fine up to one million rupees, or both.

5. Sri Lanka

Apart from a few 'computer crime' offences, and a surprising ratification of the First Optional Protocol to the International Covenant on Civil and Political Rights 1966 (ICCPR), Sri Lankan law provides no privacy significant protections.

5.1. Sri Lanka—historical and legal context

Sri Lanka is no longer involved in a civil war, so the context for development of civil liberties is perhaps somewhat improved when compared with the previous decade, but still not very promising.

History and politics of Sri Lanka

Sri Lanka, an island nation of over 21 million population, was ceded by Portugal to the British in 1796, and became independent in 1948 as Ceylon.[153] Its name changed to Sri Lanka in 1972. From 1948 to the 1980s, it was a rare developing country that was 'able to maintain a system of stable and representative government'.[154] Two decades of civil war between the Sinhalese majority and Tamil separatists commenced in 1983, there was a cease-fire (to some extent) from 2002–06, but intensified fighting eventually resulted in the 2009 **(p.457)** government announcement that its military had defeated the remnants of the LTTE (Liberation Tigers of Tamil Elam) separatists.[155] The Sri Lankan government and army has been accused of crimes against humanity in its treatment of Tamils during and following its defeat of the LTTE.

Government and legal system of Sri Lanka

Sri Lanka is a republic within the Commonwealth. The President is both head of state and head of government, with a largely ceremonial Prime Minister. The Cabinet is chosen by the President in conjunction with the Prime Minister. The 1978 Constitution was modelled to a large extent on the French system and replaced the previous parliamentary-model constitution of 1972.[156] The current President was first elected in 2005 and re-elected in 2010 for a second six-year term. There is a unicameral Parliament also with six-year terms. The next election is scheduled for 2016.[157] Transparency International's Corruption Perception Index for 2012 ranks Sri Lanka 79th (of 176 countries) for overall government sector corruption, with a score of 40. Since independence Sri Lanka has maintained basic democratic institutions, with governments changing on a number of occasions through elections, and through three changes of constitution.[158]

Sri Lanka has a mixed legal system of Roman-Dutch civil law, English common law, and Jaffna Tamil customary

law.[159] Judges of both the Supreme Court and Court of Appeals are appointed by the President. Serious questions concerning the operation of the rule of law in Sri Lanka have been raised by critics including the US State Department, following the removal from office of the Chief Justice by the Parliament in January 2013 (ostensibly on corruption charges), after she had ruled against a bill that sought to grant greater power to the President's brother, who is the Economic Development Minister.[160] Sri Lanka is a member of the Commonwealth, SAARC, and WTO, but is outside the current area of coverage of APEC.

State surveillance in Sri Lanka—ID card

The Registration of Persons Department (RPD) is responsible for registration of persons and issuing the 'National Identity Card (NIC).[161] Since its creation in 1971, the RPD has registered and issued paper-based National ID cards to Sri Lankan citizens. The ID card is now compulsory for casting votes in national elections.[162] In November 2013 Pakistan's National Database and Registration Authority (NADRA) won the tender for the Sri Lanka ID Card project, the principal purpose of which is to digitize the existing paper-based system, which is said to involve 15 million cards.[163]

(p.458) 5.2. Constitutional, treaty, and common law privacy rights

Chapter III of the Constitution of Sri Lanka 1978 is silent as to a right to privacy. Marsoof, comparing the position in India[164] with that in Sri Lanka, notes that Sri Lanka's Constitution does not have a provision such as article 21 of the Indian constitution which, although it does not provide an express right of privacy, provides for the protection of 'personal liberty' from which courts have been able to infer a right of privacy.[165]

Sri Lankan courts have not developed any general right of privacy through the common law (including Roman-Dutch law). Marsoof is only able to identify a few scattered instances of protection of household privacy.[166] However, he considers that there is some possibility of a more general civil action for privacy developing under Roman-Dutch law:[167]

> it is manifest that the remedy against a breach of individual privacy is found in the Roman Dutch law (which is the common or residuary law of Sri Lanka) in the form of an action for injury under the *actio injuriarum.* However, it must be noted that this action is very restrictive as many requirements have to be satisfied to succeed in a claim.

ICCPR and Optional Protocol

Sri Lanka has ratified the ICCPR, and also ratified the Optional Protocol to the ICCPR in 1997 (for events occurring after that date), allowing 'communications' (complaints) to be made to the UN Human Rights Committee concerning its failure to uphold Article 17. Although there have been numerous communications brought against Sri Lanka to the Human Rights Committee, only one has given minor consideration to Article 17, in the context of the interference with privacy in the building of an expressway.[168]

5.3. Statutory privacy protections

The Information and Communication Technology Agency (ICTA) is the responsible government body for implementing data protection policies, and says that a 'number of data protection guidelines which are to be used by both public and government sectors are being formulated'[169] but nothing of significance has emerged from the last decade other than some vague policies.[170]

The Electronic Transactions Act 2006,[171] unlike its counterparts in other South Asian countries, is concerned solely with electronic contracts and certification services, and does **(p.459)** not include provisions relevant to data protection, computer crime, or a tribunal that could deal with these matters. The Telecommunication Act 1996 makes the interception of telecommunication transmissions and the disclosure of their contents an offence.[172]

The Sri Lankan government continues to refuse to enact RTI legislation,[173] but there is an active campaign by NGOs to promote such legislation.[174] In 2004 the former President introduced a Freedom of Information Bill, but it lapsed with the Parliament. An opposition Bill in 2011 was defeated.[175]

Computer crimes and compensation

The Computer Crimes Act 2007[176] (CCA) contains a number of offences potentially relevant to data protection, and a significant compensation provision which, in effect, creates civil liability for privacy interferences, but does not give the data subject the right to initiate the action, because a criminal prosecution must come first.

The offences potentially relevant to data protection include those concerning unauthorized access, unauthorized modifications, dealing with illegally obtained data, illegal interception,[177] and many related offences. Section 14(1) establishes the right to compensation:

> Where a person is convicted of an offence under this Act, and where it is established that as a result of the commission of such offence—(a) loss or damage was caused to any person or institution; or (b) monetary gain accrued to the offender or any other person, the court shall, in addition to any other punishment that may be imposed on the offender, make order for the payment by the offender—(i) of compensation, to the person or institution that incurred loss or damage; or (ii) of a sum equivalent to the value of the monetary gain so accrued, to the State, as the case may be.

The compensation is for 'loss or damage'. A compensation order may be enforced in the District Court. The section provides that the court 'shall' make a compensation order where loss or damage has occurred, and the Act also provides assistance to the data subject to prove such harm:

> A Certificate under the hand of an expert containing a record of the quantum of compensation as computed by the victim and a statement whether in the opinion of the expert, the quantum of compensation is proportionate to the loss or damage caused or the monetary value of the gain accrued shall be admissible in evidence and shall be *prime facie* proof of the facts stated therein.[178]

The qualifications and appointment of such experts, and their investigative powers, are specified.[179] A compensation order 'shall not debar or prejudice any right of that person to a civil remedy for the recovery of damages', and the statute of limitations for bringing such a civil action will only run from the time such an order is made.[180] **(p.460)**

6. Maldives

The Republic of the Maldives is an island nation in the Indian Ocean, south-west of India, consisting of a double chain of 26 atolls. Its population is under 350,000. Protection of privacy in the Maldives is at present based on extensive (but untested) constitutional rights, and little else, within the context of a fragile democracy and attempts to consolidate the rule of law. Tourism is the Maldives' largest economic activity, accounting for 28 per cent of GDP and more than 60 per cent of foreign exchange receipts. Over 90 per cent of government tax revenue comes from import duties and tourism-related taxes. The country is threatened by global warming, with 80 per cent of its land area one metre or less above sea level.[181]

6.1. Maldives—political, economic, and social context

The Maldives was a sultanate from the twelfth century, became a British protectorate in 1887, and became a republic in 1968, three years after independence.[182] There has been a move toward democracy over the past decade, disrupted in recent years by political instability. President Gayoom ruled a one-party state for 30 years, 're-elected' at six successive single-party referenda. After political demonstrations in 2003, political parties were legalized in 2005. In 2008 the Special Majlis, a constituent assembly, finalized a new constitution, and the 'first-ever presidential elections under a multi-candidate, multi-party system, were held'. Gayoom was defeated in a run-off poll by a former political prisoner. However, in 2012 newly elected President Nasheed resigned 'after several weeks of street protests following his sacking of a top judge' and handed over power to his Vice President.[183] Accusations of a coup followed, but a Commonwealth-supervised investigation found the transition of power to be constitutional. New elections were supposed to be held in September 2013,[184] but there were repeated interventions by the Supreme Court (seen as loyal to the Gayoom faction) which disrupted the completion of the elections.[185] In November 2013 Abdulla Yameen, half-brother of former President Gayoom, became President after defeating former President Nasheed in a run-off election with over 90 per cent voter turnout. The Commonwealth has removed the

expulsion of the Maldives from its agenda, following the restoration of democratic government.[186] The prospect for development of laws concerning civil liberties such as data privacy under the new government is unknown.

Government and legal systems in the Maldives

Since its first written constitution in 1932, the Maldives has had six subsequent constitutions, the most recent in 2008.[187] The legislature is a unicameral People's Council **(p.461)** (People's Majlis), with five-yearly elections. The current constitution[188] declares it to be 'a sovereign, independent, democratic Republic based on the principles of Islam'.[189] 'A non-Muslim may not become a citizen of the Maldives.'[190] The President is directly elected and is both chief of state and head of government, as well as head of the armed forces. The President appoints cabinet ministers. The Maldives is a member of SAARC, the Commonwealth, and the WTO.

The legal system is 'an Islamic religious legal system with English common law influences, primarily in commercial matters'.[191] Islam is the state religion, and 'no law contrary to any tenet of Islam shall be enacted'.[192] There are no separate Islamic courts. The Maldives has a Supreme Court with judges appointed by the president with approval of the People's Council. Judges of other courts, are appointed by the Judicial Service Commission. There is at present an interim Supreme Court, some of whose judges were appointed under the previous (pre-2008) constitution, and there is considerable controversy about judicial appointments and the composition of the court.[193]

Public opinion, civil society, and surveillance in the Maldives

Calls for a privacy law for the Maldives have been prompted by serious data leaks, such as one which resulted in access via a website to the personal details of 234,000 Maldivians over the age of 17, including details such as national ID number and date of birth. It was suspected that this data was leaked from Elections Commission. The Civil Service authority also published the salaries of all civil servants on the Internet.[194] The Department of National Registration operates the Maldives ID card system.

6.2. Limited privacy protections

In theory, the Maldives has very general and strong privacy protections arising from its Constitution and supported by its treaty obligations. But it has little by way of specific statutory provisions.

ICCPR and Optional Protocol

The Maldives has ratified the International Covenant on Civil and Political Rights 1966 (ICCPR), and also ratified the Optional Protocol to the ICCPR in 2006, allowing 'communications' (complaints) to be made to the UN Human Rights Council concerning its failure to uphold Article 17. Courts interpreting constitutional rights and freedoms are required to 'consider international treaties to which the Maldives is a party'.[195] No such communications have been made concerning Article 17. The Maldives does not take a monist approach to international law, so Article 17 is not part of Maldives domestic law.

(p.462) Constitutional rights relevant to privacy

The Maldives Constitution 'guarantees to all persons, in a manner that is not contrary to any tenet of Islam', a series of rights and freedoms contained within Chapter III, subject only to reasonable and 'demonstrably justifiable' legislative limits.[196] Even limits enacted 'in order to protect and maintain the tenets of Islam' must comply with these requirements. In addition to general protections of freedom of conduct not prohibited by law,[197] three constitutional protections are particularly relevant to privacy protection:

(i) 'Everyone has the right to life, liberty and security of the person, and the right not be deprived thereof to any extent except pursuant to a law made in accordance with Article 16 of this Constitution.'[198]

(ii) 'Everyone has the right to respect for his private and family life, his home and his private communications. Every person must respect these rights with respect to others.'[199] This explicit constitutional right of privacy (similar to ICCPR Article 17) is also expressed in terms that suggest a 'horizontal' right maintainable against private parties, rather than one only available against the state. This is also implied by the obligations on all persons to respect these rights.[200]

(iii) Protection against searches of the person, and the privacy of the home, are also included.[201]

In addition there are potentially relevant protections of thought and communication, media activities, reputation, and other freedoms.[202] The Constitution also has provisions concerning the security services, including for the authority of the People's Majlis over the security services.[203]

Human Rights Commission

The Maldives' Constitution requires establishment of a Human Rights Commission,[204] now established[205] under the Human Rights Commission Act 2006 (HRC).[206] The five-member **(p.463)** independent Commission has powers to investigate complaints alleging an infringement of human rights, and to give advice to government on human rights issues.[207] It has various investigative powers.[208] After investigation it can attempt to conciliate, but if conciliation fails it can only refer the matter to a court,[209] so it is largely toothless. It is required to publish an annual report.[210] The Commission is an Associate Member of the Asia-Pacific Forum of human rights bodies (see Chapter 2, section 6.5). Because the Act requires that an appointee to the Commission 'must be Muslim',[211] this inconsistency with the Paris Principles meant that it could not be a full member.[212]

Right to Information Bill

The Maldives does not yet have a Right to Information Law. The pre-2008 Parliament rejected an RTI bill in 2007 by one vote. A Bill was before a committee in 2012, with some commentators expecting it would soon progress to the floor of Parliament for a vote.[213] The Right to Information Bill which was under consideration from 2010[214] goes beyond providing only a right of access and includes the objective of 'providing a right to every individual to ensure that information held by a public authority in relation to that individual is complete, accurate and not misleading',[215] thus including both correction and data quality rights more often associated with data privacy laws. It also includes a right of compensation for damage caused by breaches.[216]

7. Bhutan

In 1972 Bhutan's King proposed that 'Gross National Happiness' was more important than Gross National Product, and since then the idea has become one of the philosophical foundations of Bhutan, and has been developed and quantified.[217] Could a data privacy law improve Bhutan's Gross National Happiness? At present, its laws do not provide any privacy protections.

7.1. Bhutan—political, economic, and social context

The Kingdom of Bhutan is a small landlocked country of both subtropical plains and rugged mountains, located on the north-east border of India, and also shares a border with China. It has a population of around 1.5 million.[218] It has over the past decade made the transition from an absolute to a constitutional monarchy. Bhutan's small economy (a purchasing power parity GDP of less than US$5 billion) is based on agriculture and **(p.464)** forestry, with low foreign investment and use of Indian migrant labour for major construction. Bhutan is a member of SAARC and a WTO observer state. In 1999, the government lifted a ban on television and the Internet.

Government and legal system of Bhutan

British influence in Bhutan since 1865 led to the establishment of a monarchy in 1907. A 1910 treaty whereby Bhutan allowed Britain to direct its foreign affairs was assumed by India after independence in 1947. This was formalized by a treaty in 1949, renegotiated in 2007 to give Bhutan greater autonomy in foreign affairs. In 2005, Bhutan's King introduced a draft constitution including democratic reforms. In 2006, he abdicated in favour of his son, Jigme Khesar Namgyel Wangchuck. The new king ratified the country's first constitution in July 2008.[219] Elections to the country's first parliament were held in March 2008, with competitive parties in the lower house.[220] A Prime Minister, leader of the majority party, heads a Council of Ministers (Lhengye Shungtsog) nominated by the King and approved by the National Assembly. There is also an upper house. There are 10 Ministries.[221] Transparency International's Corruption Perception Index for 2012 ranks Bhutan 33rd (of 176 countries) for overall government corruption, with a score of 63. This gives Bhutan the 'least corrupt' ranking for any country in South Asia.

The legal system is based on a comprehensive codification, deriving substantially from Buddhist religious law.[222] About 75 per cent of the population are Buddhist. The Supreme Court is the apex court of appeal, in a four-level hierarchy also comprising High, Dzongkhag, and Dungkhag Courts. There are no courts or tribunals of special jurisdiction. The Supreme Court is the final authority on constitutional interpretation.[223]

State surveillance and ID cards in Bhutan

Bhutanese have an 11-digit citizenship number allocated at birth, and from age 15 a citizenship card is allocated from a central registry (Bhutan Civil Registration System) which stores thumbprints and a digital image of each person. Only Bhutanese citizens are entitled to cards. Since 2004 new plastic cards have been issued, with data encoded on a magnetic strip on the card rear.[224] The accuracy of some data in the register, such as birth **(p.465)** dates, has been questioned.[225] A sign of Bhutan's engagement in the modern world is that it now has a credit information bureau which provides positive and negative credit information, and has been developed in association with Dun & Bradstreet.[226]

7.2. Lack of privacy protections

Bhutan's Constitution does not specifically include protection of privacy in its list of fundamental rights,[227] but it includes many rights relevant to privacy protection, including rights to 'life, liberty and security of person', 'freedom of speech, opinion and expression' and 'freedom of thought, conscience and religion'. 'Freedom of the press, radio and television' is also included. The list also includes 'the right to information', but this has not yet resulted in a 'RTI law' such as has occurred in India, Nepal, and Bangladesh. Legitimate grounds for limiting these constitutional rights are defined.[228] Direct enforcement of Constitutional rights is provided: 'the right to initiate appropriate proceedings in the Supreme Court or High Court for the enforcement of the rights conferred by this Article.'[229] There is no legislation which is directly relevant to data privacy.[230]

8. Afghanistan

Whether data privacy will ever become an issue that ranks with the many other pressing issues facing the Afghan people remains to be seen, but it is likely to be a long while in the future, other than for some security-related issues such as recording of ethnicity on ID cards. However, despite Afghanistan's 35 years of civil war, major economic changes to the country, due largely to Chinese and Indian investment, mean that Afghanistan is not necessarily the captor of its recent past.[231] There are numerous Asian examples of where change, when it occurs, is far more rapid and fundamental than observers predicted.

8.1. Afghanistan—political, economic, and social context

Afghanistan has not experienced peace since 1978 when a Communist counter-coup was followed a year later with invasion by the Soviet Union.[232] Three decades of external interventions and civil wars have followed including the 1989 USSR withdrawal, the 1996 final victory of the Taliban, and the defeat of the Taliban government by the USA, its allies, and northern Afghan forces, following the 2001 attacks on New York City. After the UN-sponsored Bonn Conference in 2001 a new constitution was adopted in 2004. A Presidential election was held in 2004, and a National Assembly constituted in 2005. President Karzai was re-elected in August 2009.[233] He cannot run again in 2014 (and seems unlikely to organize a dynastic succession), but if he constitutionally transfers power to his **(p.466)** successor this will be the first such occurrence in Afghan history.[234] It is not possible for anyone to predict what will be Afghanistan's political future following the ongoing withdrawal of allied troops, and the uncertain tenure of their continued presence. Huge Chinese investment in the development of Afghanistan's mineral wealth, and Indian construction of a transport corridor from Afghanistan to an Iranian port (thereby bypassing Pakistan) means that those countries will have a much greater future stake in stability in Afghanistan.[235]

The population of Afghanistan is over 30 million, almost all of whom follow Islam. Its social situation has been described as follows:

> Afghanistan is extremely poor, landlocked, and highly dependent on foreign aid. Much of the population continues to suffer from shortages of housing, clean water, electricity, medical care, and jobs. Criminality, insecurity, weak governance, and the Afghan Government's difficulty in extending rule of law to all parts of the country pose challenges to future economic growth.[236]

Government and legal system of Afghanistan

Afghanistan under its 2004 Constitution is an Islamic republic, with an elected president and bicameral legislature. Its legal system is a mixed system of civil, customary, and Islamic law. The Supreme Court comprises nine judges, and there are also Cassation and Sharia courts. Afghanistan is a member of SAARC, and a WTO observer state. Transparency International's Corruption Perception Index for 2012 gives Afghanistan a score of 8, ranking its public sector as 'highly corrupt'. It is the equal lowest score for any country's public sector at a ranking of 174th.[237] Under these circumstances, the operation of the rule of law necessary for any data privacy protections to be effective is highly unlikely.

State surveillance and ID cards in Afghanistan

The extent of surveillance activities in Afghanistan is beyond the scope of this chapter. The Afghan government's Electronic National ID Card (eNID) project wants to issue chip-based ID cards (called 'taskera' or 'tazhira') to citizens before the April 2014 presidential election, to replace existing ID cards. 'Under the proposed format of the new biometric documents holders' ethnicity would in fact be contained on the cards' smart chips. Their ethnicity, however, would not be printed on the face of the card itself.'[238] There is considerable controversy over whether ethnic identity should be visible on the card face.

8.2. Privacy-related provisions

Chapter III of the 2004 Constitution[239] on 'Fundamental Right and Duties of Citizens', lists many rights which could under different circumstances be relevant to privacy protection, including 'liberty and dignity', freedom of expression, protection against entry into or inspection of private residences 'without prior permission of the resident or holding a court order', and confidentiality of all forms of communication 'unless authorized by the **(p.467)** provisions of law'. It also provides for 'the right of access to the information from the government offices in accordance with the provisions of law'. There is no specific right to rely upon these rights to found an action before a court.

Afghanistan has ratified the International Covenant on Civil and Political Rights 1966 (ICCPR), but not its First Optional Protocol, so complaints to the UN Human Rights Committee are not possible. It does not take a monist approach to international law, so Article 17 is not part of Afghan domestic law. The Afghanistan Independent Human Rights Commission has been established[240] by law in 2005,[241] as required by the Constitution.[242] It was admitted in 2005 as a full member of the Asia-Pacific Forum of national human rights institutions.[243] Understandably, data privacy issues are not high on its agenda. A draft Access to Information Law[244] was prepared in 2011 in Afghanistan after consultation between government and civil society organizations, but not yet enacted. International NGOs have assessed the draft law as broadly applicable to all public bodies, with good access mechanisms and reasonably narrow exceptions, but failing to meet some other desirable international standards such as the provision of an independent oversight body.[245] However, there does not seem to have been progress towards its enactment since then.

Notes:

([1]) Transparency International, 'Corruption by Country/Territory' <http://www.transparency.org/country>.

([2]) This summary is derived from Y.K. Malik et al., ch. 25 (Nepal) 'Political Heritage and Culture' in *Government and Politics in South Asia* (6th Edn., Westview Press, 2009) and *CIA World Factbook*, 'Nepal: Background' <https://www.cia.gov/library/publications/the-world-factbook/geos/np.html>.

([3]) On 1 June 2001, 'King Birendra's entire family was massacred, presumably by Crown Prince Birendra': Malik et al., *Government and Politics in South Asia*, p. 397.

([4]) See International Crisis Group, 'Nepal's Constitution: The Political Impasse' <http://www.crisisgroup.org/en/publication-type/media-releases/2012/asia/nepal-nepals-constitution-the-political-impasse.aspx> 10 February 2014; and The Economist, 'Constitutional crisis in Nepal: Ceremonial time', *The Economist*, 17 November 2012 <http://www.economist.com/news/asia/21566659-government-fails-hold-promised-elections-speculation-grows-about-how-president-will> 10 February 2014; also S.K. Sharma, 'Nepal: the constitutional Holy Grail' on India Strategic Studies <http://strategicstudyindia.blogspot.com.au/2013/01/nepal-constitutional-holy-grail.html>.

([5]) Gardiner Harris, 'Nepal Picks New Premier, Putting End to Stalemate' (*New York Times*, 10 February 2014).

([6]) For an overview of Nepal's legal system, see M.E. Karim and S.S. Pokhrel, *Research Guide of the Legal System of Kingdom of Nepal*, on GlobaLex October 2012 <http://www.nyulawglobal.org/globalex/Nepal.htm>. See also *CIA World Factbook*, 'Nepal: Government'. The following account is drawn from both sources.

([7]) CCRI website <http://www.ccrinepal.org/>.

([8]) Privacy International, 'Nepal' (*Privacy in the Developing World*, 22 October 2012) (hereinafter PI Nepal Report) 'III Surveillance policies: Law Enforcement communications surveillance' <https://www.privacyinternational.org/reports/nepal/iii-surveillance-policies>; Bill on Control and Punishment of Organized Crimes 2067 BS (2010).

([9]) PI Nepal Report, 'III Surveillance policies: Search and seizure'.

([10]) PI Nepal Report, 'IV Privacy Issues: DNA database'.

([11]) PI Nepal Report, 'IV Privacy Issues: Cyber-cafes'.

([12]) National ID Management Center <http://www.nidmc.gov.np/index.php/en/>.

([13]) *PI Nepal Report*, 'IV Privacy Issues: National ID card'; consultants were funded by the Asian Development Bank, and World Bank funding is being sought for the project.

([14]) *PI Nepal Report*, 'IV Privacy Issues: National ID card'; see also 'Progress Status' at <http://www.nidmc.gov.np/index.php/en/progress-report> 11 February 2014.

([15]) 'ID-ing Nepal: A national ID card system is cause for both good cheer and fear' (*Nepal Times*, 23 April 2010) <http://nepalitimes.com/news.php?id=17017>. According to the Joint Secretary of the Office of Prime Minister and Council of Ministers in 2010: 'Eventually, we aim to make it a multi-purpose card and it can be used to hold information about property ownership, driving licenses and criminal records.'

([16]) Nepal Election Channel, '10 Million Appeared for Biometric Voter ID Card' (13 April 2012) <http://www.nepalelectionchannel.org/english/stories/353-102-million-appeared-for-biometric-voter-id-card-ec.html>.

([17]) Article 19 NGO, *Memorandum on the Right to Information Act 2007 of the State of Nepal*, January 2008 <http://www.article19.org/data/files/pdfs/analysis/nepal-rti-act.pdf>; 'Arguably, the rule of the ICCPR, to which Nepal is a party, should prevail over the RTI Act. Section 9.1 of Nepal Treaty Act 1990 reads: "If any provision of the treaty of which His Majesty's Government or the Kingdom of Nepal is party, after such treaty is ratified, acceded or approved, is inconsistent with any law in force, such law to the extent of such inconsistency, shall be void and the provision of the treaty shall come into force as law of Nepal."'

([18]) The Chair of the Committee on Fundamental Rights and Directive principles of the Constituent Assembly, Privacy International, and Privacy Nepal have suggested that the following language should replace that of the Interim Constitution: 'Everyone has the right to the protection of the law against arbitrary or unlawful interference with his privacy, home, property, communications, or information; Any limitation to the exercise of this right must be provided for by law and respect the essence of this right'; PI Nepal Report, 'II Legal Framework: Constitutional Provisions for Privacy'.

([19]) *PI Nepal Report*, 'II Legal Framework: Supervisory Authority for Privacy Laws and Complaints' which refers to the cases *Annapurna Rana v Kathmandu District Court and Others*, Nayadoot, Nepal Bar Association, 1998, No. 2, p. 53, SAB (1998), No 7, p. 11 and *Sapana Pradhan Malla for FWLD v Government of Nepal*, writ no. 3561 of 2063.

([20]) *PI Nepal Report*, 'II Legal Framework: Statutory Protections for Privacy' cites only Postal Act, 1962 (s. 47 and s. 58); Telecommunication Act 1962 (ss. 23 (a), 24, and 27 (b)); and the Chapter on Court Procedure (s. 172) of Muluki Ain.

([21]) National Human Rights Commission <http://www.nhrcnepal.org/>.

([22]) *PI Nepal Report*, 'II Legal Framework: Supervisory Authority for Privacy Laws and Complaints'.

([23]) Right to Information Act 2007 (Nepal) <http://www.moic.gov.np/acts-regulations/right-to-information-act.pdf> (unofficial English translation).

([24]) 'The RTI Act was the result of approximately 15 years worth of advocacy led by the media and civil society organizations…Pressure from media and civil society organizations was also indispensable in establishing the National Information Commission (NIC)': *PI Nepal Report*, 'IV Privacy Issues: Freedom of Information / Right to Information Laws' <https://www.privacyinternational.org/reports/nepal>.

([25]) T.R. Ayral, 'Assessment of Right to Information Law Regime in Nepal for Creating Conducive Environment for Effective Implementation' (*1st National Convention on Right to Information Kathmandu*, Nepal March 28–29, 2011) <http://www.freedomforum.org.np/content/attachments/article/121/WorkingPaper_RTI%20Law_TRAryal.pdf>.

([26]) T.R. Aryal, General Secretary of the NGO 'Citizen's Campaign for Right to Information' states: 'In 1994 the Supreme Court, in *Arun III hydropower case*, described the importance of RTI and directed the government to enact RTI law. Further, in this case, the court also set eight-point procedures to provide copy of documents by public agencies until any such law is enacted.' Ayral, 'Assessment of Right to Information Law Regime in Nepal', citing *Advocate Gopal Siwakoti et al v Ministry of Finance and others, Writ Petition* 3049/050.

([27]) Right to Information Regulation 2009 (Nepal) <http://www.moic.gov.np/acts-regulations/right-to-information-rules.pdf>.

([28]) RTI Act (Nepal) s. 11.

([29]) RTI Act (Nepal), s. 9.

([30]) RTI Act (Nepal), s. 10.

([31]) RTI Act (Nepal), s. 34.

([32]) RTI Act (Nepal), s. 19.

([33]) NIC <http://nic.gov.np/>.

([34]) RTI Act (Nepal), s. 3.

([35]) RTI Act (Nepal), s. 2.

([36]) RTI Act (Nepal), s. 2.

([37]) *Padma Kumar Medhasi Sha (Appellant) and Nepal Share Markets and Finance Ltd (Defendant)* (NIC Annual Report, 2011/12) pp. 80–1.

([38]) RTI Act (Nepal), s. 30.

([39]) Open Society Foundation, 'Students Win Right to Information Case at Nepal's Supreme Court' (Press Release 14 June 2011) <http://www.opensocietyfoundations.org/press-releases/students-win-right-information-case-nepals-supreme-court>.

([40]) *Ashesh Neupane (Appellant) and Examination Controller Office (Defendant)* (NIC Annual Report, 2011/12) 68.

([41]) RTI Act (Nepal), s. 5(3).

([42]) RTI Act (Nepal), s. 45.

([43]) RTI Act (Nepal), s. 3(3)(e).

([44]) RTI Act (Nepal), s. 3(3).

([45]) RTI Act (Nepal), s. 3(4).

([46]) RTI Act (Nepal), s. 27(1).

([47]) RTI Act (Nepal), s. 27(2).

([48]) RTI Act (Nepal), s. 27(3).

([49]) RTI Act (Nepal), s. 27(5)–(6).

([50]) RTI Act (Nepal), s. 27(4).

([51]) This paragraph is based on the NIC's Annual report, 2011/12, p. 22 as translated by Mr Shalik Ram Sharma.

([52]) RTI Act (Nepal), s. 7(1).

([53]) RTI Act (Nepal), s. 31(2).

([54]) RTI Act (Nepal), s. 28(1).

([55]) RTI Act (Nepal), s. 28(2).

([56]) RTI Act (Nepal), s. 32.

([57]) The name 'Shangri La' was coined by James Hilton in his 1933 novel *Lost Horizon*, 'to describe a magical place, where people lived amiably amid spectacular natural beauty'. The Chinese government has now re-named part of the Kham region of eastern Tibet as Shangri La in order to tap its tourism potential: D. Zurich, ch. 5 'A Map of Shangri La' in *Himalaya: Encounters with the Roof of the World* (The Centre for American Places at Columbia College Chicago, 2011), pp. 69–86.

([58]) Article 19 NGO, *Memorandum on the Right to Information Act 2007 of the State of Nepal*, p. 2; The assessment was made jointly with the Federation of Nepali Journalists and Freedom Forum.

([59]) Ayral, 'Assessment of Right to Information Law Regime in Nepal', p. 12.

([60]) For the modern history of Bangladesh, see Francis Pike, *Empires at War: A Short History of Modern Asia Since World War II* (I B Tauris, 2010), chs. 13, 24, 41 and 48. See also Malik et al., *Government and Politics in South Asia*, chs. 14–18.

([61]) Malik et al., *Government and Politics in South Asia*, p. 247.

([62]) Malik et al., *Government and Politics in South Asia*, chs. 15 and 16.

([63]) CIA *World Factbook*, 'Bangladesh', 14 December 2012 <https://www.cia.gov/library/publications/the-world-factbook/geos/bg.html>. Other demographic and economic data in this section are from this source unless otherwise specified.

([64]) T. Ahmed, 'Govt set to monitor phone calls despite writ pending with High Court' (*NewAge*, 27 August 2008) <http://struggleforliberty.wordpress.com/2008/08/29/govt-set-to-monitor-p.>. See also Privacy International, *Bangladesh*, Privacy in the Developing World Project, 22 October 2012 <http://www.privacyinternational.org/reports/bangladesh> (hereinafter 'PI Bangladesh Report').

([65]) Malik et al., *Government and Politics in South Asia*, ch. 15 summarizes the fluctuations of democracy.

([66]) Since 2007 Bangladesh statutes are no longer enacted in English but only in Bengali. However, it is common for statutes to require the implementing agency to provide an English translation following enactment.

([67]) PI Bangladesh Report, Part I.

([68]) VOICE <http://www.voicebd.org>.

([69]) 'Right to communication' (VOICE) <http://www.voicebd.org/communication>.

([70]) VOICE, 'Speakers demanded privacy and data protection law in the national convention' <http://www.voicebd.org/node/361>.

([71]) PI Bangladesh Report, Part II.

([72]) National Identity Registration Act 2010 (Bangladesh).

([73]) NIR Act (Bangladesh), s. 5.

([74]) NIR Act (Bangladesh), s. 3.

([75]) NIR Act (Bangladesh), s. 7.

([76]) NIR Act (Bangladesh), ss. 14–21.

([77]) BBC, 'A card that fosters national identity in Bangladesh' (*BBC News: India*, 19 July 2012) <http://www.bbc.co.uk/news/world-asia-india-18261373>.

([78]) BBC News India.

([79]) Editorial, 'National ID card for all' (*The News Today* Dhaka, Bangladesh, 30 July 2013) <http://www.newstoday.com.bd/index.php?option=details&news_id=2352387&date=2013-07-30>.

([80]) BBC, 'A card that fosters national identity in Bangladesh'.

([81]) Central Intelligence Agency (US), *CIA World Factbook: Bangladesh*, 'People and Society' <https://www.cia.gov/library/publications/the-world-factbook/geos/bg.html>.

([82]) English translation available at <http://www.infocom.gov.bd/ic/forms/rti_english.pdf>.

([83]) RTI Act (Bangladesh), s. 32 and Schedule.

([84]) RTI Act (Bangladesh), s. 4.

([85]) RTI Act (Bangladesh), s. 7(h).

([86]) RTI Act (Bangladesh), s. 7(i).

([87]) RTI Act (Bangladesh), s. 7(r).

([88]) Section 3 of the RTI Act (Bangladesh): 'Of any existing law—(a) the provisions of providing information shall not be affected by the provisions of this Act; and (b) the provisions of creating impediment in providing

information shall be superseded by the provisions of this Act if they become conflicting with the provisions of this Act.'

([89]) RTI Act (Bangladesh), s. 10.

([90]) RTI Act (Bangladesh), s. 9.

([91]) Information Commission <http://www.infocom.gov.bd/ic/index.php?lang=en>.

([92]) RTI Act (Bangladesh), s. 12.

([93]) RTI Act (Bangladesh), s. 13.

([94]) RTI Act (Bangladesh), s. 13(5).

([95]) RTI Act (Bangladesh), s. 14–16.

([96]) RTI Act (Bangladesh), s. 24.

([97]) RTI Act (Bangladesh), s. 25(10).

([98]) RTI Act (Bangladesh), s. 27.

([99]) RTI Act (Bangladesh), s. 25(11)(a)(vi).

([100]) Information Commission of Bangladesh, *Annual Report 2011* (Translated version of Bangla Annual Report from chs. 1–6) <http://www.infocom.gov.bd/ic/images/stories/annual_report_2011_english.pdf>.

([101]) Information Commission, *Annual Report 2011*, Executive Summary.

([102]) Information Commission, *Annual Report 2011*, Executive Summary.

([103]) Enforcement was summarized by the Commission as follows: 'The total number of collected applications from all over the country starting from 1st January 2011 to 31st December, 2012 [2011?] using the RTI Act prescribed form is 7808. Among them, 7671 applications were submitted to the government authorities and 137 to the NGOs, which demonstrate 98.25% and 1.75% of the total collected applications successively. Out of all applications, 7616 (97.54%) appeals have been responded with the sought information, 104 (1.33%) applications are pending and 88 (1.12%) applications have been discarded. The rejected appeals are minimal in number as most of the applications have been responded with information. No case of taking action against any Designated Officer was found in any report. However, one official has been fined tk. 1000/- (One thousand) as he was proved culpable at the end of the hearing of a petition in Information Commission. Since its establishment, the Commission has taken 44 complaints into account amongst the 104 filed complaints. 60 complaints have been discarded by the Commission as they were found faulty.'

([104]) ICT Act 2006 (Bangladesh) <http://www.prp.org.bd/downloads/ICTAct2006English.pdf>.

([105]) ICT Act (Bangladesh), s. 43.

([106]) ICT Act (Bangladesh), s. 68.

([107]) ICT Act (Bangladesh), s. 82.

([108]) ICT Act (Bangladesh), s. 84.

([109]) For the modern history of Pakistan, see Pike, *Empires at War*, chs. 13, 24, 41, 51, and 60, and pp. 720–1. See also Malik et al., *Government and Politics in South Asia*, chs. 8–13.

([110]) *CIA World Factbook*, 'Pakistan', 17 January 2013 at <https://www.cia.gov/library/publications/the-

world-factbook/geos/pk.html>.

([111]) Omar Sial, 'Update: A Legal Research Guide to Pakistan', '5. Government' (GlobaLex, January 2009) <http://www.nyulawglobal.org/globalex/pakistan1.htm>.

([112]) Constitution of Pakistan, 1973 (as amended), Article 2 <http://www.pakistani.org/pakistan/constitution/>.

([113]) Sial, 'Update: A Legal Research Guide to Pakistan', '8. The Court System'.

([114]) Bytes4All is a Pakistani NGO which focuses on the use of information and communications technologies for social justice, and collaborates with Privacy International in its 'Privacy in Asia' project. See <http://content.bytesforall.pk/>.

([115]) PI Pakistan Report, section III 'Statutory protections for privacy: Communications privacy'. <https://www.privacyinternational.org/reports/pakistan/iii-statutory-protections-for-privacy>.

([116]) 'Most recently, the Pakistan Telecommunication Authority commissioned a new wave of surveillance and censorship, whereby all emails, telephone calls and communications will be monitored. Service providers have less than three months to adopt arrangements to facilitate such mass surveillance, which will come at a cost of millions of dollars to the Pakistani taxpayer. The government has sought to justify the move by emphasizing the need to protect individuals from obscenities and instances of blasphemy in the digital communications sphere. Yet no legal procedures or mechanisms have been proposed to protect an individual's online freedom of expression and privacy. The scheme is no more than a veiled attempt to increase State control over individuals, chilling free expression and quashing dissent and political activism.' Bytes4All, 'A new wave of surveillance in Pakistan' 30 October 2012, in PI Update Issue 1, December 2012.

([117]) N. Dad, 'Pakistan needs comms security not restrictions' on Privacy International website at <https://www.privacyinternational.org/blog/pakistan-needs-comms-security-not-restrictions>.

([118]) See NADRA <http://www.nadra.gov.pk/>. See also Wikipedia entry 'National Database and Registration Authority'.

([119]) The CNIC has the following information on it: legal name, gender, father's name (husband's name for married females), identification mark, date of birth, national identity card number, family ID number, current address, permanent address, date of issue, date of expiry, signature, photo, and fingerprint (thumbprint).

([120]) Staff author, '90% adults registered with NADRA: Tariq Malik' (*The Express Tribune*, Pakistan, 29 June 2010) <http://tribune.com.pk/story/24554/90-adults-registered-with-nadra-tariq-malik/?print=true>.

([121]) Tariq Malik, quoted in '90% adults registered with NADRA: Tariq Malik'.

([122]) Constitution 1973 (Pakistan), art. 4(2).

([123]) Constitution 1973 (Pakistan), art. 14(1).

([124]) Constitution 1973 (Pakistan), art. 19.

([125]) PI Pakistan Report, section III 'Statutory protections for privacy: Financial privacy'.

([126]) PI Pakistan Report, section III 'Statutory protections for privacy'.

([127]) Article 227 states: 'All existing laws shall be brought in conformity with the Injunctions of Islam as laid down in the Holy Quran and Sunnah, in this Part referred to as the Injunctions of Islam, and no law shall be enacted which is repugnant to such injunctions.'

([128]) Authors of the report *Pakistan*, 'Privacy in the Developing World' project, published by Privacy

International, 23 October 2012 <https://www.privacyinternational.org/reports/pakistan> (hereinafter 'PI Pakistan Report').

([129]) PI Pakistan Report, section II 'Constitutional provisions for privacy'.

([130]) Sial, 'Update: A Legal Research Guide to Pakistan', '8.7 The Ombudsman (Wafaqi Mohtasib)'.

([131]) *Sharif v Pakistan*, PLD 1993 S.C. 471.

([132]) Freedom of Information Ordinance 2002 (Pakistan).

([133]) Banisar explains that 'In October 2002, President Pervez Musharraf promulgated the Freedom of Information Ordinance 2002, largely at the urging of the Asian Development Bank. Although the Ordinance should have lapsed within 6 months, the President has issued a constitutional decree which has ensured the continuance of the Ordinance. The Ombudsman ruled in April 2004 that the Ordinance still was in force even in the absence of the regulations. Rules were issued in June 2004, but without any input from stakeholders' (footnotes in original omitted): D. Banisar, *Freedom of Information Around the World 2006* (Privacy International, 2006) 118, at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1707336>.

([134]) See definition of 'public body' in art. 4(2).

([135]) Banisar, p. 68 similarly notes 'some ambiguity'.

([136]) Apparently a misprint, because exemptions are provided in s. 14, but the 'subject to' proviso to s. 3(1) would still apply.

([137]) Section 2(i) states '"record" means record in any form, whether printed or in writing and includes any map, diagram, photography, film, microfilm, which is used for official purpose by the public body which holds the record'.

([138]) FIO (Pakistan), s. 7.

([139]) FIO (Pakistan), s. 3(2).

([140]) FIO (Pakistan), s. 8.

([141]) 'Pakistan Senate Forms Committee to Study FOI' (freedominfo.org 20 July 2012) <http://www.freedominfo.org/2012/07/pakistan-senate-forms-committee-to-study-foi/>.

([142]) W. Naeem, 'Flawed ordinance: Access to information often denied despite law' (Express Tribune, 6 September 2012) at <http://tribune.com.pk/story/432175/flawed-ordinance-access-to-information-often-denied-despite-law/>.

([143]) Examples are 'Our Right to Know' (NGO) <http://www.ourrighttoknow.org/>.

([144]) PI Pakistan Report, section III 'Statutory protections for privacy: Freedom of Information'.

([145]) PPC (Pakistan), s. 509.

([146]) PI Pakistan Report, section III 'Statutory protections for privacy: Criminal law'.

([147]) Electronic Transaction Ordinance 2002 (Pakistan) <http://www.fia.gov.pk/ETO.pdf>.

([148]) The Prevention of Electronic Crimes Ordinance 2007 (PECO) was more detailed but lapsed in November 2009. See PI Pakistan Report, section III 'Statutory protections for privacy: Criminal law'.

([149]) ETO (Pakistan), s. 36 'Violation of privacy of information'.

([150]) ETO (Pakistan), s. 37(1) 'Damage to information system, etc.'.

([151]) ETO (Pakistan), s. 37(2) 'Damage to information system, etc.'.

([152]) ETO (Pakistan), s. 1(p) provides that '"information system" means an electronic system for creating, generating, sending, receiving, storing, reproducing, displaying, recording, or processing information'.

([153]) For the modern history of Sri Lanka, see Pike, *Empires at War*, ch. 33 and pp. 723–4. See also Malik et al., *Government and Politics in South Asia*, chs. 19–24.

([154]) Malik et al., *Government and Politics in South Asia*, p. 307.

([155]) 'Sri Lanka: Background' in *CIA World Factbook* 'Sri Lanka', 18 January 2013, at <https://www.cia.gov/library/publications/the-world-factbook/geos/ce.html>.

([156]) Malik et al., *Government and Politics in South Asia*, ch. 20 'Sri Lanka', section 'Government Structure'.

([157]) 'Sri Lanka: Government' in *CIA World Factbook* 'Sri Lanka'.

([158]) Malik et al., *Government and Politics in South Asia.*

([159]) 'Sri Lanka: Government' in *CIA World Factbook* 'Sri Lanka'.

([160]) Agence France-Presse, 'Sri Lankan law chief says family in danger after sacking' (*Sydney Morning Herald*, Australia 17 January 2013).

([161]) RPD, 'Obtaining NIC' page, at <http://www.rpd.gov.lk/>.

([162]) Information and Communications Technology (ICTA) <http://www.icta.lk/en/programmes/re-engineering-government/131-main-projects/275-enational-id-card.html>.

([163]) Staff reporter, 'Nadra wins Sri Lanka ID Card project' (*The Nation*, Pakistan, 9 November 2013) <http://www.nation.com.pk/pakistan-news-newspaper-daily-english-online/islamabad/09-Nov-2013/nadra-wins-sri-lanka-id-card-project>.

([164]) A. Marsoof, 'The Right to Privacy in the Information Era: A South Asian Perspective' (2008) 5(3) SCRIPTed.

([165]) Marsoof, 'The Right to Privacy in the Information Era'.

([166]) Marsoof, 'The Right to Privacy in the Information Era': 'Privacy issues have arisen in Sri Lankan courts in several contexts, ranging from servitudes, criminal trespass, divorce and defamation to unlawful arrest. In a case in the early-twentieth century, the court recognized a right to household privacy in upholding a custom in the Jaffna peninsula, where adjoining landowners were permitted to enter the neighbour's land to protect his fence with the covering of *ola* leaves. It is noteworthy that the Sri Lankan courts have been bold to hold that even an owner of an estate or a superintendent has no right to enter the labourer's lines and invade his privacy.'

([167]) Marsoof, 'The Right to Privacy in the Information Era'.

([168]) (Communication concerning) *Sri Lanka* [2006] UNHRC 48; CCPR/C/87/D/1331/2004 (14 September 2006) <http://www.worldlii.org/int/cases/UNHRC/2006/48.html>.

([169]) ICTA website <http://www.icta.lk/index.php/en/component/content/article/69>.

([170]) For details of ICTA-developed policies under the 'Re-engineering government' project, see Privacy International, *Sri Lanka Report*, 12 December 2006 <https://www.privacyinternational.org/reports/sri-lanka>.

([171]) Electronic Transactions Act 2006 (Sri Lanka) <http://www.icta.lk/pdf/ElectronicTransactionActNo19of2006.pdf>.

([172]) Telecommunication Act No. 27 of 1996, ss. 53 and 54 (1); see Privacy International, *Sri Lanka Report*, 12 December 2006 <https://www.privacyinternational.org/reports/sri-lanka>.

([173]) S. Ferdanindo, 'Govt. won't introduce "Right to Information Act" at the expense of national security' (*The Island*, 1 February 2013) <http://www.island.lk/index.php?page_cat=article-details&page=article-details&code_title=58012>.

([174]) See website of Transparency International Sri Lanka <http://www.tisrilanka.org/?cat=70>.

([175]) B. Deitz, 'No right to information in Sri Lanka', 7 August 2012, Committee to Protect Journalists website at <http://cpj.org/blog/2012/08/no-right-to-information-in-sri-lanka.php>.

([176]) Computer Crimes Act 2007 (Sri Lanka) <http://www.icta.lk/pdf/ComputerCrimesActNo24of2007.pdf>.

([177]) CCA (Sri Lanka), ss. 3, 4, 5, and 8 respectively.

([178]) CCA (Sri Lanka), s. 14.

([179]) CCA (Sri Lanka), s. 17.

([180]) CCA (Sri Lanka), s. 14(4).

([181]) *CIA World Factbook*, 'Maldives' (CIA, 7 January 2013) <https://www.cia.gov/library/publications/the-world-factbook/geos/mv.html>.

([182]) *CIA World Factbook*, 'Maldives'.

([183]) This paragraph is derived from the *CIA World Factbook*, 'Maldives'.

([184]) 'Maldives to hold first polls since president toppled' (channelnewsasia 6 February 2013) <http://www.channelnewsasia.com/stories/afp_asiapacific/view/1252591/1/.html>.

([185]) Ellen Barry, 'Protests Over Delay of Election in Maldives' (*New York Times*, 11 November 2013) <http://www.nytimes.com/2013/11/12/world/asia/maldives-political-turmoil.html?_r=0>.

([186]) 'Abdulla Yameen sworn in as new Maldivian president' (*Times of India*, 17 November 2013) <http://timesofindia.indiatimes.com/world/south-asia/Abdulla-Yameen-sworn-in-as-new-Maldivian-president/articleshow/25953127.cms>.

([187]) Mohamed Ibrahim and Md. Ershadul Karim, 'Research Guide on Legal System and Research of Maldives' (GlobaLex, June 2013) <http://www.nyulawglobal.org/globalex/Maldives.htm>.

([188]) Constitution of the Republic of Maldives 2008 (functional translation), at <http://www.maldivesinfo.gov.mv/home/upload/downloads/Compilation.pdf>.

([189]) Constitution (Maldives) 2008, s. 2.

([190]) Constitution (Maldives) 2008, s. 9(d).

([191]) *CIA World Factbook*, 'Maldives'.

([192]) Constitution (Maldives) 2008, s. 10.

([193]) Ibrahim and Karim, '12. The Court System'.

([194]) Iru Veli, 'Need for a Privacy Act in the Maldives', 18 June 2011, blog entry

<http://iruveli.blogspot.com/2011/06/need-for-privacy-act-in-maldives.html>.

([195]) Constitution (Maldives) 2008, s. 68.

([196]) Constitution (Maldives) 2008, s. 16(a): '[S]ubject only to such reasonable limits prescribed by a law enacted by the People's Majlis in a manner that is not contrary to this Constitution. Any such law enacted by the People's Majlis can limit the rights and freedoms to any extent only if demonstrably justified in a free and democratic society.' The onus of proof of justification of any limitation is placed on the State or the person asserting the limitation by the same section.

([197]) Constitution (Maldives) 2008, s. 19: 'A citizen is free to engage in any conduct or activity that is not expressly prohibited by Islamic Shari'ah or by law. No control or restraint may be exercised against any person unless it is expressly authorised by law.'

([198]) Constitution (Maldives) 2008, s. 21.

([199]) Constitution (Maldives) 2008, s. 24.

([200]) Constitution (Maldives) 2008, s. 67.

([201]) Constitution (Maldives) 2008, s. 47: '(a) No person shall be subject to search or seizure unless there is reasonable cause; (b) Residential property shall be inviolable, and shall not be entered without the consent of the resident, except to prevent immediate and serious harm to life or property, or under the express authorisation of an order of the Court.'

([202]) 'Everyone has the right to freedom of thought and the freedom to communicate opinions and expression in a manner that is not contrary to any tenet of Islam' (s. 27); The guarantees of freedom of the media are coupled with a privacy protection: 'No person shall be compelled to disclose the source of any information that is espoused, disseminated or published by that person' (s. 28); 'Everyone has the right to protect one's reputation and good name' (s. 33). Freedoms to acquire and impart knowledge (s. 29), freedom of association (s. 30), and freedom of assembly (s. 32) may also readily be shown to imply freedom from surveillance activities which would impinge on them.

([203]) Constitution (Maldives) 2008, ss. 236–246.

([204]) Constitution (Maldives) 2008, ss. 189–198.

([205]) Human Rights Commission of the Maldives website at <http://www.hrcm.org.mv/Homepage.aspx>.

([206]) Human Rights Commission Act 2006 (Maldives) (English Translation) <http://www.hrcm.org.mv/publications/otherdocuments/HRCMActEnglishTranslation.pdf>.

([207]) HRC (Maldives), s. 21.

([208]) HRC (Maldives), s. 22.

([209]) HRC (Maldives), s. 23.

([210]) HRC (Maldives), s. 32.

([211]) HRC (Maldives), s. 6.

([212]) Andrew Byrnes, Andrea Durbach, and Catherine Renshaw, 'Joining the Club: the Asia Pacific Forum of National Human Rights Institutions, the Paris Principles, and the Advancement of Human Rights Protection in the Region' (2008) 14(1) *Australian Journal of Human Rights*, pp. 63–98 <http://ssrn.com/abstract=1397466>.

([213]) 'Maldives Official Signals RTI Bill May Move This Year' (Freedominfo.org 25 October 2012)

<http://www.freedominfo.org/2012/10/maldives-official-signals-rti-bill-may-move-this-year/>.

([214]) Right to Information Bill (Maldives) (Unofficial Translation from the Dhivehi Original) <http://www.law-democracy.org/wp-content/uploads/2010/07/Maldives.FOI_.May10.dra_.pdf>.

([215]) RTIB (Maldives), s. 2(d).

([216]) RTIB (Maldives), s. 49(d).

([217]) See Centre for Bhutan Studies <http://www.grossnationalhappiness.com/> and Bhutan's Gross National Happiness Commission <http://www.gnhc.gov.bt/>.

([218]) Numbers are uncertain, with the 2005 census only counting Bhutanese citizens (635,000), but estimates of an additional migrant population are as high as 45 per cent of the population. See 'People & Population', Bhutan News Service <http://www.bhutannewsservice.com/people-population/>.

([219]) Constitution of the Kingdom of Bhutan 2008 <http://www.wipo.int/wipolex/en/details.jsp?id=5214>.

([220]) This paragraph, and some other parts of this section, paraphrase the *CIA World Factbook*, 'Bhutan' entry at <https://www.cia.gov/library/publications/the-world-factbook/geos/bt.html>.

([221]) National Portal of Bhutan <http://www.bhutan.gov.bt/government/index.php>.

([222]) 'In 1959, the National Assembly, under the guidance of the Third King Jigme Dorji Wangchuck enacted the first comprehensive codified law code, the Thrimzhung Chhenmo or the Supreme Law. The Thrimzhung Chhenmo covers almost all civil and criminal matters and includes sections on land law, marriage, inheritance, weights and measures, theft and murder. Although many of the chapters have been amended by subsequent legislation, the Thrimzhung Chhenmo is considered to be the basis for all the subsequent laws enacted in Bhutan': 'Introduction to the Bhutanese Legal system' on the National Portal of Bhutan website at <http://www.judiciary.gov.bt/html/judiciary/legal.php>.

([223]) 'Structure of the Royal Court of Justice' on National Portal of Bhutan <http://www.judiciary.gov.bt/html/judiciary/structure.php>.

([224]) 'The size of a standard credit card, the new plastic citizenship cards has an assortment of world-class security features compared to the old paper ID cards. The card has anti-copier micro-texts, ultra violet security module, ghost printing and engraved images as security features. The front of the card carries only basic information of an individual with two pictures of the card-holder. A 2D bar code strip runs on the back of the card which contains detailed information of the holder as reflected in the old ID cards': Kinley Dorji, 'New citizenship ID cards in Bhutan' (findBiometrics 29 August 2004) <http://findbiometrics.com/new-citizenship-id-cards-in-bhutan/>.

([225]) 'New Bhutanese National ID Card Mismatch leads to longer wait' (Bhutanese Majestic Travel 9 October 2010) <http://www.bhutanmajestictravel.com/news/2010/new-bhutanese-national-id-card-mismatch-leads-to-longer-wait.html>.

([226]) Credit Information Bureau of Bhutan <https://www.cib.bt/>.

([227]) Constitution 2008 (Bhutan), art. 7.

([228]) Constitution 2008 (Bhutan), art. 7 cl. 22.

([229]) Constitution 2008 (Bhutan), art. 7 cl. 23.

([230]) See 'Acts' on National Portal of Bhutan <http://www.bhutan.gov.bt/government/acts.php>.

([231]) Thomas Barfield, *Afghanistan: A Cultural and Political History* (Princeton University Press, 2012) pp. 344–50.

([232]) For Afghanistan's modern history, see Barfield, *Afghanistan: A Cultural and Political History*, chs. 4–6.

([233]) Much of the data concerning Afghanistan is derived from the *CIA World Factbook*, 'Afghanistan' entry, 10 January 2013 <https://www.cia.gov/library/publications/the-world-factbook/geos/af.html>.

([234]) William Dalrymple, 'How Is Hamid Karzai Still Standing?' (*New York Times*, 20 November 2013) <http://www.nytimes.com/2013/11/24/magazine/how-is-hamid-karzai-still-standing.html>.

([235]) Barfield, *Afghanistan*, pp. 344–6.

([236]) *CIA World Factbook* 'Afghanistan'.

([237]) Transparency International Corruption Perceptions Index <http://www.transparency.org/research/cpi/overview>.

([238]) Frud Bezhan, 'Controversial ID Cards Expose Ethnic Divisions in Afghanistan' (Radio Free Europe 18 December 2013) <http://www.rferl.org/content/afghanistan-id-cards-ethnic-divisions/25205181.html>.

([239]) Constitution of Afghanistan 2004 <http://www.asianlii.org/af/legis/const/2004/index.html>.

([240]) Afghanistan Independent Human Rights Commission <www.aihrc.org.af>.

([241]) *The Law on Structure, Duties and Mandate of the Afghanistan Independent Human Rights Commission*, 14 May 2005 <http://www.aihrc.org.af/home/law/360>.

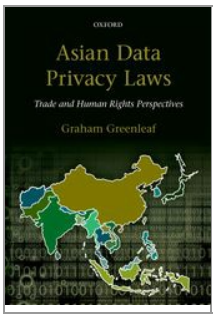
([242]) Constitution 2004, art. 58.

([243]) Byrnes, Durbach, and Renshaw, 'Joining the Club'.

([244]) Draft Access to Information Law <http://www.sartian.org/media/k2/attachments/Afghanistan-AtIDraftLaw_English-Sep11.doc.txt>.

([245]) Centre for Law and Democracy, 'Afghanistan—Comments on the Draft Access to Information Law', November 2011 <http://www.law-democracy.org/live/afghanistan-comments-on-the-draft-access-law/>.

University Press Scholarship Online
Oxford Scholarship Online



Asian Data Privacy Laws: Trade & Human Rights Perspectives
Graham Greenleaf

Print publication date: 2014
Print ISBN-13: 9780199679669
Published to Oxford Scholarship Online: December 2014
DOI: 10.1093/acprof:oso/9780199679669.001.0001

Comparing Protections and Principles—An Asian Privacy Standard?

Graham Greenleaf

DOI:10.1093/acprof:oso/9780199679669.003.0017

[–] Abstract and Keywords

This chapter compares the sources of privacy protection available in each of the 26 jurisdictions discussed in Part II. It then compares the 11 jurisdictions that have private sector data privacy laws. Across Asia, as well as specialist data privacy laws, a wide variety of other legal instruments are used for protection of privacy, and have potential for greater use, but this varies a great deal between countries. Those in active use include constitutional protections against government actions, criminal prosecutions, and civil law actions. Use of international agreements (namely, the ICCPR) has not yet occurred. The chapter then compares data privacy laws in 11 jurisdictions under these main headings: scope; data privacy principles; liabilities (controllers, processors, and others); and international dimensions. Conclusions are drawn concerning the extent to which these Asian laws are restricted to the 'minimum' principles of the 1980s, or are closer to 'European' principles.

Keywords: data protection, privacy, Asia, sources, scope, privacy principles, liabilities, data exports

1. Introduction

This chapter first compares the sources of privacy protection available in each of the 26 jurisdictions discussed in Part II. There is then a comparison, for the 11 jurisdictions that have private sector data privacy laws, of their scope, and the privacy principles included in each. From these comparisons it is then possible to conclude what is the current 'Asian standard' for principles in data privacy laws, which could be considered by other Asian countries currently without data privacy laws, or companies wanting to implement Asia-wide internal standards. In the next chapter, the enforcement methods provided by each data privacy law will be compared. In both of these chapters, references to **(p.472)** specific Acts and sections are not given, as they are already provided in Part II, and would reduce the readability of the discussion. Details concerning each country can be found in the relevant chapter in Part II, when needed, with the assistance of the Index.

2. Comparing sources of privacy protections

To obtain a full picture of the potential for privacy protection within a country, and to compare countries on this basis, it is necessary to consider the full range of sources from which data privacy developments can arise, including constitutional rights, rights arising from treaties, rights of civil action (arising from a civil code or tort law), provisions in the general criminal law, whether there is a right to information law (which provides part of a data privacy code for the public sector), as well as whether there is a data privacy law. Whether a country is a democracy, and what international organizations it is part of, are also relevant factors.

2.1. Sources of privacy protections

Table 17.1 summarizes each of these factors across all 26 Asian jurisdictions. If there is a data privacy law, its sectoral coverage, and whether there is a data protection authority, is included. The table is followed by a brief comparative discussion of the occurrence and importance of each factor across jurisdictions.

2.2. Occurrence and use of protections other than data privacy laws

Constitutional protections

Constitutional protections have two main functions in protecting privacy: most often, they enable

constitutional courts to strike down other legislation which is inconsistent with them (negative use). If they can be the basis of a right of action (positive use), they may give similar protection to Civil Code or tort actions, although often only against the state.

First, the constitution must include privacy-related rights. Only four of the 26 countries provide no such constitutional protections (Brunei, Lao People's Democratic Republic (PDR), Sri Lanka, and Singapore) although they are of uncertain scope in three others (Afghanistan, Bhutan, and Malaysia), and they cannot be used either negatively or positively in at least two other states (China and North Korea) and possibly some others (eg Vietnam). That leaves as many as 16 Asian jurisdictions where constitutional protections may be of value to protect privacy. Timor Leste has the only constitutional provision which explicitly protects data privacy and requires enactment of a data privacy law. Many of the other constitutional provisions have wording similar to the International Covenant on Civil and Political Rights 1966 (ICCPR) Article 17 and do explicitly refer to the protection of privacy, but in others (including India, Taiwan, and Japan) the protection of privacy is implied from other protections such as those for liberty or human dignity.

The function of striking down privacy-hostile legislation or government actions lacking legislative authority (negative use) has already been significant in court decisions in Hong Kong, Indonesia, India, Japan, Pakistan, the Philippines, South Korea, and Taiwan. The subject matter of the legislation struck down has included ID card schemes (the Philippines, India, Taiwan), government requirements of information disclosure (Pakistan, South Korea, Taiwan), data matching (Taiwan), telecommunications interception without sufficient legal authority (Hong Kong, Indonesia, India, Japan), excessive interference in **(p.473)**

Table 17.1 Comparison of sources of privacy protection in Asian jurisdictions

Jurisdiction	Region	Democ	Con	Civ	Cr	ICCPR	Mon	OP	Groups	HRI	RTI	ID	DP law	DPA
Afghanistan	SAsia	Semi	U	N		Ratified	No	No	SAARC	Y*	N	Y	No	N/A
Bangladesh	SAsia	Dem	Y	N	Y	Ratified	No	No	SAARC	Y	Y	Y	No	N/A
Bhutan	SAsia	Auth	U	N		N/A	No	No	SAARC	N	N	Y	No	N/A
Brunei	SEAsia	Auth	N	N		No	No	No	ASEAN	N	N	Y	No	N/A
Cambodia	SEAsia	Semi	Y	N		Ratified	M	No	ASEAN	N	N	Y	No	N/A
China	NEAsia	Auth	Y	Y*	Y*	Signed	M	No	APEC	N	Y	Y*	E-comm	Min
Hong Kong	NEAsia	Semi	Y*	N	Y	In effect	No	No	APEC	N	N	Y	Comp	DPA
India	SAsia	Dem	Y*	N	Y	Ratified	No	No	SAARC	Y*	Y	Y	PrivS	Min
Indonesia	SEAsia	Dem	Y*	N		Ratified	No	No	ASEAN; APEC	Y*	Y	Y	E-comm	Min
Japan	NEAsia	Dem	Y*	Y*		Ratified	M	No	APEC; OECD	N	Y	Y*	Comp	Min
Korea (N)	NEAsia	Auth	Y	N		No	M	No	None	N	N	Y	No	N/A
Korea (S)	NEAsia	Dem	Y*	Y*		Ratified	M	OP	APEC; OECD	Y*	Y	Y*	Comp	DPA
Lao PDR	SEAsia	Auth	N	N		Ratified	No	No	ASEAN	N	N	Y	No	N/A
Macau SAR	NEAsia	Semi	Y	Y	Y*	In effect	No	No	None	N	N	Y	Comp	DPA
Malaysia	SEAsia	Semi	U	N		No	No	No	ASEAN; APEC	Y*	N	Y	PriS	DPA
Maldives	SAsia	Dem	Y	N		Ratified	No	OP	SAARC	Y	N	Y	No	N/A
Myanmar	SEAsia	Auth	Y	N		No	No	No	ASEAN	Y	N	Y	No	N/A

Nepal	SAsia	Semi	Y	N		Ratified	M	OP	SAARC	Y*	Y	Y	PubS	DPA
Pakistan	SAsia	Semi	Y	N	Y	Ratified	No	No	SAARC	N	N	Y	No	N/A
Philippines	SEAsia	Dem	Y*	Y*		Ratified	M	OP	ASEAN; APEC	Y*	N	Y	Comp	DPA
Singapore	SEAsia	Semi	N	N		No	No	No	ASEAN; APEC	N	N	Y	PriS	DPA
Sri Lanka	SAsia	Semi	N	N	Y	Ratified	M	OP	SAARC	Y	N	Y	No	N/A
Taiwan	NEAsia	Dem	Y*	Y*	Y*	N/A	No	No	APEC	N	Y	Y*	Comp	Min
Thailand	SEAsia	Dem	Y	N		Ratified	No	No	ASEAN; APEC	Y*	Y	Y	PubS	DPA
Timor Leste	SEAsia	Dem	Y	N		Ratified	M	No	ASEAN candidate	Y*	N	Y	No	N/A
Vietnam	SEAsia	Auth	Y	Y	Y	Ratified	No	No	ASEAN; APEC	N	N	Y	E-comm	Min

Key

Democ = Whether country is a democracy (Dem/Semi/Auth). (Note: for explanation of categorizations used ('democratic', 'semi-democratic', and 'authoritarian') see Chapter 1, section 5.3.)

Con = Does it have constitutional provisions protecting privacy? (Y/No/U); * = Cases on the provision are known. (Note: U represents for 'uncertain': constitutional rights such as 'life, liberty and security of person' might or might not be interpreted to provide implied protection of privacy, but this has not yet occurred.)

Civ = Is there a tort or civil code action to protect privacy? (Y/N); * = Cases are known.

Cr = Are there offences by third parties (not data controllers) for misuse of personal data? (Y/N); * = Convictions are known.

ICCPR = Status in relation to the International Covenant on Civil and Political Rights 1966 (Ratified/Signed/No/Not applicable (N/A) because not a UN member state).

Mon = Does it take a monist approach to international obligations? (M/No).

OP = Has ratified the Optional Protocol to the ICCPR (OP/No).

Groups = Members of international bodies listed.

HRI = Does the country have a national Human Rights institution? (Y/N) * = Full member of APF-NHRI.

RTI = Is there a Right to Information law? (Y/N).

ID = Is there a national ID system? (Y/N); * = Law on privacy of ID system.

DP law = Is there a data privacy law? (Sectoral scope of Law/No).

DPA = Is there a Data Protection Authority or Ministerial enforcement? (DPA/Min/N/A if no data privacy law).

(p.474) sexual relationships (India, but overturned), and 'real name' Internet requirements (South Korea). The positive use of constitutional rights to found actions for privacy remedies is potential rather than actual as yet. It did occur once in China in a case of identity theft before the Supreme People's Court ruled that the constitution could not be used in this way.

In Asia, constitutional protections against government legislation and government actions lacking legislative authority are therefore very important privacy protections, which have been used in at least nine jurisdictions, and could possibly be used in seven others. Many of the provisions have very similar wording, and there is potential for interpretations made by a constitutional court in one Asian country on privacy issues to influence decisions in other Asian countries, but this is not yet known to have occurred.

Treaty protections

The countries that have not ratified the ICCPR—Brunei, China (signed only), Malaysia, North Korea, and Singapore—are similar to the group of countries that do not have constitutional rights of privacy or where they cannot be utilized as legal rights. Bhutan and Taiwan cannot ratify as they are not UN members. In Hong Kong and Macau, adherence to the ICCPR is required by the Basic Law of each. The other 17 jurisdictions have ratified the ICCPR. However, as Table 17.1 shows, only six of those states take a monist approach to international law, so that ratified treaties automatically become part of their domestic law (Cambodia, South Korea, Nepal, the Philippines, Sri Lanka, and Timor Leste). Court actions based on Article 17 ICCPR as a treaty-based right are not, however, known to have occurred.

The other means of enforcing Article 17's right to privacy is via a communication (complaint) to the UN's Human Rights Committee. This can only be done in the handful of Asian countries that have ratified the Optional Protocol to the ICCPR, namely South Korea, the Maldives, Nepal, the Philippines, and Sri Lanka. However, no significant communications concerning privacy have been made in relation to any of these countries (see Chapter 2, section 4.1).

Civil Code or tort actions

There are only seven Asian countries where it is clear that there is a statutory civil right to take court action to protect at least some privacy interests: China, Japan, South Korea, Macau SAR, the Philippines, Taiwan, and Vietnam. No common law countries in Asia have developed such a right, either at common law or in equity, although there have been some developments at first instance concerning a tort of harassment in both Singapore and Hong Kong. Claims that such rights exist in India are dubious. Such actions under the Civil Code are already common in Taiwan and South Korea, have occurred in Japan and Vietnam, and are starting to develop under China's Tort Law. They are possible in Macau but have not occurred. Habeas data actions have commenced in the Philippines but not proceeded.

Criminal law actions

Most countries have some provisions in their general criminal law relevant to misuse of personal information, but it is increasingly common in recent years for specific 'computer crime' and e-commerce provisions to be enacted criminalizing the wrongful provision, receipt, or sale of personal data. Such provisions are distinct from criminal law sanctions **(p.475)** for breaches of data privacy laws, which are usually (but not always) aimed at data controllers, not third parties. Provisions criminalizing trafficking in personal data have been enacted in at least Bangladesh, China, India, Macau, Pakistan, South Korea, Sri Lanka, Taiwan, and Vietnam. As yet, China makes the most active use of provisions in the general criminal law against misuse of personal data, although this also occurs in Taiwan, South Korea, and Macau, and possibly India.

Right to Information (RTI) Acts

Where a country does not have a data privacy law, a right to information (RTI) or freedom of information (FOI) law will at least provide people with a right to access their personal data held by public bodies, and sometimes a right to correct it. Such a law should also protect their personal data from being accessed by others except where this is justifiable on public interest grounds, or after redaction of their personal data. RTI/FOI laws are sometimes the first step toward development of full data privacy laws. In Asia, nine jurisdictions have RTI/FOI laws (Bangladesh, China, India, Indonesia, Japan, South Korea, Nepal, Taiwan, and Thailand). India's law is a paradigm of active enforcement, used constantly by citizens and their non-governmental organization (NGO) representatives.

Only in Japan, Taiwan, and Korea are those RTI laws now to some extent redundant to privacy protection

because data privacy laws cover the same field, but even there they may provide more convenient procedures for people to access their own records. The RTI laws of Nepal, Bangladesh and Thailand also include other elements of a data privacy law for the public sector. RTI laws should also be of continuing value when a country's data privacy law only covers the private sector. However, in the three Asian jurisdictions with the most limited data privacy laws, only India has a RTI law. Singapore and Malaysia do not.

Human rights commissions—a 'Cinderella' right

Privacy is unequivocally a human right, recognized in every human rights instrument since the Universal Declaration in 1948 through to the 2013 UN resolution. But insofar as human rights commissions are concerned, it has been something of a Cinderella, regarded as not a priority until more important human rights are addressed. There are national human rights bodies in at least 13 Asian countries, as shown in Table 17.1, nine of which are full members of the Asia-Pacific Forum of National Human Rights Institutes (see Chapter 2, section 6.5). The South Korean National Human Rights Commission has intervened in a number of data privacy issues, but no others have done so, or even show an interest in such issues on their websites.

International memberships by countries

Membership of international organizations may affect a country's privacy commitments. Bhutan and Taiwan are not members of the UN. As discussed in Chapter 2, membership of the Association of Southeast Asian Nations (ASEAN) does involve privacy commitments, but membership of the South Asian Area of Regional Cooperation (SAARC) does not. Membership of the Asia-Pacific Economic Cooperation (APEC) (by 10 Asian economies) does involve a commitment to implement the APEC Privacy Framework, but not necessarily by legislation. Only two Asian countries (Japan and South Korea) are OECD members, and they have already met their commitments to the OECD. Twenty-two of **(p.476)** the 26 Asian countries are now World Trade Organization (WTO) members[1] (all except Afghanistan, Bhutan, North Korea, and Timor Leste); however, WTO membership does not yet have significant implications for development of data privacy laws (see Chapter 2).

2.3. The surveillance context—national ID cards, systems, and legislation

Every country and jurisdiction in Asia has a national identity card and number. They are the rule, not the exception, in Asia. There is no difference between common law and civil law countries, or between democratic and authoritarian countries. The extent to which ID cards and numbers are used in the public and private sectors varies widely, but accurate information is not readily available in most jurisdictions.

However, the extent to which there are any legal protections of privacy against misuse of ID cards and numbers, whether in general data privacy laws, or in the laws establishing the ID systems, or in constitutional decisions, varies a great deal. Only in Hong Kong, Macau, and South Korea are there institutions which have actively intervened to prevent abuses of existing national ID systems, but in Japan (at first instance), the Philippines, India, and Taiwan the courts have intervened to limit their establishment or extent. In Japan and the Philippines, data protection authorities (DPAs) which will have powers to limit abuses are being established. DPAs in Malaysia and Singapore have little scope to do so.

In all jurisdictions, and particularly those that do have not have any existing independent controls, one of the main tasks of the development of data privacy laws must be to control the potential abuses of national ID systems by both the state and the private sector. The many dangers to privacy posed by national ID systems (including cards, numbers, and back-end systems) intensify where they combine a number of the following 10 factors:[2] (i) are compulsorily allocated to everyone in a jurisdiction (usually national not regional) and therefore universal; (ii) are multipurpose, either by law or *de facto*; (iii) embody the ID number in one or more convenient tokens (e.g. an ID card); (iv) the card contains a photograph (more so if it also contains any other biometric identifiers); (v) the card contains a chip (usually called a 'smart card'); (vi) the chip is capable of being read at a distance ('contactless') rather than requiring physical contact to be read; (vii) it is compulsory to carry the card at all times; (viii) the card records group classifications such as religion, race, or ethnicity; (ix) the card records individual disabilities such as criminal records;

and (x) the card or number enables numerous authorities to have immediate access to back-end systems to obtain further information.

Many analyses of ID systems are available,[3] but none cover all Asian jurisdictions or provide a compelling framework for analysis. It is beyond the scope of this book to analyse and compare the ID systems in the 26 Asian jurisdictions, beyond the brief descriptions given of systems in Part II, and the observation that in most countries there are not yet sufficient data privacy controls over such systems.

(p.477) 2.4. Conclusions about the sources of data privacy protections

Putting aside specialist data privacy laws, it is apparent that across Asia a wide variety of other legal instruments are in fact used for protection of privacy, and have potential for greater use, but that this varies a great deal between countries. Those in active use include constitutional protections against government actions, criminal prosecutions, and civil law actions. Use of international agreements (namely, the ICCPR) has not yet occurred.

The countries in Asia which have been shown to have the most effective combinations of other legal instruments with which to protect privacy (and some track record in their being used) are South Korea, Taiwan, and Macau (all with use of constitutional, criminal, and civil remedies). In China both criminal prosecutions and civil remedies are being actively used. In numerous countries constitutional protections, or one of the other forms of protection, are occasionally used. However, that leaves at least half the countries of Asia where it does not seem any of the other forms of protection of privacy are in active use, usually because they are not available in their legal systems.[4] In some of them (Singapore and Malaysia), recent data privacy laws will now fill part of the gap.

3. Comparing the scope of data privacy laws

Before considering the privacy principles or enforcement measures in a data privacy law it is necessary to consider its scope. An otherwise strong law can have most of its effectiveness removed by strategic exemptions of important sub-sectors or activities. On the other hand, the compliance requirements of data privacy laws could easily be stifling and bureaucratic in the wrong context.

3.1. Differences in sectoral scope

Of the 13 Asian jurisdictions that have significant data privacy laws, only six have comprehensive laws covering both the public and private sectors (Hong Kong, Japan, South Korea, Macau, the Philippines, and Taiwan). Three others have laws which cover most of their private sector (India, Malaysia, and Singapore), although in all cases with very significant exclusions (see section 3.2 of this chapter) and no public sector coverage. A further three (China, Vietnam, and Indonesia) have laws which only cover their e-commerce and consumer sectors, but not the entire private sector. Vietnam's IT and e-commerce laws could be applied to the public sector, but this would require clarification in regulations. Nepal and Thailand cover their public sectors only (but with a private sector Bill before the Thai legislature).

Asia is unusual in comparison with other regions with data privacy laws. Outside Asia, of the 101 countries with data privacy laws, the only other countries with 'private sector only laws' are the Dubai and Qatar special economic zones.[5] Similarly, only two countries outside Asia now have 'public sector only' data privacy laws (Zimbabwe and the USA), though this was once not so unusual outside Europe.[6] The other 92 data privacy laws **(p.478)** worldwide are comprehensive, covering both public and private sectors. Over 90 per cent of the world's data privacy laws are comprehensive: it is the situation in Asia that is aberrant.

It is therefore very significant whether India and Indonesia enact comprehensive laws covering their public sectors and reverse what could otherwise become an Asian rejection of the democratic dimension of data privacy laws represented by coverage of the public sector. Thailand is more complex: enactment of a new 'private sector only' law would not be so detrimental, if Thailand also greatly improved its extremely limited public sector law. In the longer run, a major question will be whether Singapore, Malaysia, India, and other Asian countries that have started with the development of 'private sector only' laws will

subsequently expand them to be comprehensive laws. In the past such expansions have usually been in the opposite direction, with public sector laws later including the private sector.

3.2. Differences in exemptions from scope

All data privacy laws have specific exemptions relevant to the jurisdiction, and it is not possible to compare all such exemptions here. Only major issues of scope, and unusual and significant exemptions are covered. Vietnam and China are not discussed here, as their laws are inherently limited to e-commerce and consumer matters.

There are no international data privacy agreements in Asia which impose any enforceable obligations concerning scope of data privacy laws (see Chapter 3, section 3). The OECD Guidelines and the APEC Privacy Framework say little about exemptions.[7] Where possible, the position in Asian jurisdictions is compared with the requirements of the European Union (EU) Data Protection Directive.[8]

Breadth of exceptions—complete or partial?

A significant test of the strength of a data privacy law is how comprehensive is its application. It is useful to distinguish between partial exemptions from particular principles but where the other principles continue to apply, and complete exclusions from the Act as a whole which create a 'privacy free zone'. In general, the latter are anti-privacy and poor policy. The laws in South Korea, Macau, and Hong Kong have few complete exemptions, although Hong Kong has a lot of partial exemptions. In contrast, Singapore has a complete exemption for 'publicly available' information, and for a 'public agency', which has an uncertain meaning. Malaysia's law excludes everything outside 'commercial transactions', and has a very unclear definition of what the exclusion of 'governments' means. India's Rules have so many exclusions and points of uncertain scope that they become almost irrelevant, including limiting most principles to 'sensitive' data, and most only to 'providers' of data (not data subjects).

(p.479) Forms of data included

Information must be embodied in a document before it is regulated (all jurisdictions except the Philippines), with 'document' being given a very wide definition, sometimes on the basis of capacity to reproduce the data (Hong Kong), or its inclusion in a database or otherwise being systematically organized (Japan, Malaysia). Information held only in a person's mind is therefore exempt, with the exception of the Philippines, which specifies that it refers to personal information 'whether recorded in a material form or not'. No Asian laws are restricted to data processed by automated means, except in India. Other Acts include organized manual filing systems, as in Europe.[9]

Scope of 'personal data'

All Asian data privacy laws take the approach, conventional since the minimum principles of the 1980s and adopted in European laws,[10] that what is personal data is determined by its capacity to identify a person (not actual identification). One Chinese regulation may go further and mean that 'call data' information is by itself regarded as personal data, irrespective of whether it is collected in conjunction with data with the capacity to identify. Whether the conventional definition is now sufficient for privacy protection is now very questionable, but that is not the purpose of this discussion, or pursued here.

Hong Kong imposes a restriction that the information must be collected with the intention to identify the individual (*Eastweek Case*), but this has not been applied elsewhere. India is the only exception to the conventional approach, because many of its principles only apply to 'sensitive' data (very narrowly defined). India then adds the additional restriction that half of its principles only apply to 'providers' of personal data, not to data subjects per se, making them irrelevant to data subject in many cases.

'Public information' exceptions

Data privacy laws must indicate (expressly or impliedly) whether or when personal data can become sufficiently 'public' so that some or all data protection provisions do not apply. European law does not provide any general exemption for publicly available information, but does allow specific exemptions to be made for public registries containing personal data, and relaxes the special protections for sensitive data

which have been 'manifestly made public by the data subject'.[11] The APEC principles suggest limited application to publicly available personal data.[12]

Hong Kong takes a position similar to European law in having no express exemptions at all for publicly available information, but allowing each public register to set its own conditions for use of the information in it. This is illustrated by the decision concerning the 'Do No Evil' app which amalgamated and published personal data from many Hong Kong public registers. Because there is no exemption for 'publicly available information', **(p.480)** information found in public registers can only be used for the purpose for which the register expressly or impliedly provides it. Similarly, the laws in Macau and South Korea contain no such exemption.

At the other end of the spectrum, Taiwan exempts 'collection in a public place or a public activity'. Similarly, Singapore exempts completely from its Act 'personal data that is generally available to the public'. Malaysia's limitation of scope to 'personal data in respect of commercial transactions' may well have the same effect. There are therefore two opposite positions being taken on this question. European law has no such exemption for publicly available information.

Taiwan also exempts 'audiovisual data that is not combined with any other personal data', which might exempt CCTV footage and photography/video taken in public places. This could give a somewhat similar result to Hong Kong's 'Eastweek' exemption. In contrast, Macau specifically includes all forms of video surveillance and other processing of sounds and images. There is therefore little consensus in Asian laws on this issue.

Personal affairs and non-commercial activity exemptions

The conventional exemption, found in the EU Directive,[13] for personal data held or used only for personal, household, or family affairs, is found in all Asian jurisdictions. Most jurisdictions broaden the exemptions somewhat beyond that, often to areas of non-government activity that are of importance in the jurisdictions but sensitive to regulate. Exemptions of differing scopes for the activities of clubs and voluntary associations are found in numerous laws, such as South Korea. Religious organizations are exempt in Japan, and 'missionary activities' are exempt in South Korea. Political parties are only exempt for electioneering purposes in South Korea, and generally exempt in Japan. In Hong Kong the organs of the Chinese central government have the only complete exclusion from the Act. All types of non-commercial transactions are completely exempt from Malaysia's law, so most activities of clubs, NGOs etc. will be excluded. India's law also applies only to 'corporations', although this is defined to include most business entities.

Macau specifically limits the 'personal affairs' exemption so that it does not apply to processing for 'systematic communication and dissemination'. Widely accessible publication by individuals via the Internet will probably fall outside the 'personal affairs' exemption in any event, but Macau has made this explicit.

'Small business' and 'government business' exceptions

Japan excludes some types of commercial activities, namely where a business holds personal data on no more than 5,000 persons. They are completely excluded from any obligations, except that some ministerial sectoral guidelines reimpose some duties on them. Such exemptions are completely opaque to both data subjects and other businesses dealing with the business concerned, and are poor policy. Singapore has a unique exclusion of any business if they happen to be working for the Singapore government—even though this may be unknown to the data subject. Malaysia does not go so far, only excluding processing for the purpose of regulatory functions, and then only when applying the Act would be likely to prejudice those functions.

(p.481) Application to deceased persons, and to legal persons

With few exceptions, Asian data privacy laws apply only to living persons. Application to deceased persons is a matter left to national laws by EU law.[14] Singapore's PDPA applies its restrictions on disclosures and security obligations to data concerning persons deceased for less than 10 years, but this does not apply to

information in records that have existed for at least 100 years. The Philippines also explicitly provides that the rights of the data subjects survive death or incapacity, which may be a complex question in other jurisdictions depending on how rights are characterized. In Asia, legal persons are never protected by data privacy laws, only natural persons (deceased in some cases). Although the EU Data Protection Directive only requires protection of natural persons, some European laws do in fact provide protection to legal persons.[15]

News media and other freedom of speech exceptions

In Europe the protection of freedom of expression is guaranteed both by European human rights law and by the Directive, which exempts processing 'solely for journalistic purposes or the purpose of artistic or literary expression' and only to the extent necessary to reconcile freedom of expression with privacy protection.[16] Matters are not so straightforward in Asia, where there are no enforceable treaty-based protections of freedom of expression,[17] and some jurisdictions do not have constitutional guarantees of freedom of expression. It is essential in such Asian jurisdictions, if a data privacy law exists, that the news media receive some explicit exemptions within it from data privacy laws, so as to appropriately protect the public interest in freedom of speech. Perhaps not surprisingly, the strongest media exceptions in data privacy laws are found in the Philippines, Hong Kong, Japan, and South Korea, jurisdictions which in any event provide constitutional guarantees for freedom of expression which a privacy law cannot avoid. Macau does not have an explicit media exemption, but protections of freedom of speech in the Basic Law would be likely to limit severely the capacity of the privacy law to interfere with that. The same may be said of Taiwan's Constitution. Singapore, and Malaysia have no constitutional guarantees, but do at least have some protective provisions for the media in their privacy laws.

The Philippines law provides what is probably the strongest exemption for 'journalistic, artistic, literary or research purposes', giving freedom of speech a complete priority. In Hong Kong, the media is exempt from most aspects of the Ordinance where personal data is collected and held for a news activity until after publication. A person cannot request access or correction until after a story is published. There is a significant and unusual exemption from the disclosure principle which permits the disclosure of personal data to a data user engaged in news activities where the disclosing party (for example, a whistleblower) reasonably believes this to be in the public interest. South Korea has a general exemption for personal information 'used for reporting by the press'. Malaysia has a carefully drawn partial exemption from most principles for publishing 'journalistic, literary or artistic material', but only to the extent of reasonable belief that the principle cannot be complied with. In Singapore there are exemptions allowing collection without consent for 'news organizations' (defined narrowly) solely in relation to 'news activities', but no **(p.482)** exemption from other principles. China and Vietnam have no specific exemptions for media organizations, but their laws have only limited application to such organizations.

There is no accepted formula for a reasonable 'news media exemption', and it seems that the above exemptions in varying ways try to strike a reasonable balance, though the Singaporean approach is probably too narrow. However, all data privacy laws in Asia are sensitive to free speech issues, except for those in India, Vietnam, and China, which do not address the issue.

Standard exemptions—defence, security, legal proceedings, archives, etc.

All Asian laws contain some exemptions for such matters as defence, national security, international relations, criminal investigation, legal proceedings, and legal professional privilege, and protection of an individual's mental and physical health (e.g. Hong Kong). Singapore's law has exceptionally long schedules of exemptions from specific principles, as well as more general exclusion provisions. Research and statistical uses are often exempted, at least where published results are de-identified (e.g. Hong Kong), and this is implied in ambiguous provisions in the Philippines. These exemptions are too lengthy to be catalogued and compared here. Their breadth is often one of the weak points of these laws.

Discretionary exemptions by a DPA or minister, and subordination to other Acts

Singapore allows the minister to completely exclude any class of organization or class of data. Singapore's DPA can do likewise, with ministerial approval, granting complete or partial exemptions. Singapore's Act is

also subordinate to any other Act, or any other legal requirements, to the extent of any inconsistency. In Malaysia, there is a similar ministerial capacity to exempt, on the advice of the Commission, and such exemptions may be partial or complete. Other Asian laws do not do this. Such blanket powers to create exemptions are foreign to EU law, which specifies the permissible grounds of exemption.[18]

3.3. Conclusions concerning the scope of coverage and exemptions

The legislation in Hong Kong, Macau, and South Korea has not only the broadest scope in the sectors they cover, but is also similar in having relatively few exemptions. These are usually partial exemptions from particular principles, not complete exclusions or 'privacy free zones' for particular organizations, activities, or information. The Philippines law is also very comprehensive, but with a few exemptions of uncertain scope. Not far removed in terms of comprehensiveness are the laws of Japan and Taiwan, which are of broad scope but marred by various complete exclusions. All six of these laws can reasonably be described as comprehensive of both the public and private sectors.

Singapore's combination of public sector exemptions of unknown scope, mechanisms for further exemptions, and lengthy exceptions to specific principles, give its Act potentially the narrowest scope in Asia, and the most uncertain. Malaysia's law also has extremely narrow scope due to its limitation to business transactions. India's law is just a mish-mash of different types of ambiguous exclusions despite its superficial appearance of application to most commercial activities. In terms of its scope, the Indian law is a travesty, as it will **(p.483)** very rarely apply to benefit residents of India, being essentially a law to provide some protection to overseas outsourcers (data controllers). From the data subject's perspective, the laws of Singapore, Malaysia, and India are 'second class' in Asia in terms of scope. The laws of China, Vietnam and Indonesia only claim to be sectoral.

4. Comparing data privacy principles

The comparison in this section and Tables 17.2–17.5 cover the 11 Asian jurisdictions which currently have data privacy laws regulating significant parts of their private sectors.[19] Vietnam and China are included because they have significant and detailed sectoral laws covering e-commerce and consumer protection. India is included despite the fact that the scope of its law is quite uncertain (see Chapter 15), and entries for India assume (only for purposes of comparison) that each principle in its law does apply to the whole private sector. Indonesia is omitted because its law is so brief that the content of most aspects of the table would be speculation. Nepal and Thailand, which have laws only covering their public sectors, are omitted. Detailed references to statutory provisions for each country are not included but can be found in the chapters concerning each country.

4.1. Comparison of principles in Asian data privacy laws

Tables 17.2–17.5 classify privacy principles (or alternative versions thereof) under numerous headings, indicating whether each is present (√) or absent (X), with an occasional 'unknown' (–). The binary nature of the Table (X/√) means that it can only be a 'best fit' approximation for what are often very complex provisions. Only the 11 jurisdictions which have data privacy laws covering most of their private sectors are included.

The 'Source' column of the table categorizes the principles in terms of their origins, using for convenience a four-letter code:

- 'OECD' refers to the 'minimum' principles, originally arising from the OECD Guidelines and Council of Europe (CoE) Convention in the 1980s (see Chapter 3, section 3.1);
- 'EURO' indicates the 'European' principles arising from the 1995 EU Directive and 2001 CoE Convention Additional Protocol (see Chapter 3, section 3.2).
- 'APEC' indicates the three principles unique to the APEC Privacy Framework (see Chapter 2, section 3.2).
- 'ASIA' indicates principles which do not fit into any of these categories, but are found in at least one Asian data privacy law. This use of 'ASIA' may overestimate Asian origins, and the following discussion will indicate whether this is the case, if a principle's known to have some

other origin (e.g. the USA for data breach notification).

Accompanying each table, there is a discussion of each main heading ('Collection Principles' etc.) which brings out points of comparison across the data privacy laws of these 11 jurisdictions.

Reference must be made to the chapters on each country for details. **(p.484)**

Table 17.2 Comparison of general principles and collection principles

	Source	CN	HK	IN	JN	KR	MA	MY	PH	TW	SN	VN
General principles												
'Fair and lawful processing' general requirement	EURO	√	X	X	X	√	√	√	√	√	X	X
'Personal data' defined in terms of identifiability	OECD	√	√	√	√	√	√	√	√	√	√	√
Specified contact at controller (accountable data controller)	OECD	√	√	√	√	√	√	√	√	√	√	√
'Privacy officer' required	ASIA	X	X	X	X	√	X	X	X	X	X	X
Onus of proof on controller	ASIA	X	X	X	X	X	√	X	X	X	X	X
Openness re policies on personal data	OECD	√	√	X	√	√	√	X	X	√	√	X
Published privacy policy	ASIA	√	√	√	X	√	√	√	X	√	√	√
'Preventing harm'	APEC	X	X	X	X	X	X	X	X	X	X	X
'Choice'	APEC	X	X	X	X	X	X	X	X	X	X	X
Collection principles												
Collection—'limited' (only)	OECD	X	X	X	√	X	X	√	√	X	X	√
Collection—'minimum necessary' for purpose	EURO	√	√	√	X	√	√	X	X	√	√	X
Anonymity if possible (collection)	ASIA	X	X	X	X	√	X	X	X	X	X	X
No denial of service (minimal collection)	ASIA	X	X	X	X	√	X	X	X	X	√	X
Purpose of collection 'specified' by time of collection	OECD	√	√	√	√	√	√	√	X	√	√	√
Purpose may be specified asap after collection	ASIA	X	X	X	X	X	X	X	√	X	X	X
Notice on collection from data subject (including purpose, etc.)	EURO	√	√	√	X	√	√	√	X	√	√	X
Notice on collection from third parties (including purpose, etc.)	ASIA	X	X	X	X	√	√	X	X	√	X	X
Collection only with consent	ASIA	√	X	X	X	√	X	X	√	X	X	√
Consent must be express	–	X	√	√	X	√	√	√	√	√	X	X
Unbundling and/or segregation of items requiring consent	ASIA	X	X	X	X	√	X	√	X	X	X	X
Collection by lawful means	OECD	√	√	X	√	√	√	X	√	√	√	√
Collection by fair means	OECD	√	√	X	√	√	√	X	√	√	√	√

4.2. General principles

General requirement of 'fair and lawful processing'

The European approach of a general principle requiring 'fair and lawful processing' is included in half of the Asian laws: South Korea, Macau, Malaysia, the Philippines, and **(p.485)** Taiwan. China's laws have differing

versions of a similar formula.[20] In the other jurisdictions, there is no similar general requirement concerning processing, only obligations concerning specific aspects of processing: Hong Kong, India, Japan, Singapore, and Vietnam. Such an approach is more similar to the structure of the OECD Guidelines. However, these differences between a European and OECD general 'flavour' to a law do not seem to indicate any clear division between stronger and weaker laws.

Data quality

All Asian jurisdictions except India and China include the minimum requirement of data quality, that personal data must be relevant, accurate, complete, and up to date, relative to its purpose.

Other general principles

There are a number of other general principles which can affect the operation of all other principles. All jurisdictions require data controllers to have a specified contact person who can receive complaints or enquiries.[21] This is the 'minimum' principles requirement for 'accountability'. Only South Korea goes beyond that and requires a specific 'privacy officer', with designated qualifications, tasks and rights, and even a function of providing 'remedial compensation'. South Korea is also the only country to put the onus of proof on the data controller concerning compliance with all data privacy principles, when challenged before a DPA, court, or tribunal in a civil matter. Otherwise, the onus of proof of breaches of principles (or other legislative requirements) would normally lie with the plaintiff, with the burden of proof (at least in common law countries) being on the balance of probabilities, and in criminal law matters proof being required 'beyond reasonable doubt', with corresponding differences in civil law countries.

The minimum requirement of the principle of 'openness' (as the OECD described it), is that any person should be able to find out about personal data processing practices, whether or not they are a data subject. It is the minimum principle which is least often implemented in Asian laws, being found in an explicit form in the legislation of only seven of the 11 Asian jurisdictions, but not in India, Malaysia, the Philippines, and Vietnam. However, all Asian laws except those of the Philippines and Japan require a published privacy policy, including those of India, Malaysia, and Vietnam. The Philippines' 'fair and lawful processing' principle also requires 'adherence to the principles of transparency'. So all Asian jurisdictions require openness in personal data processing to some extent.

APEC's 'Choice' and 'Preventing harm' principles are, fortunately, not found anywhere. See Chapter 2, section 3.2 for why they are not desirable as principles.

4.3. Collection principles, and notice

All 11 Asian jurisdictions under consideration impose some collection limitations based on the purpose of collection, but the majority go further and allow only minimal or necessary collection.

(p.486) Minimal collection, anonymous transactions, and service denial

The majority of jurisdictions in Asia (China, Hong Kong, India, South Korea, Macau, Taiwan, and Singapore) implement the stricter European approach of 'minimal' collection, that personal data should only be collected where it is necessary for a (legitimate) specified purpose,[22] rather than the weaker minimum principles (OECD and APEC) limitation that collection should be 'not excessive'. Japan, Malaysia, the Philippines, and Vietnam (only by implication) adopt the less strict 'not excessive' approach. Only South Korea takes the next step in data minimization, requiring that, wherever possible, transactions should be anonymous.[23] It also requires the business to prove that it only collected the minimum necessary information.

South Korea also has a very unusual explicit 'no denial of service' principle, that goods and services cannot be refused because a person refuses to provide more than the minimum necessary information. Singapore is similar in its provision prohibiting organizations, as a condition of providing a product or service, from requiring an individual to consent to the collection, use, or disclosure of their personal data beyond what is reasonable to provide the product or service. These provisions give strong support to minimal collection requirements, and are not yet found in the European principles. At best, such

restrictions are only implied in other laws.

Purpose of collection and notice required

The minimum principles only require that the purposes must be 'specified' by the time of collection but are ambiguous about what notice to the data subject is required. The European principles require that notice of such purposes must be given to the data subject,[24] as do the APEC principles. All Asian jurisdictions require that the purpose of collection be specified by the time of collection from the data subject, but in the Philippines it may be specified as soon as possible thereafter (as allowed by the minimum principles).

All jurisdictions except the Philippines and Japan require notice of such purpose, and other matters, to be given to the data subject by the time of collection of personal data from the data subject. In Japan the requirement of individual notice can be avoided if the purpose of collection is obvious.

The content of the notice that must be given to data subjects is specified in greatly differing detail between laws, and is best seen by reference to the country chapters in Part II. At the very specific end are China's Guidelines (but not its laws). For example, Macau requires data subjects to be informed (unless they already have the information) of the purposes of processing, the recipients of the data, the consequences of not providing the information, and rights of access and correction. Hong Kong requires much the same.

When personal data is collected from third parties, there is a requirement to provide notice to the data subject in three laws only (South Korea, Macau, and Taiwan). This is not **(p.487)** required in the minimum principles. Macau requires the notice to be given when the data is recorded, or not later than when it is used or disclosed. No law explicitly requires notice to be given when data is collected by observation or from documentary sources, but where laws require consent of the data subject as a condition for processing to be legal, this may have the same effect. Japan's law implies that public notice is sufficient in such cases. Malaysia seems to only require such notice where the data user proposes to change the purpose of use to one different from the original purpose of collection.

Consent to collection, and definitions of consent

Half of the Asian laws explicitly require consent for collection from the data subject, and other forms of processing. Others do not, even though they usually require notice. Notice requirements to data subjects may often mean that there is implied consent to the purpose of collection. South Korea, Taiwan, Macau, and Malaysia do explicitly require consent before collection, with few and relatively narrow exceptions. The Philippines' law, while ostensibly requiring consent, has so many exceptions that consent is just one of many methods by which processing may be legitimate. China and Vietnam require consent (in the consumer and e-commerce contexts).

Macau requires 'unambiguous consent'. Taiwan requires written consent. The Philippines requires that consent be a 'freely given, specific, informed indication of will' and that it be 'evidenced by written, electronic or recorded means', which leaves open the possibility of an express 'opt-out' but not implied consents. Hong Kong often requires 'prescribed consent', which must be express, and can be withdrawn. The South Korean law concerning consent is unusually strict in that it requires not only writing but (i) separate consents for each item requiring consent (i.e. 'unbundling' of consents); and (ii) segregation on consent forms of those items that require consent and those that do not ('unbundling' non-consents). Malaysia also requires unbundling of consents. This lack of consistency, even though express consent is most commonly required, is likely to cause difficulty for companies attempting to do business across multiple Asian jurisdictions, and it might be easier to adopt a standard approach of explicit unbundled consents.

Lawful, fair, and non-intrusive collection

Laws in almost all Asian jurisdictions follow the minimum requirements that collection must be by lawful means, and by fair means (which is a substantive limitation going beyond other existing laws), with only India and Malaysia omitting these minimum requirements. China only includes them explicitly in its Guidelines, but some of its laws refer to general principles of fairness and good faith. In Hong Kong, 'fair'

has been interpreted by a tribunal to include 'non-intrusive' means in a case concerning paparazzi. It is not clear to what extent the fair processing requirements in other jurisdictions place similar restrictions on media intrusions, or will consider other forms of intrusive collection to be 'unfair'.

Visual surveillance

Special provision limiting visual surveillance are found in the data privacy laws of South Korea and Macau, but in other jurisdictions they may only be found in other laws. **(p.488)**

Table 17.3 Comparison of processing, use, disclosure, and security principles

	Source	CN	HK	IN	JN	KR	MA	MY	PH	TW	SN	VN
Fair processing principles												
'Fair and lawful processing' basis	EURO	√	X	X	X	√	√	√	√	√	X	X
Data quality principles	OECD	X	√	X	√	√	√	√	√	√	√	√
Use and disclosure principles												
Uses limited to purpose of collection, consent or law	OECD	X	√	√	√	√	√	√	√	√	√	√
Disclosure limited to collection purpose, consent, or law	OECD	X	√	√	√	√	√	√	√	√	√	√
Secondary uses/disclosures allowed if 'compatible'	OECD	X	√	√	√	√	√	X	√	√	√	√
Secondary purpose 'specified' at change of use (or stricter)	OECD	X	X	√	√	√	√	√	√	X	√	X
New disclosures/uses allowed after notice	ASIA	X	X	X	√	X	X	√	X	X	X	√
Security principles												
Security safeguards—'reasonable steps'	OECD	√	√	√	√	√	√	√	√	√	√	√
Data breach notification to DPA	USA	√	X	X	√	√	X	X	√	X	X	√
DB notification to data subject	USA	X	X	X	X	√	X	X	√	√	X	X

4.4. Use and disclosure principles

'Finality' principles—use and disclosure limited by original purpose of collection

All of the Asian data privacy laws include to some extent the principle of 'finality', that the original purpose of collection of personal data is the starting point in determining what uses may be made of the data, including disclosures of it. This is achieved in different ways, primarily either by specifying what constitutes 'fair and lawful processing', or by principles stating what uses and disclosures are allowed. In either case, the main issue becomes what exceptions to 'finality' based on purpose of collection are allowed. These are usually described as 'secondary' uses or disclosures.

Secondary uses/disclosures based on 'compatibility', etc.

Both the minimum and European principles allow additional uses/disclosures that are 'not incompatible' with the purpose of collection. In the EU, this very general criterion for secondary uses has been interpreted differently between member states, but is usually accompanied by requirements that data subjects be informed very specifically of the purpose of collection, thus limiting what can be regarded as 'compatible'.[25] In Asia quite **(p.489)** a range of wordings are used to indicate allowed secondary uses, including (from potentially least restrictive to potentially most restrictive) the wordings of 'not incompatible' (Macau), 'compatible' (the Philippines), 'reasonably expected' (Singapore), 'duly related' (Japan), 'directly related' (Hong Kong, Malaysia), 'in conformity with' (Taiwan), 'within the scope' (South Korea), for the 'purpose and scope announced' (Vietnam), and 'for the purpose for which it has been collected' (but with limited application) (India). China's more recent laws use a variety of wordings. The differences (if any) between the meanings of these terms is speculative in the absence of decisions

interpreting them, but it seems likely that a considerable range of differences will emerge.

South Korea only allows uses and disclosures 'within the scope' of the purpose of collection, so this may mean that there is no allowance for merely 'compatible' uses, but that other exceptions must be relied upon, including consent. This may be the most restrictive requirement in Asia. In the Philippines, mere 'compatibility' does not seem sufficient unless the use/disclosure is also for 'legitimate interests' or within another exception.

At the other end of the spectrum, in Malaysia, secondary disclosures are allowed where 'directly related' (and for other reasons), but secondary uses do not have to be 'directly related'. Singapore's Act does allow secondary use on the basis of purposes that a reasonable person would consider appropriate, but secondary uses will more often be based on 'deemed consent', lengthy schedules of exceptions, and other legislation. Consent and notice play the role of residual provisions where none of these other broad exceptions are available. These may be the least restrictive provisions in Asia, but are too complex for this to be clear. China's various provisions are as yet inconsistent between themselves.

The exceptions to the finality aspects of use and disclosure vary so considerably that reference is best made to each country chapter in Part II for details. Macau and the Philippines have exceptions based on the EU exception for protection of the legitimate interests of others, but only if they are not overridden by interests in protecting the fundamental rights of the data subject.[26] In Macau there are complaint resolutions based on this.

Exceptions based merely on notice

The minimum principles require that every change of purpose must be 'specified'. South Korea has detailed notice requirements when consent is sought for change of purpose. The minimum principles do not state that giving notice is sufficient in itself (as an exception to the finality requirement) to be the basis of a change of purpose. However, Japan allows new disclosures (unrelated to the purpose of collection) after notice is given on a website, with an opt-out allowed, but this does not apply to new secondary uses by the original data user. It is therefore questionable whether Japan's law complies with the minimum principles. Malaysia has exceptions for disclosure which depend on notice, but also require the disclosures being 'directly related' to the purpose of collection.

Exceptions based on consent

Consent is always an allowed ground for change of use or for new types of disclosure of personal data, but the conditions for valid consent vary. The South Korean requirements **(p.490)** for such consent are strict and require disclosure of identity of recipients, and of the consequences of refusing consent (see also section 4.3 of this chapter).

4.5. Data security and data breach notification principles

Security

All jurisdictions require security safeguards, which must usually be against 'loss or unauthorised access, destruction, use, modification or disclosure' (minimum requirements), and only state the requirements in such abbreviated form. The standard of care required is sometimes phrased as requiring 'appropriate' measures, which is the European terminology[27] (Macau and Taiwan), or to take 'reasonable' steps, which is the OECD terminology. Some jurisdictions have an arguably stronger formulation such as 'necessary and proper steps' (Japan), 'whatever is necessary' to secure data (South Korea), or other formulations such as 'practical steps' (Malaysia). Detailed security requirements may also be specified (e.g. South Korea, Malaysia, and Macau), and are likely to be more important than the words used to specify a standard. The Philippines has special security provisions for government agencies holding sensitive data, and requirements that contractors holding such data must register with the DPA.

Data breach notification

Issuing of compulsory data breach notifications by companies can be a considerable sanction because of their potential effects on a company's reputation and financial situation. Various jurisdictions in the USA

have had data breach notification requirements for some years. They exist in the laws of some European jurisdictions, and are compulsory under EU law for telecommunications providers.[28] They are now required under the revised 2013 OECD Guidelines (see Chapter 19, section 3.1). In Asia, data breach notification is required by four laws, and they occur in practice in two other jurisdictions. They can best be seen as part of the security principle, although they can also be viewed as an enforcement mechanism. In South Korea, the Philippines, and Taiwan, individuals likely to be affected must be notified of data breaches. In China, the Philippines, and South Korea (when affecting more than 10,000 data subjects) the DPA or relevant ministry must be notified. In Hong Kong, government agencies have reached agreement with the privacy commissioner to notify him immediately of such breaches, but this does not apply to the private sector, despite the recent revisions to the Hong Kong law. In Japan, ministerial guidelines require notification to the relevant ministry, the basis of a quasi-voluntary data breach notification system. It is possible that compulsory notification may become part of the government's proposed reforms. The lack of any such provisions in the comparatively recent Singaporean and Malaysian laws now makes them appear to be lagging behind recent developments. Its omission from Macau's law reflects the state of EU law a decade ago. There are no data breach notification provisions in India's legislation. **(p.491)**

Table 17.4 Comparisons of user rights and 'special concern' principles

	Source	CN	HK	IN	JN	KR	MA	MY	PH	TW	SN	VN
User rights												
Access to individual data	OECD	X	√	√	√	√	√	√	√	√	√	√
Correction of individual data	OECD	X	√	√	√	√	√	√	√	√	√	√
Access to disclosures to third parties	ASIA	X	√	X	X	√	X	X	√	√	√	X
Right to copy of structured e-data	ASIA	X	X	X	X	X	X	X	√	X	X	X
Corrections advised to third parties	ASIA	X	√	X	X	X	√	X	√	√	√	X
Deletion/anonymization after use completed	EURO	X	√	√	X	√	√	√	√	√	√	X
Deletion of data on request	ASIA	X	X	X	X	√	X	X	X	X	X	X
Block use of data on request	ASIA	X	X	X	X	√	√	√	X	√	X	X
Transmissibility of rights to heirs	ASIA	X	X	X	X	X	X	X	√	X	X	X
User rights on sale of businesses	ASIA	X	X	X	X	√	X	X	X	X	X	X
Data and processing of special concern												
'Sensitive data'	EURO	X	X	X	X	√	√	√	√	√	X	X
Automated decisions	EURO	X	X	X	X	X	√	X	√	X	X	X
Marketing—'opt-out' required	EURO	√	√	X	X	√	√	√	X	√	X	√
Marketing—'opt-in' required	ASIA	√	√	X	X	√	X	X	X	X	X	X
Prior checking of some systems	EURO	X	√	X	X	√	√	√	X	X	X	X
Data matching	ASIA	X	√	X	X	X	√	X	X	X	X	X
Public registers	ASIA	X	√	X	X	X	X	X	X	X	X	X
ID numbers, etc.	ASIA	X	√	X	X	√	X	X	√	X	X	X
Visual surveillance	ASIA	X	X	X	X	√	√	X	X	X	X	X

Key

Jurisdictions: CN = China; HK = Hong Kong SAR; IN = India; JN = Japan; KR = South Korea; MA = Macau SAR; MY = Malaysia; PH = the Philippines; TW = Taiwan; SN = Singapore; VN = Vietnam.

4.6. User rights

The minimum principles of user access and correction rights are found in all Asian jurisdictions except China. All of China's data privacy laws primarily address the obligations of the administrator of personal information, and do not clearly state the rights of data subjects, although the 2013 Guidelines, for the first time, clearly assume and imply rights of access and correction. Taiwan has an unusual and strong provision that user rights 'may not be waived in advance nor limited by special agreement'.

Access, and data portability

South Korea exemplifies the broadest access rights, requiring access not only to the content held, but also the purpose of collection and use, the retention period, details of disclosures to third parties, and details of consents by the data subject. At least Singapore, Hong Kong, **(p.492)** the Philippines, and Taiwan also require disclosures to third parties to be included in replies to access requests (requiring specific request in Singapore).

The Philippines' novel contribution to Asian data privacy laws is a person's right to obtain a copy of their file in a commonly used machine-readable form, anticipating proposals for reform of the EU Directive. Exceptions to rights of access and correction vary a great deal, best seen in the country chapters in Part II. Macau requires the DPA to be informed of some types of refusal.

Corrections and notifications

Half of the Asian laws do require notification of corrections to third parties who have had access to a person's file: Hong Kong, Singapore, Macau, Taiwan, and the Philippines. Macau extends this to blocking and erasure, and requires third parties to do likewise. In South Korea, correction (and deletion) requests must be decided within 10 days, and if denied the reasons (including information about how to appeal) must be provided in a standard outcome notice, but it leaves it up to the data subject to inform third parties.

Where a correction is refused, the data subject is explicitly entitled to add their own version of the situation to their file, in Hong Kong, Malaysia, and Taiwan, although there is variation in what may be added. Other laws may allow this by implication of the data quality principle. This does not seem to occur in Japan.

Deletion and blocking of use—automatic and on request

Automatic (i.e. not requiring request) deletion or anonymization of data, once the reason for its collection is completed, is not required by the minimum principles, but is required by European principles. It is required in all Asian jurisdictions except Japan, Vietnam, and China. The Philippines provisions have many exceptions and are ill-drafted. In Singapore the provision for deletion of data is easily circumvented. India's provision is defective in only applying to sensitive information and only prohibiting retention of information beyond when it may lawfully be used, which is not the same as when its purpose of collection has expired. There is often ambiguity, as in Taiwan, about whether data must be deleted, or can be anonymized.

Deletion of data on request, including data provided by third parties, is provided in South Korea. This is close to a 'right to be forgotten' in its implementation. In Japan there is a vague provision allowing data subjects to request deletion, but it is not clear when the data controller can refuse to do so. A right to block the use of data is found in South Korea, Macau, Malaysia, the Philippines, and Taiwan. India allows consent to use information to be withdrawn, which implies that use is blocked, but not deletion. Hong Kong allows 'prescribed consent' to collect data to be withdrawn, implying a right to block use of data originating from the data subject. There are no such provisions in China or Vietnam.

South Korea is unusual in having a specific provision that data subjects must be informed of the transfer of their personal information as the result of sale of a business in whole or part, and that they have a right to opt-out (withdraw consent) from their personal information being transferred.

Similarly, the Philippines is unusual in providing that the heirs and assigns of a data subject may exercise

their rights both when they are incapacitated (some other laws have equivalent provisions) but also after their death. This seems to apply to rights that the deceased had when alive, which is different from the Singaporean provision which **(p.493)** continues to apply some data privacy rights to persons after they are deceased, exercisable by their estate.

4.7. Data and processing of special concern

Particular categories of personal data, of processing, or of information systems, raise concerns that have resulted in additional principles to deal with them.

Principles concerning direct marketing

In the EU, the right to object to personal data being used for direct marketing is supposed to be able to be exercised before data is transferred to third parties,[29] not only as the data subject's response to a direct marketing communication. The European-influenced principle of a right to opt-out from direct marketing is found in Macau, South Korea, Malaysia, Taiwan, and Vietnam. Hong Kong (after the 2012 amendments) and South Korea now go further: if consent to collect data is being obtained for any marketing purposes, the data subject must be told this, and their consent to that use obtained. Therefore, 'opt-in' is in fact required. Both of China's highest level laws may require similarly. India has a weak form of opt-out through withdrawal of consent, and Japan a different but equally weak opt-out through notices on websites. Seven Asian laws therefore take an approach at least as strong as that of the EU. Overall, this is one of the strongest implementations of a 'European' principle across Asian jurisdictions. Only Singapore and the Philippines do not require either opt-out or opt-in procedures (no matter how weak), so in those countries the only limit is whether a particular form of marketing is allowed as a secondary use of the personal data.

'Sensitive data' principles

The European-influenced principles of additional protection for a broad range of categories of sensitive personal data are found in half of the Asian laws, namely South Korea, Macau, Malaysia, the Philippines, and Taiwan. The definitions of 'sensitive data' vary considerably across jurisdictions, everywhere. Although the EU Directive has specified categories[30] of sensitive data, EU 'Member States differ substantially in their definitions of sensitive data, and in the permissible grounds for processing them'.[31] South Korea largely follows the EU approach, but also includes 'DNA information obtained from genetic examination'. Macau is similar, following the EU categories and adding 'genetic data'. The Philippines adds to the EU categories marital status, age, 'education' and genetic information, and (in effect) legally privileged information. Taiwan, while including genetics, otherwise only includes a subset of the EU categories: medical treatment and health examinations, sexual life, and criminal records.

Malaysia also includes only a subset of the EU categories; physical or mental health or condition; political or religious or similar beliefs; and allegations of commission of offences (but arguable not convictions). Racial or ethnic origin, trade union membership, and sex **(p.494)** life are not included, despite these being sensitive topics in Malaysian life. However, the minister may determine by order that any other personal data may be turned into sensitive data. Sensitive data must also be 'personal data',[32] and since 'personal data' is limited to 'information in respect of commercial transactions', this also restricts the scope of protection of 'sensitive' data.

In each jurisdiction, the exceptions for use of sensitive information are also different. In South Korea, separate 'unbundled' consent is required for uses of sensitive data. Singapore, Hong Kong, India, Vietnam, and China do not have special protections for sensitive data. India has the strange approach that standard privacy protections apply to 'sensitive' data, but fewer of them apply to all personal data, so this is not a 'sensitive data' protection. There are no special protections in any Asian data privacy laws for protection of children's personal data, an area in which US law is arguably more strict than European laws,[33] but where Asian laws do not yet provide any special protections.

Businesses dealing with personal information across a range of Asian jurisdictions are likely to find these differences in the meaning, and administration, of sensitive personal information difficult and potentially

dangerous.

Aside from these general data protection laws, most jurisdictions are likely to have specific laws dealing with particular categories of sensitive information, particularly financial and credit information, and medical information. Japan has various separate laws dealing with such data, and a number of ministry guidelines. Hong Kong also has specific laws dealing with such matters as old criminal records, and Singapore has a number of laws dealing with 'sensitive' categories. Such sectoral laws are not covered here.

Automated processing and other 'sensitive processing' principles

The right to object to automated individual decisions, which implies that final decisions on significant matters should be subject to human oversight, is required by the EU Directive, and said to be implied by the CoE Convention.[34] These European-influenced principles of controls on automated decision-making are found in Macau (fully, plus requiring disclosure of the logic of automated processes) and the Philippines (only requiring disclosure of the logic of automated processes), but not in any other Asian jurisdictions. With the increasing technical sophistication decision-making in Asian economies, it will be surprising if there is not more call for introduction of such a principle in future.

Regulation of ID systems

Although every Asian country has ID cards or numbers, specific regulation by general data privacy laws of the use of ID numbers is only found in Hong Kong, South Korea, and the Philippines. Their use is not specifically exempt from the laws in the other jurisdictions,[35] and so will to some extent be regulated, but only within the sectoral limits of each jurisdiction's legislation (e.g. not in Singapore or Malaysia's public sectors). Laws establishing ID systems in some countries also provide significant limitations on their use (e.g. China, Hong Kong). Japan has such a new law to deal specifically with its ID number.

(p.495) Visual surveillance

Special provision on some aspects of the use of visual surveillance devices are found only in the data privacy laws of South Korea and Macau, but it is likely that in most other jurisdictions some uses of such devices are regulated. The extent to which their use is regulated in public areas is likely to vary considerably between jurisdictions, depending, for example, on the extent to which 'publicly available information' or news media are regulated (see section 3.2 of this chapter), and on whether the collection principles include provisions on fair and non-intrusive collection (see section 4.3 of this chapter).

5. Comparing liabilities—controllers, processors, and others

One of the most difficult issues is to determine which parties—controllers, processor, or others—have legal liability to data subjects when there is a breach of a data privacy law. The question of against whom a data subject can make a complaint or take court action is crucial to their rights, particularly if one possible party is outside the jurisdiction or insolvent, and the other is not. It is also important whether company officers or government employees have personal liability for corporate breaches, particularly for deterrent purposes. Table 17.5 summarizes the position, each item of which is then discussed, but it is only a summary guide to what is almost always a complex situation.

5.1. Controllers and processors

The distinction between controller and processor is fundamental to determining issues of liability under European law,[36] and many Asian jurisdictions have adopted a similar distinction, if not the terminology.

Liability of processors as well as controllers

In Europe, legal obligations are supposed by the Directive to apply only to data controllers, but nevertheless some jurisdictions impose them on processors as well.[37] Similarly, in

Table 17.5 Comparison of liabilities—data controllers, data processors, and others

	CN	HK	IN	JN	KR	MA	MY	PH	TW	SN	VN
Liability of processors											

Processor liable for breaches	√	X	√	X	√	√	X	√	√	X	X
Controller's statutory liability for processors											
Due diligence re processors	√	X	X	√	√	X	√	√	√	X	X
Vicarious liability for processors	X	√	X	X	√	√	X	X	√	√	√
No liability for processors at all	X	X	√	√	X	X	√	√	X	X	X
Contractual liability to data subjects											
Third party benefit contracts	–	X	X	√	√	√	√	√	√	√	–

Key

Jurisdictions: CN = China; HK = Hong Kong SAR; IN = India; JN = Japan; KR = South Korea; MA = Macau SAR; MY = Malaysia; PH = the Philippines; TW = Taiwan; SN = Singapore; VN = Vietnam.

(p.496) Hong Kong, Malaysia, and Singapore, obligations are imposed almost exclusively on data controllers. Hong Kong only imposes obligations on processors in relation to the requirement to delete data when its purpose has expired, and Singapore only in relation to security. However, in Singapore it is clear that if the processor goes outside the processing instructions, the position is reversed and the processor becomes liable and not the controller.

In contrast, in South Korea, Taiwan, Macau, and the Philippines, processors are required to comply with all the requirements of the law, giving data subjects more options against whom they may take actions. Taiwan's law implies that processors are liable to comply with all aspects of it, and that is consistent with the fact that it imposes specific obligations on processors. Enforcement of some aspects against processors is questionable in Macau. China's definitions of who is liable for compliance are probably broad enough to encompass processors. In Vietnam, whether controller or processor has liability for actions carried out by the processor depends on the contract between them, but in the absence of any provisions the controller has vicarious liability. It seems certain that processors will be liable in India, but to whom and for what are more difficult questions. In Japan, whether a processor is liable depends on whether, in a particular situation, it is using personal data for 'its business'.

Where processors are located overseas, the question is more complex because the legislation will only in a minority of instances have extraterritorial effect and thus impose liability on them (see section 6 of this chapter). Also, where a processor is located within the jurisdiction, but carrying out processing for a foreign controller, there is often in effect an 'outsourcing exemption' so that the processor is not liable and, perhaps, nor is the controller (see section 6 of this chapter).

Controller's liability for acts of processors

South Korea, Taiwan, Singapore, Malaysia, and Macau make data controllers vicariously liable for breaches of the law by the processor. There is always a further question of whether a controller is only liable for the actions of a processer who is acting within the course of the processing instructions, or whether the controller will be liable for all actions in breach by a processor even when they are unauthorized. That is usually left ambiguous in the legislation, but might be resolved by the law of agency in the country concerned. Singapore and Malaysia adopt this more limited approach to vicarious liability, and Macau seems to. Macau provides that persons who suffer damage as a result of breaches of the data privacy law are entitled to compensation (indemnity) paid by the controller, unless it proves it is not responsible for the damage.

Due diligence in the choice of a processor, and care in the supervision of the processor is often explicitly required (South Korea, Taiwan, the Philippines, and Japan), otherwise this is in itself a breach of the law. China's laws are ambiguous as to whether there is some vicarious liability, or only a due diligence requirement. In Singapore the requirement of due diligence is not express, but implied by the implied liability consequences for processors.

India and Japan impose no explicit vicarious liability on controllers for breaches by processors, and India imposes no due diligence requirements. However, in both Japan and India the law of agency may impose vicarious liability on local companies that have engaged processors.

(p.497) 5.2. Liabilities of other parties

In addition to data controllers or processors, other parties may sometimes have personal liabilities, either in regards to fines or prosecutions, or to data subjects.

Vicarious liability for employees

In Singapore, any act done or conduct engaged in by an employee in the course of his or her employment will be treated as done or engaged in by the employer as well, whether or not it was with the employer's knowledge or approval. It is a defence to criminal liability for the employer to prove that it took such steps as were practicable to prevent the employee from doing the act or engaging in the misconduct. South Korea is also imposing complex obligations.

Personal liability of company officials

Singapore imposes personal liability on company officers for offences that involve the consent, connivance, or neglect of a company officer. Similar provisions apply to partnerships, unincorporated associations, and limited liability partnerships. In South Korea, company officials may face up to five years in prison for failure to protect customer data, and prosecutions have occurred.

Disclosure of outsourced processing or sale of businesses

South Korea is the only jurisdiction that does require disclosure to a data subject that processing has been outsourced, whether locally or overseas. There, data subjects must also be notified of sales of businesses, and can opt-out from transfer of their data.

6. Comparing the international dimensions of data privacy laws

The issues surrounding the transfer of personal data between countries, and the overseas operation of data privacy laws, are very contentious, and have generated a substantial literature.[38] There are four issues requiring consideration in any situation where a local data controller exports personal data to another jurisdiction (see Chapter 3, section 3.3), and can be collectively regarded as providing 'protection outside the jurisdiction'. Each is discussed here. There is also the question of an 'outsourcing exemption', which concerns personal data imports, not exports. Table 17.6 provides a comparison of the international dimensions of data privacy laws in Asian jurisdictions.

6.1. Protection outside the jurisdiction

The extraterritorial operation of data privacy laws, limits on data exports, and third party benefit contracts between controllers and overseas processors, are sources of possible protection for data subjects.
(p.498)

Table 17.6 Comparison of international dimensions of data privacy laws

	INTL	CN	HK	IN	JN	KR	MA	MY	PH	TW	SN	VN
Extraterritorial application												
Has extraterritorial scope	–	X	X	√	X	X	√	√	√	√	√	X
Applies to nationals overseas	ASIA	X	X	X	X	X	X	√	√	√	X	X
Applies to local equipment use	EURO	X	X	√	X	X	√	X	√	X	X	X
Data export limitations												
Depends on law of receiving countries ('adequacy')	EURO	X	X	√	X	√	√	√	X	√	X	X
Contractual protections required	ASIA	X	X	X	X	X	X	X	X	X	√	X
DPA/Min discretion to limit	ASIA	X	X	X	X	X	X	X	X	√	X	√

'Due diligence' required	APEC	X	X	X	X	X	X	X	X	X	X	X
No restrictions	OECD	√	√	X	√	X	X	X	√	X	X	√
Other international transfer rules												
Imported data exception ('outsourcing exemption')	ASIA	X	√	X	X	X	X	√	√	X	√	X
Privity of contract (no third party benefit contracts)	–	–	√	√	X	X	X	√	√	X	X	X
Controller's vicarious liability for foreign processors	–	X	√	X	X	X	X	X	X	√	√	X

Key

Jurisdictions: CN = China; HK = Hong Kong SAR; IN = India; JN = Japan; KR = South Korea; MA = Macau SAR; MY = Malaysia; PH = the Philippines; TW = Taiwan; SN = Singapore; VN = Vietnam.

Extraterritorial operation

Does the law of the controller's jurisdiction assert extraterritorial operation? The extent to which the laws of EU member states are required by the EU Directive to have extraterritorial operation is disputed.[39] However, there is obviously some element of extraterritoriality in the requirement of the Directive's Article 4(1)(c) that those laws apply to processing by a controller located outside the EU who 'for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of said Member State'. The question of what is an 'establishment' within an EU state is also a possible source of (in effect) extraterritorial operation of EU laws.

In Asia, explicit assertions of extraterritorial application are unusual in data privacy laws. In Taiwan, Malaysia, and the Philippines there are extraterritorial provisions which aim to benefit only their own nationals, but in different ways in each case. In Hong Kong, the question is not settled. Japan's public sector law applies to some offences committed overseas, but that is all. India's law asserts extraterritorial operation provided computers in India are used, and that this applies irrespective of from where outside India a person controlled the computer.

(p.499) However, it is a more difficult question whether there are implied assertions of extraterritorial application. Macau's law does not explicitly assert that it operates where a foreign controller uses equipment located in Macau, equivalent to the Directive's Article 4(1)(c), but that is its probable operation. It may also apply wherever a controller domiciled or based in Macau carries out processing outside Macau. The Philippines' law also applies where equipment in the Philippines is used. Singapore's approach only claims jurisdiction over activities that take place in Singapore, but this still has an extraterritorial effect because those activities in Singapore may be the results of data processing activities that primarily occur outside Singapore. This only leaves South Korea, China, and Vietnam where there seems to be no extraterritorial scope (and perhaps Hong Kong and Japan) so perhaps Svantesson is correct that such claims are 'relatively common' in the Asia-Pacific.[40] As he points out, there is nothing unusual about this as a matter of international law, as it has been recognized that, in relation to extraterritorial operation of statutes:[41]

> Far from laying down a general prohibition [international law leaves states] with a wide measure of discretion which is only limited in certain cases by prohibitive rules; as regards other cases, every State remains free to adopt the principle which it regards as best and most suitable.

Restrictions on transfers (data exports)

Under what conditions are transfers to a foreign jurisdiction allowed, whether to contracted data processors, or to third parties? Macau and Malaysia have limitations based on the law of the destination jurisdiction, as would Hong Kong if its data export provisions were to be brought into force. These restrictions are subject to exceptions similar to those in Article 26 of the EU Data Protection Directive.

Macau's DPA assesses numerous applications for authorization of overseas transfers, and has fined companies for failing to obtain such authorizations. Taiwan's restrictions can only be imposed at the discretion of relevant Ministries, but one of the grounds of restriction is the state of the law in the receiving county. India's export restrictions are largely incomprehensible: they may depend on the law of the jurisdiction of import, or perhaps only the standards adhered to by the importing company; the 'same level' standard that has to be met is uncertain; and they only apply to a limited class of personal data. South Korea's requirements of express consent are the strictest in the region. No Asian jurisdictions require that the data subject be made aware of the county of destination of exports (which reduces the value of South Korea's consent requirement), nor the state of data privacy law there, nor the identity of the party to which data is to be transferred.

Singapore's data export provisions require contractual protection of data subjects (not data subject consent), and Singapore does not have the restriction of privity of contract, so this can at least work in theory. However, it has not yet made regulations. The Philippines also has an 'accountability' requirement, that requires that the exporter must use 'contractual or other reasonable means to provide a comparable level of protection', but whether this means that the controller still has legal liability for any breaches of this protection by a processor, or by the third party, remains uncertain but unlikely. The doctrine of privity of contract in Philippines law also means that any contractual protections will not be enforceable by the data subject. The protective value of the Philippines provisions is therefore very uncertain.

(p.500) Four jurisdictions, Hong Kong, Japan, Vietnam, and the Philippines, have no effective limitations, and China's restrictions are based only on Guidelines as yet. Overall, the Asian jurisdictions with data privacy laws have a fairly low level of restrictions on personal data exports. Those without data privacy laws have none.

Export contracts and privity (third party benefit contracts)

Can the data subject enforce a contract against the recipient of exported data? In most Asian jurisdictions data subjects can (in theory) enforce contracts made between a local data controller and a foreign processor which are expressed to be for the benefit of data subjects, such as are required (for example) in Standard Contract Clauses for data exports from EU countries (see Chapter 2, section 3.2). However, no Asian jurisdiction explicitly requires that such export contracts be made for the benefit of data subjects, although it would be difficult to comply with Macau's law without making an export contract that benefits data subjects. Nor do they require that data subjects be informed where their data is being exported. Enforcing such a contract is also likely to be prohibitively expensive. So protections based on controller-processor contracts are largely fictional, from the data subject's perspective. Although Singapore has contract-based export provisions, and no doctrine of privity of contract, it does not require third party benefit contracts and in reality the prospects of enforcement by data subjects (the individuals who suffer harm) are very slight.

Some common law jurisdictions, including India, Malaysia, Hong Kong, and the Philippines also have a doctrine of privity of contract which prevents third parties (data subjects) for whose benefit contracts are made from enforcing those contracts. Any form of 'standard contractual clauses' are therefore useless as a form of protection providing rights to data subjects, in relation to exports from those jurisdictions. Singapore has reformed the doctrine of privity of contract to allow such enforcement, and Hong Kong is currently considering law reform proposals to introduce recognition of a third party benefit exception.

Data processor ('intermediary') rules including vicarious liability for processors

Are there special rules for controller-to-processor transfers, and do they make the controller vicariously liable for breaches by a foreign processor? Many jurisdictions make a controller/processor distinction, and have particular rules concerning processors, including South Korea, India, Taiwan, and Japan, and Singapore's differentiation of 'intermediaries'. Some jurisdictions in Asia (Taiwan, Singapore, and Hong Kong) impose a limited vicarious liability on (local) controllers for acts by a (foreign) processor which are within the scope of the processing contract, but nevertheless in breach of the law. Singapore's legislation is ambiguous, and may give no protection in relation to outsourced processing outside Singapore, or

alternatively (but less likely), may impose a form of vicarious liability on Singaporean data controllers for overseas processing by intermediaries, at least where it is within the terms of the processing contract. South Korea and Macau are the only two Asian jurisdictions that appear to impose liability on the (local) controller when a (foreign) processor acts outside its instructions.

In India, Malaysia, and Japan no explicit statutory liability is imposed upon a controller for acts of a processor located outside the jurisdiction, but it is possible that some liability may arise from the law of agency or its equivalent. In Hong Kong, a processor on behalf of others was not a 'data user' and not subject to any obligations under its law, until the 2012 **(p.501)** amendments made processors liable under statute for deletion of personal data (in addition to contractual obligations).

Overall position of protection outside the jurisdiction

To summarize the position under the above four questions across Asia is difficult. There are many differences between the requirements for personal data exports from different jurisdictions, which creates complexity for companies wishing to operate multinational businesses. Only in South Korea and Macau can the overall requirements be described as somewhat strict on business involved in data exports, and protective of data subjects. Almost everywhere else data subjects are generally in a very weak position. The laws in Hong Kong, Japan, Taiwan, the Philippines, China, and Vietnam place no restrictions on the export of personal data based on the lack of protection in the jurisdiction of the recipient, or any other significant restriction in its place. Singapore's provisions are not yet completed. Some of these laws compensate by including provisions on extraterritoriality or through limited vicarious liability for acts of processors, but these are not an adequate substitute for either consent based on full disclosure or full liability for such breaches as may occur.

6.2. 'Outsourcing exemptions'

There is a fifth question when a locally based processor imports personal data into a jurisdiction for processing, from a foreign data controller: Does the local law (in the processor's jurisdiction) exempt such outsourced processing (in full or part), so that there is a lower level of data protection required for processing of foreign-sourced personal data than for processing of local personal data? It seems that there is such an 'outsourcing exemption' in Singapore, Malaysia, the Philippines, and Hong Kong, although the exemptions arise in different ways. However, the Philippines law, through poor drafting, may often not be effective. The position in China and Vietnam is that their laws would be unlikely to apply to such imported personal data because of the restricted scope of the laws to e-commerce and consumer transactions. Such 'outsourcing exemptions' may be effective in relation to attracting outsourced processing from the USA and some other countries (though the poor drafting in countries such as the Philippines make this uncertain), but it seems very likely that they would prevent any 'adequacy' finding by the EU.

There is no 'outsourcing exemption' in South Korea, Macau, or Taiwan, where importing processors must observe the same rules as local data controllers. However, in Macau the penalties for non-compliance are uncertain, and may in effect be an 'outsourcing exemption'. India is a special case: many aspects of its law do seem to apply to personal data imported for processing from overseas, and might not apply to processing of local Indian personal data. It is possible but unlikely that this type of arrangement (the opposite of an 'outsourcing exemption') might meet the EU 'adequacy' requirements for data exports, because they appear to provide adequate protection to the personal data of Europeans imported from Europe. The European Commission and other EU authorities have not yet decided that this is 'adequate'. When personal data is imported into EU countries, it does not seem that any such exemption applies.[42] **(p.502)**

7. Strength and consistency of data privacy principles across Asian laws

From the preceding discussion in sections 4 and 5 of this chapter, it is possible to draw some conclusions about the extent to which the laws in the 11 Asian jurisdictions under consideration implement the 'minimum' principles shared by all international instruments from the 1980s, the extent to which they implement the stronger 'European' principles, and the extent to which they include additional innovative ('post-Directive') principles.

7.1. Implementation of the minimum principles

Eight minimum principles were identified in Chapter 3, section 3.1. The extent to which they have been implemented in the 11 Asian laws (to at least the extent required by the minimum principles, or stronger) is as follows: collection limitation (11/11); data quality (9/11); purpose specification (10); use limitation (9); security safeguards (11/11); openness (10); individual participation (10); and accountability (11/11) (to give them their OECD names). On average, each principle is implemented in slightly more than 10/11 jurisdictions. Asian experience therefore bears out the argument that these principles are the universally accepted basis of data privacy laws.

By jurisdiction, the weaknesses detracting from full implementation of the minimum principles in Asia come from: China (data quality; use and disclosure limitations; individual participation); India (data quality); the Philippines (purpose specification; openness); Japan (new disclosures merely by notice); Malaysia (secondary uses inconsistency). As yet, China's laws still omit or are ambiguous on too many of the minimum principles to be properly regarded as a data privacy law, particularly clarity in use and disclosure limits, and unambiguous access and correction rights (see Chapter 3, section 1.1). India's laws are far worse than only one omission which is recorded here, because so many other principles are of ambiguous scope (see Chapter 15).

7.2. Additional principles with wide acceptance in Asia

Eight 'European' principles were identified in Chapter 3, section 3.2. The extent to which they have been implemented (or more strongly implemented) in the 11 Asian laws is as follows: data export restrictions based on destination (5/11); minimal collection (7/11); 'fair and lawful processing' (5/11); deletion (8/11); sensitive data protections (5); automated processing controls (2/11); prior checking (4/11); and direct marketing opt-out, or opt-in (8/11). On average, each of these eight principles is implemented in more than five of the 11 jurisdictions, and on average each jurisdiction implements almost four principles. Clearly, special controls on automated decision-making (2/11) is the least implemented European principle in Asia. This is remarkable, given the absence of any treaty obligations.

In contrast, the three 'APEC principles' identified in Chapter 2, section 3.3 have had little implementation. Two of the APEC principles, 'preventing harm' and 'choice', have not been implemented in any data privacy law in Asia. A version of the third, which could be called 'data export accountability', is arguably implemented in Singapore, but it is a strong version which could also be seen as going considerably beyond APEC's 'due diligence' approach and be better regarded as *sui generis* (with implementing regulations still to come).

It seems, therefore, that at their present state of development, most Asian jurisdictions that have implemented data privacy laws have done so in a manner which—on average—could be described as 'halfway' between the minimum principles and the European principles. The principles of minimum collection, deletion on expiry of use, and direct **(p.503)** marketing restrictions (opt-out or opt-in) have become normal aspects of Asian data privacy laws, implemented in a majority of these laws. Destination-based export restrictions, 'fair and lawful processing' and sensitive data restrictions are also each very close to being in the 'majority' category. Other principles could also be considered as 'European' principles adopted in Asian, most notably a requirement to give notice of purpose etc., to data subjects before collection, adopted in 8/11 jurisdictions.

7.3. Additional and innovative 'Asian' principles

Asian data privacy laws have not merely adopted these two sets of pre-existing data privacy principles, to a greater or lesser extent. Individual Asian countries have continued to add to the principles, but as yet these novel principles that have not received wide adoption in other countries. The following principles, or implementations of principles, are not required by either the minimum or European sets of data privacy principles, but are found in at least one Asian law: privacy officer required (South Korea); onus of proof on controller (South Korea); anonymity in transactions where possible (South Korea); no denial of service (South Korea, Singapore); 'unbundling' of consents (South Korea); segregation of consent and non-

consent items (South Korea); marketing requiring opt-in (Hong Kong, South Korea); data breach notifications to DPA (China, Japan, South Korea, the Philippines, Vietnam); data breach notifications to data subjects (Taiwan, the Philippines, South Korea); right to copy of structured e-data (Malaysia); deletion of data on request (South Korea); user rights on sale of businesses (South Korea); and data privacy rights transmissible to heirs (the Philippines). It is obvious from this list that South Korea's law is the main location for innovations in Asian data privacy principles, but also that some innovations are found in most other jurisdictions. There is every reason to expect that Asian data privacy laws will increase as a source of innovation, as more jurisdictions adopt such laws, and 'second generation' laws strengthen existing laws.

7.4. A legislative standard for other Asian countries, and for corporations

Half the countries in Asia do not yet have any extensive data privacy laws, and a number have laws covering only parts of their private sectors, and with incomplete standards (China, India, Vietnam, and Indonesia). If any of those 17 countries wished to enact legislation which is based on what has already been enacted in existing data privacy laws in Asian countries, what principles would they include? Similarly, what standards could companies operating in Asian countries which do not yet have data privacy laws decide to implement in their binding corporate rules (BCRs) or common contract clauses (CCCs)?

The approach suggested here is that if any of the 16 'minimum' or 'European' principles (see Chapter 3, section 3), or some aspect of their implementation, is included in at least seven of the 11 Asian jurisdictions with significant data privacy laws, then a 'best fit' approach to developing a model law or corporate standard should include it. Such an approach does not give a 'lowest common denominator' approach (all laws must adopt it or it is excluded), or an overly idealistic approach including all elements that could be argued to be desirable (such as some of the innovative South Korean requirements). Nor is it based on what future international standards might be. It is a realistic approach, based on what the leading Asian jurisdictions are already enacting.

Based on the comparative analysis in this chapter, the following 11 principles (and aspects of implementation) would be a 'best fit', in that they have been adopted in at least seven of the 11 jurisdictions considered. Where there is some refinement of a principle that **(p.504)** has been adopted in at least four jurisdictions, it is put in parentheses as '+ Requiring consideration':

(i) *Purposes specified*—A specific purpose of collection should be specified prior to collection of any personal data; stated in a publicly available privacy policy prior to collection; and clearly communicated to the data subject by notice (express or implied) no later than the time of collection.
(ii) *Minimal collection*—Collection should be limited to only the 'minimal' or necessary personal information for the specified purpose.
(iii) *Fair and lawful collection*[43]—Collection should be only by means that are lawful and fair (+ Requiring consideration: to be only by non-intrusive means of collection).
(iv) *Uses and disclosures limitation*—Uses and disclosures should be limited to the purpose of collection, plus any purposes directly related to that purpose; with any such changes of purpose specified and communicated to the data subject; and any exceptions limited to the minimum necessary in the public interest.
(v) *Data quality*—Personal data should be relevant to the specified purposes, and as necessary for those purposes, accurate, complete, and kept up to date.
(vi) *Security safeguards*—Personal data should be protected by appropriate security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data; (+ Requiring consideration: the circumstances when data breaches must be notified, and to whom).
(vii) *Deletion*—Personal data should be destroyed or anonymized after the purposes for which it is held are completed.
(viii) *Direct marketing*—A readily available facility should be provided to allow opt-out of direct marketing uses of personal data, or there should be an opt-in requirement.
(ix) *Openness*—There should be a general policy of openness to any person about developments,

practices, and policies with respect to personal data systems; including means by which any person can readily establish the existence and nature of personal data, its main purposes of use, and the identity and contact information of the data controller.
(x) *Individual participation*—An individual should be able to (a) obtain confirmation whether a data controller holds personal data about him or her; (b) access that data; (c) obtain correction of contested data by having it erased, rectified, completed, or amended as appropriate; (d) obtain reasons for any refusal of confirmation, access, or correction; and (e) challenge any such refusals;[44] (+ Requiring consideration: corrections should be notified to third parties who have had access to a person's file).
(xi) *Accountability*—A data controller should be accountable for complying with measures which give effect to the principles stated in (i)–(x).

(p.505) Such a set of principles is not as high a standard as is found in the EU Directive, but is higher that the minimum principles found in the OECD Guidelines or APEC Framework. It does not contain many of the strong and innovative forms of implementation already found in Asian laws (see section 7.3 of this chapter).

There are good reasons for legislation and corporate standards in Asia to exceed this moderate 'best fit' set of standards. If a country wants to obtain an 'adequacy' finding from the European Union, then there are three additional principles that need to be considered, although it is not clear that any one of them is strictly necessary for an 'adequate' assessment to be obtained. Each of these principles is already implemented in five Asian jurisdictions, almost half of the existing laws.

(xii) *'Fair and lawful processing'*—Personal data should be processed fairly and lawfully. (This general principle does not only apply to collection, as in (iii) above.)
(xiii) *Sensitive data protections*—Categories of sensitive data should be specified and given additional protections.
(xiv) *Data export restrictions based on destination*—There should be restriction on exports of personal data to countries which do not have a sufficient standard of privacy protection (defined in Europe as 'adequate'), so as to ensure that the personal data does have sufficient protection, and the data subject can ensure that protection is observed.

The two remaining of the 16 principles are currently infrequently implemented in Asian data privacy laws, but may become more common as Asian economies increase the sophistication of their decision-making and the scope (and potential dangers) of their information systems.

(xv) *Automated processing controls*—Data controllers should ensure that automated decision-making which significantly affects data subjects is subject to human checking; and data subjects should be able to know the logic of such automated data processing.
(xvi) *Prior checking*—Personal data systems which raise potentially high levels of risk should be identified and examined before they operate.

Data privacy principles and standards continue to evolve, and the revisions of the international standards first established in the 1980s and 1990s is occurring at present (see Chapter 19). Also, the trajectory of Asian data privacy laws in recent years, particularly in the amendments to existing laws, is towards stronger principles. Innovations in Asian countries and elsewhere are also developing new standards. But at present the principles (i)–(xi) set out above can reasonably be described as the 'best fit' standard that has been adopted by data privacy laws in Asia, one which is halfway between the minimum standards of the 1980s and the later European standards. It is a standard which is already being exceeded in some Asian jurisdictions.

Notes:
([1]) 'Members and Observers' (WTO, 2 March 2013) <http://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm>.

([2]) For a draft analysis, see Graham Greenleaf, 'National ID systems in Asia: Surveying a "growth area"' (unpublished, 1st HKU/UNSW Law Faculty Research Symposium, 2 December 2010) <http://www2.austlii.edu.au/~graham/publications/2010/Asian_ID_article1210.doc>.

([3]) See Colin Bennett and David Lyon (Eds.), *Playing the Identity Card* (Routledge, 2008), and Identity-Cards.Net <http://www.identity-cards.net>.

([4]) Afghanistan, Bangladesh, Bhutan, Brunei, Cambodia, North Korea, Lao PDR, the Maldives, Myanmar, Nepal, Pakistan, Singapore, Sri Lanka, Thailand, and Timor Leste may fall into this category.

([5]) Graham Greenleaf, 'Scheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories', *Journal of Law & Information Science* (forthcoming 2014); including 'Global Tables of Data Privacy Laws and Bills (3rd Ed, June 2013)' <http://ssrn.com/abstract=2280877>.

([6]) In the Asia-Pacific, the development of data privacy laws started with 'public sector only' laws in Australia, Canada, South Korea, and Japan in the 1980s, and it took another decade or more before these laws became comprehensive.

([7]) The OECD Guidelines allow exclusion of data which does not 'pose any risk to privacy or individual liberties', and says exceptions should be as few as possible and made known to the public (arts. 3 and 4). The only specific exclusion from the APEC Privacy Framework is uses for personal, family and household affairs, plus a suggestion that publicly available information may be excluded (art. 11). The only limit it suggests on local exceptions are that they should be (a) proportional to their objectives, and '(b)(i) made known to the public; or, (b)(ii) in accordance with law'. This last use of 'or' appears to be a drafting error and should say 'and' (art. 13).

([8]) References are given to Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (2nd Edn., Oxford University Press, 2007), in which references to the specific provisions in the Directive, selected European laws, and court decisions, may be found. References are also given to European Union Agency for Fundamental Rights (FRA) *Handbook on European Data Protection Law* (FRA, 2013).

([9]) Kuner, *European Data Protection Law*, p. 99.

([10]) Kuner, *European Data Protection Law*, pp. 91–8.

([11]) Kuner, *European Data Protection Law*, p. 93.

([12]) The APEC Privacy Framework gives 'publicly available information' a broad definition, including the flexible category of information 'that the individual knowingly makes or permits to be made available to the public' (art. 11). However, 'publicly available information' is not excluded from the definition of 'personal information', and such information is only excluded from the requirement that individuals be given notice of its collection by third parties collecting it, or choice of whether it is collected. They do not give the collector of publicly available information any right, per se, to disclose the information to others.

([13]) EU Directive, Art. 3(2).

([14]) Kuner, *European Data Protection Law*, p. 79.

([15]) Kuner, *European Data Protection Law*, pp. 77–8.

([16]) Kuner, *European Data Protection Law*, pp. 84–7.

([17]) The extreme limitations in enforcing Art. 19 of the International Covention on Civil and Political Rights in Asia are the same as for Art. 17, and discussed in Chapter 2, section 4.1.

([18]) EU Directive, Art. 13.

([19]) Jurisdictions: CN = China; HK = Hong Kong SAR; IN = India; JN = Japan; KR = South Korea; MA = Macau SAR; MY = Malaysia; PH = the Philippines; TW = Taiwan; SN = Singapore; VN = Vietnam.

([20]) One law refers to 'the principles of equality, free will, fairness and good faith', and another requires companies to 'follow the legal, legitimate and necessary principles'.

([21]) This can be seen as based on both the 'openness' and 'accountability' minimum principles.

([22]) Kuner, *European Data Protection Law*, pp. 73–4.

([23]) The 'anonymity principle' is rare in data privacy laws, having originated in German legislation, and also found in Australia's private sector law since 2001, but now weakened by 2012 reforms. See Kuner, *European Data Protection Law*, p. 74 concerning the German law.

([24]) Kuner says 'the data controller must specifically inform the data subject of the purposes for which data are being collected': Kuner, *European Data Protection Law*, p. 100.

([25]) Kuner, *European Data Protection Law*, pp. 99–100.

([26]) FRA, *Handbook on European Data Protection Law*, pp. 84–90; see EU Directive, Art. 7(f).

([27]) FRA, *Handbook on European Data Protection Law*, pp. 95–6.

([28]) FRA, *Handbook on European Data Protection Law*, pp. 96–7.

([29]) FRA, *Handbook on European Data Protection Law*, p. 119; see Art. 14(b) of the EU Directive.

([30]) EU Directive, Art. 8 protects 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life'; see Kuner, *European Data Protection Law*, pp. 101–3.

([31]) Kuner, *European Data Protection Law*, pp. 103–6 provides many examples.

([32]) PDPA (Malaysia), s. 4, definition 'sensitive personal data'.

([33]) For an outline, see Simon Chesterman, 'From Privacy to Data Protection' (Simon Chesterman (Ed.), *Data Protection Law in Singapore* (Academy Publishing, 2013), pp. 28–30.

([34]) FRA, *Handbook on European Data Protection Law*, p. 117.

([35]) Subject to India, Malaysia, Singapore, China, and Vietnam regulating the private sector only.

([36]) FRA, *Handbook on European Data Protection Law*, pp. 49–55.

([37]) Kuner, *European Data Protection Law*, pp. 128–9.

([38]) For leading examples, see Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press, 2013) and Dan Svantesson, *Extraterritoriality in Data Privacy Law* (Ex Tuto Publishing, 2013).

([39]) For a discussion of different positions, see Svantesson, *Extraterritoriality in Data Privacy Law*, ch. 7. See also Kuner *Transborder Data Flows and Data Privacy Law*, ch. 6.

([40]) Svantesson, *Extraterritoriality in Data Privacy Law*, p. 121.

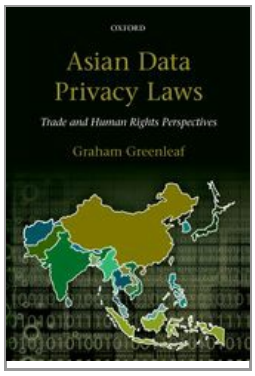
([41]) Svantesson, *Extraterritoriality in Data Privacy Law*, p. 121, citing the *Lotus case* PCIJ Ser A, No 10

(1927) 19.

([42]) Kuner *European Data Protection Law*, p. 173.

([43]) There are two collection principles, because the first derives from the European standards, the second is part of the minimum standards.

([44]) The OECD Guidelines 13 states this principle in full as follows: 'An individual should have the right: (a) to obtain from the a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; and (iv) in a form that is readily intelligible to him; (c) to be given reasons if a request made under sub-paragraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.'



Asian Data Privacy Laws: Trade & Human Rights Perspectives
Graham Greenleaf

Print publication date: 2014
Print ISBN-13: 9780199679669
Published to Oxford Scholarship Online: December 2014
DOI: 10.1093/acprof:oso/9780199679669.001.0001

Assessing Data Privacy Enforcement in Asia—Alternatives and Evidence

Graham Greenleaf

DOI:10.1093/acprof:oso/9780199679669.003.0018

[–] Abstract and Keywords

This chapter compares the enforcement measures of the 11 Asian jurisdictions with data privacy laws, the scope and principles of which were compared in the previous chapter. Comparison commences with the question of what type or types of enforcement agencies are used (data protection authority, or ministry-based), and their independence. Methods of reactive enforcement are then compared, including investigation types and types of enforcement measures (compliance orders, administrative fines, criminal prosecutions, compensation, etc). Systemic methods of enforcement are then compared. Transparency, the evidence of enforcement, is compared. Finally, the extent to which Asian data privacy laws meet the goals of 'responsive regulation' is discussed.

Keywords: data protection, privacy, Asia, enforcement, transparency, responsive regulation

1. Comparing enforcement measures in Asian jurisdictions

Chapter 3, section 3, sets out the complexities involved in determining standards for evaluating enforcement methods in data privacy laws. It is suggested there, drawing on theories of 'responsive regulation' and European criteria, that that best results are likely to be obtained by a data privacy law that has (i) a diverse range of enforcement mechanisms, at least some of which are capable of being applied to provide sanctions varying from mild to very severe; (ii) both reactive and systemic enforcement measures; (iii) measures supporting compliance in addition to those dealing with breaches; (iv) transparency in how sanctions are applied in practice; and (v) the ability of individuals to seek enforcement through the courts. This chapter compares the enforcement measures of the Asian jurisdictions with data privacy laws, the scope and principles of which were compared in the previous chapter. As in the previous chapter, section references are omitted here, in order to make comparisons readable. Full details are in each country chapter in Part II. All fines, etc., are also given in US dollars, to make comparisons easier.

(p.508) A 2013 study of data protection remedies in the 28 European Union (EU) member states by the EU Agency for Fundamental Rights (FRA)[1] found that, even with the 'harmonizing' effect of the EU Data Protection Directive on these countries' laws, 'sanctions that DPAs are empowered to impose differ between Member States', and that complainants had strong preferences for some remedial measures over others. This study is a useful touchstone throughout this chapter for comparisons with the equivalent position across Asia. Kuner had noted in 2007 that, although there was considerable enforcement of EU data protection law, 'the imposition of penalties is often not particularly visible', with fines and other penalties often not being a matter of public record in various EU member states.[2] Since then, penalties appear to have become more frequent, larger, and more visible in the EU, but systematic evidence of this (like the FRA report) is still limited.

2. Choice of privacy enforcement agency

Comparison of enforcement measures must commence with the question of what type or types of enforcement agencies are used, and their independence.

2.1. Data protection authorities or ministry-based enforcement?

The *de facto* global standard in data privacy laws covering the whole private sector was shown in Chapter 3, section 4.4, to be a dedicated data protection authority (DPA). The advantages of a specialized DPA were noted. The majority of Asian jurisdictions have such specialized DPAs: Hong Kong, Macau, Singapore, Malaysia, the Philippines (not yet appointed), and South Korea (with complexities noted below). But Asia also has the only notable global exceptions, with ministry-based enforcement in place in Taiwan and Japan, and to some extent in India's non-functioning system. It also exists in the sector-based (e-commerce and/or consumer sector) laws in China, Vietnam, and Indonesia, but this is also found in other countries outside Asia (e.g. Turkey).

Japan, South Korea, and Taiwan previously shared for a decade or so what could have been called the 'Northeast Asian civil law model' of a data privacy law enforced at the sectoral level by various ministries responsible for each industry sector, but with no coordinating data protection authority. The Macau SAR, a civil law jurisdiction, did not adhere to that model, and had a separate DPA, influenced by both Portugal and Hong Kong (another Northeast Asian jurisdiction but with a common law system). However, South Korea's new law in 2011 added a DPA (two if you count its specialized mediation body as well) while retaining a high degree of ministry-based enforcement and one central coordinating ministry. It can be said to have a mixed DPA/ministry enforcement model. Japan has now enacted a law with a DPA for its new ID system, with further reforms announced, apparently intended to establish a DPA with responsibilities for all uses of personal data, but probably retaining a strong element of ministry-based enforcement as well. China is as yet relying on ministry-based enforcement for its various laws, and there are no signs of change to that. The position in Northeast Asia is therefore still fluid, but only Taiwan and China are adhering to a strict ministry-based system with no central DPA.

(p.509) In the Association of Southeast Asian Nations (ASEAN) countries, there is acceptance of the DPA model where sector-wide laws have been enacted (Singapore, Malaysia, the Philippines), and in the Thai Bill. The two jurisdictions with only e-commerce laws (Vietnam and Indonesia) have no DPA, and are unlikely to introduce one until they at least enact laws covering the whole private sector or both sectors. It seems likely that the DPA model will become the norm in ASEAN. In India all versions of the proposals for reform of India's laws include a national DPA, and that is likely to be the eventual result, particularly given the difficulties that India's current laws have in obtaining acceptance from the European Union as 'adequate'. Nepal has a public sector DPA.

This will leave Taiwan as the only adherent to strict ministry-based enforcement, of countries with full data privacy laws. It remains to be seen whether China, Vietnam, Indonesia, and other Asian countries will follow the dominant model of a DPA. It is not a comfortable fit for the legal systems of China or Vietnam.

2.2. Independence of data privacy authorities (DPAs)

International standards for the independence of DPAs were set out in Chapter 3, section 4.4. Twelve attributes contributing to independence were identified, as in Table 18.1, with attributes 1–5 being most commonly mentioned in the international sources used, attributes 6–11 less frequently mentioned, and attribute 12 (appointment by the legislature) not mentioned despite its clear relevance. Examination of Asian legislation shows that two further attributes of independence (13th and 14th) are relevant and should be added: fixed remuneration, as this reduces the capacity of the Executive to influence the Commissioner; and a prohibition on holding subsequent appointments, to avoid a Commissioner being on a 'good behaviour bond' in the hope of an attractive next appointment by either government or the private sector.

This table shows the distribution of those attributes in the six Asian jurisdictions which do currently have DPAs, and the 2011 government-developed Bill in India. Not enough

Table 18.1 Table of 'independence attributes' of Asian DPAs

	Jurisdictions*	HK	MA	MY	KR	PH	SG	IN	TTL
	Factors								
1	Established by legislation	√	X	√	√	√	√	√	6
2	Independence required by legislation	√	X	X	√	√	X	√	4
3	Fixed term of office	√	X	X	√	√	X	√	4
4	Defined removal from office	√	X	X	√	√	X	√	4
5	Report to legislature and/or public	√	√	X	√	√	X	√	5
6	Immunity against suits	√	X	√	X	√	√	X	4
7	Adequate resources guaranteed	√	X	X	X	X	X	X	1
8	Positive qualifications specified	X	X	X	√	√	X	√	3
9	Prohibition on concurrent positions	√	X	X	√	√	X	√	4

10	Prohibition/disclosure of conflicts	√	X	X	√	X	X	√	3
11	Subject to right of appeal	√	√	X	√	X	√	√	5
12	Appointment by Parliament	X	X	X	√	X	X	X	1
13	Remuneration fixed	X	X	X	√	√	X	√	3
14	Prohibition on subsequent positions	X	X	X	X	X	X	√	1
	Total attributes	**10**	**2**	**2**	**11**	**9**	**2**	**11**	**48**

(*) Jurisdictions: CN = China; HK = Hong Kong SAR; IN = India; JN = Japan; KR = South Korea; MA = Macau SAR; MY = Malaysia; PH = the Philippines; TW = Taiwan; SN = Singapore; VN = Vietnam.

(p.510) details of the Bill currently before the Thai Parliament are available for this comparison. Not all these factors are of even weight, and therefore the totals presented in the table, while informative, can be misleading. The absence of attribute 2 (independence guaranteed by legislation) is not in itself fatal to independence, but if there are explicit legislative requirements that the DPA must follow the instructions of a Minister, as there are in Malaysia but not elsewhere, then this must weigh very heavily against any assessment of independence.

From the right column of the table, it can be seen six of the attributes of independence are most frequently found (ie 4/7 instances or more) in the Asian data privacy laws with DPAs.[3] In order of frequency, they are: legislative basis (6); right of appeal against DPA decisions (5); ability to report directly to the public, and/or legislature (annual report at least) (5); independence guaranteed by legislation (ability to investigate free of direction, etc.) (4); appointment of Commissioners for a fixed term (4); and immunity against personal lawsuits arising from a Commissioner's conduct of office (4); removal only for specified inadequate conduct, usually only by the legislature (4); and forbidden to hold other concurrent positions (4). The remaining six attributes of independence are less commonly found (i.e. three instances or less) in these DPAs: positive attributes required for appointment (3); remuneration fixed (3); prohibition on Commissioners with conflicting interests, or requirement to disclose (2); appointment by the legislature rather than the executive (1); resources determined independently of the executive (1); and prohibition on subsequent positions (1).

The table indicates that the DPAs of Hong Kong and South Korea (and the DPA in the Indian draft Bill) appear to have the most independence, followed by the as yet unappointed Philippines DPA. In contrast, the DPAs of Macau, Singapore, and Malaysia seem to have the least. However, despite its lack of formal independence, the Macau DPA has demonstrated considerable independence from government, and this may also occur with the Singaporean and Malaysian DPAs, which are not yet in full operation. Part of the explanation for this is that Singapore's and Malaysia's DPAs are unusual among the 85 DPAs which have been so far been created worldwide[4] because they are the only two that have jurisdiction over the private sector but not the public sector.[5] These two are not a 'watchdog on government', unlike other DPAs. The strong and obvious need for

DPAs which have as part of their function the prevention of abuses by a government to be independent of that same government, do not therefore apply with the same strength in Singapore and Malaysia (see Chapter 3, section 4.4).

3. Reactive enforcement—complaints, investigation, and remedies

Reactive sanctions, in response to particular situations where it appears that privacy principles are being, or have been, breached in particular situations, are the principle means of enforcement of data privacy laws in Asian countries. They come into operation either as a result of complaints received by DPAs, or of media (or other) reports resulting in 'own-motion' investigations by DPAs. In contrast, systemic enforcement mechanisms, discussed in the next section, have relatively little use as yet.

(p.511) ### 3.1. Reactive enforcement mechanisms in Asian laws

Tables 18.2 (reactive enforcement measures by DPAs) and 18.3 (reactive enforcement measures applied by courts) classify reactive enforcement measures under six main headings, in each of the 11 jurisdictions considered. They indicate whether each enforcement measure is present (√) or absent (X). However, in many instances, data privacy legislation is not specific about whether a particular enforcement measure is available, but it may be available under the general principles of administrative law or other branches of law in a country. In some such cases, the table takes a conservative approach and includes a dash (–) to indicate 'not certain'. In many cases a measure may only exist subject to significant qualifications. The tables also indicate the presumed 'aim' or primary purpose of each type of sanction/enforcement measure, classified (if appropriate) as: deterrence; prevention; guarantee of rights; and remedial. Each type of measure is then discussed briefly in the rest of this section.

3.2. DPA/ministry investigation types and powers

In the EU, the Fundamental Rights Agency (FRA) found that complaints to DPAs were preferred to judicial remedies:[6]

> Most complaints were lodged with the national DPAs and very few went through judicial procedures. Most individuals will not pursue cases before a court because of the lengthy, time-consuming and complicated procedures and costs involved. This view is widely shared by judges and practising lawyers. Reasons why people more often lodge complaints with national DPAs include the following factors: DPAs do not necessitate high costs; their complaint procedure is shorter and less complex; and the procedure does not demand legal representation.

Table 18.2 Table of reactive enforcement measures by DPAs

Jurisdictions*	Aim	CN	HK	IN	JN	KR	MA	MY	PH	TW	SN	VN
DPA/Ministry investigation types												
Complaint investigation	N/A	√	√	√	X	√	√	√	√	X	√	√
Own motion investigations	N/A	√	√	X	√	√	√	√	√	√	√	√

Own motion findings enforceable	N/A	√	√	X	√	√	√	X	√	√	√	√
Class complaints permitted	N/A	X	√	X	X	√	√	X	√	X	X	X
Investigative powers/procedures												
Onus of proof on data user	N/A	X	X	X	X	√	X	X	X	X	X	X
Use of ADR facilitated	N/A	X	X	X	X	√	X	X	X	X	√	√
Time limits on decision	N/A	X	X	√	X	√	X	X	X	X	X	X
DPA/Ministry remedies & orders												
Orders to prevent breaches	PRE	√	√	√	X	√	X	X	√	√	√	√
Orders to assert rights	GUA	√	√	√	X	√	√	√	√	X	√	√
Rectification orders	REM	√	√	X	√	√	√	√	√	√	√	√
Compensation awards	REM	X	X	X	X	√	X	X	√	X	X	√
Admin. penalty to breach Principles	DET	√	X	X	X	√	√	X	X	√	√	√
Publishing identified decisions	DET	√	√	√	X	√	√	X	X	X	X	√
Rescind/suspend licences	DET	√	X	X	X	X	X	X	X	X	X	*X*
Confiscate illegal profits/earnings	DET	√	X	X	X	√	X	X	X	X	X	*X*
Appeals against DPA/Min. orders	–	√	√	√	X	√	√	X	X	√	√	√

(*) Jurisdictions: CN = China; HK = Hong Kong SAR; IN = India; JN = Japan; KR = South Korea; MA = Macau SAR; MY = Malaysia; PH = the Philippines; TW = Taiwan; SN = Singapore; VN = Vietnam.

(p.512)

Table 18.3 Table of reactive enforcement measures applied by courts

Jurisdictions*	Aim	CN	HK	IN	JN	KR	MA	MY	PH	TW	SN	VN
Offences												
Some form of offences	DET	√	√	√	√	√	√	√	√	√	√	X
Offence to breach any Principles	DET	X	X	X	X	X	X	X	X	√	X	X
Offence to breach specified Principles	DET	X	X	X	X	√	√	X	√	?	√	X
Offence to breach ministry/DPA order	DET	X	√	X	√	X	√	√	X	?	√	√
Offence to mislead/interfere	DET	X	√	–	X	–	√	√	X	–	√	X
Offence of improper disposal	DET	X	X	X	X	√	√	X	√	X	X	X

Offence of sale of personal data	DET	√	√	√	X	√	√	√	√	X	X	X
Offence of trafficking (third parties)	DET	√	√	√	X	√	√	X	√	X	√	√
Personal liability (corporate officers)	DET	√	X	X	X	√	X	X	√	√	√	X
Punishments (government officers)	DET	X	X	X	–	√	X	X	√	√	X	X
Court action to enforce Principles												
Individual right of action in Court	REM	√	√	√	X	√	√	X	√	√	√	√
No need to prove breach ab initio	REM	X	√	X	–	√	√	–	X	X	X	X
Includes right to seek compensation	REM	√	√	√	X	√	√	X	√	√	√	√
'Class actions' before Courts	REM	√	X	X	X	√	X	X	√	√	X	X
DPA can intervene in Court cases	REM	X	√	X	X	X	X	X	X	X	X	X
Compensation cases to mediation	REM	X	X	X	X	√	X	X	√	X	√	X

(*) Jurisdictions: HK = Hong Kong SAR; IN = India; JN = Japan; KR = South Korea; MA = Macau SAR; MY = Malaysia; PH = the Philippines; TW = Taiwan; SN = Singapore; VN = Vietnam.

Acts in those Asian jurisdictions with a DPA (Hong Kong, Macau, South Korea, the Philippines, Malaysia, and Singapore) have clearly described complaint systems, and the DPAs have sufficient powers to investigate complaints, often with strong powers to compel answers, obtain documents, and inspect premises. In the three jurisdictions that do not have DPAs (Japan, Taiwan, and India) there are no transparent or effective systems for individuals to make complaints to the ministries that are supposed to supervise the data privacy laws. In Japan there is no evidence of the effectiveness of the alternative systems of complaint to the consumer bodies, local government bodies, or industry bodies. Japan's legislation says nothing about how persons should make complaints to any of the types of bodies entitled to receive them, nor how those bodies should deal with them. India's system does have rules about how Adjudicating Officers (AOs) are to investigate complaints, but they are unused to acting in relation to privacy.

Types of investigations permitted—complaints, and 'own motion'

The DPAs in Hong Kong, and Singapore are explicitly empowered to initiate investigations of their own volition ('own motion' or suo moto investigations). In the Philippines this seems to be covered by the DPA's power to 'institute investigations'. The AO system in India is only reactive: AOs do not initiate investigations themselves. The Macau DPA does

so, though lacking a law fully defining its functions. There is some evidence of ministries in Japan and Taiwan carrying out 'own motion' investigations. They do so in South Korea, China, and Vietnam.

It is a separate question whether a DPA (or ministry) has the ability to use its enforcement powers following such own-motion investigations. It is possible in Japan and Taiwan, but in practice does not occur to a significant extent. It is possible in South Korea, China, and Vietnam. The powers of the Macau DPA are not defined in terms of responding to complaints. The Singapore and Hong Kong DPAs can enforce own motion findings, and **(p.513)** this also seems to be implied in the Philippines. The enforcement powers of the Malaysian DPA are tied to the existence of a complaint (even if it has been withdrawn), so enforcement of own motion investigations is not possible.

Class complaints and representative actions

Provisions for complaints by classes or groups of complainants, with consequent remedies to benefit all members of the class, are included in the laws of some jurisdictions only. They are obviously important in relation to mass data spills, but in many other types of complaints as well. Hong Kong has a flexible procedure for complaints by one person on behalf of others similarly affected. Taiwan has specific procedures for collective actions before courts, but none in relation to complaints to ministries. South Korea has formal provisions allowing mediation of collective complaints within its mediation system, and also precise rules for representation in court disputes. The provisions in Vietnam and China are restricted to court actions. Vietnam's consumer law provides for the roles of 'Social organizations to protect consumers' interests' (i.e. consumer non-governmental organizations (NGOs)), including '[t]aking legal action on behalf of consumers or taking legal action by virtue of the public interests'. In China, official consumer associations are also since 2013 able to commence court actions on behalf of consumers, including where the rights of very large numbers of consumers are infringed. Japan has no specific procedures for class complaints (or court actions) in its Act. Complaints to the Malaysian DPA can only be by individuals, with no provision for representative complaints.

3.3. DPA/ministry powers to decide and enforce decisions

DPAs and ministries may have a broad range of enforcement powers: compliance orders; administrative penalties (fines); compensation orders; mediation roles (or referral powers); 'name and shame' publication. Rights of appeal from their decisions are a very important attribute, but not universal.

Compliance orders

Most DPAs can issue orders requiring data controllers to comply with privacy principles (or other Act requirements) whenever a breach is found, with failure to comply constituting a criminal offence, and possibly with other consequences. Compliance orders include powers to order access to, or correction of, personal records where this was improperly denied. For example, Macau's law makes failure to comply with its DPA's orders a crime. Hong Kong's law was amended in 2012 to allow compliance orders

whether or not continuing non-compliance was considered likely. The Malaysian law has the same deficiency as the pre-2012 Hong Kong law: the DPA cannot issue enforcement notices unless breaches are continuing or likely to be repeated. If they are, it can order steps to remedy a contravention, or the cessation of processing. The Philippines DPA can compel any entity to comply with its orders, and can 'facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity', so it can order considerably more than compliance with the Act. In Japan, the relevant ministry has power to issue compliance orders, but this never happens. Ministries only issue 'recommendations' to companies, and even then only rarely. In Taiwan, the power to order remedial actions is also provided, but used rarely. In India AOs may issue compliance orders but none have done so. Administrative sanctions apply to any violations of Vietnam's e-commerce regulations, but **(p.514)** the provisions are not specific. Ministries in China are empowered to issue a wide range of compliance and other orders.

DPAs do not normally have powers to issue injunctions against threatened or likely breaches which have not yet occurred. For example, Singapore requires a plaintiff to show 'loss or damage directly as a result of a contravention'. The Philippines' law implies its DPA has such powers. Under the Australian legislation, either a complainant or the Commissioner can seek an injunction from a court against such an anticipated breach, but this is an unusual provision. In some jurisdictions, courts may be able to issue injunctions against breaches of a statute.

Administrative penalties (fines)

In the EU, 'the most common course of action taken by DPAs is issuing a fine or pecuniary sanction', based on data from 19 EU states.[7] Over a three-year period, such administrative fines were very frequent in some countries such as Spain (1,715 instances), the Czech Republic (279), and Estonia (101), but much less so in others. The maximum possible fines varied widely between national laws, with the high end of the scale occupied by Spain (€600,000), the UK (€500,000), France (€300,000), and Greece (€150,000). Judicial fines often have comparable maximum amounts, as discussed later.

Although it is increasingly common in Asia for DPAs to be able to issue such fines or 'administrative penalties' for breaches, some still have no such powers, including in Hong Kong, Malaysia, and the Philippines. Contraventions of any of the substantive principles of the Macau law are offences carrying maximum fines of either US$5,000 or US$10,000. In Taiwan, companies can be subjected (as an alternative to criminal prosecutions) to an administrative fine by a ministry, up to US$15,000 for breaches of more important provisions. Company officers can be fined similarly unless they can prove they fulfilled their duty to prevent such a breach. In South Korea, a list of minor offences may be enforced by administrative penalties. Chinese ministries can issue fines up to US$82,250 where there are no illegal earnings, but also confiscate illegal earnings, or impose a fine 10 times the illegal earnings. In Vietnam there can be administrative sanctions for any breaches of principles, but the amounts of fines are not specified. Reforms underway in South Korea will introduce very high fines.

At present, Singapore's DPA carries the biggest 'stick', and the only one comparable with many European countries, because if it considers that an organization 'is not complying' with any of the privacy principles it may require payment of a financial penalty not exceeding S$1 million (US$790,000). The possibility of this 'million-dollar penalty' is an impressive dissuasive sanction. While such high levels of sanctions are generally desirable from the perspective of increased likelihood of compliance, it is only if they are used with an appropriate sense of proportion will they be desirable in practice.

Compensation orders by DPAs or ministries

In Europe, although the EU Data Protection Directive requires that compensatory damages be available, and in most EU countries judicial authorities can award damages,[8] but DPAs cannot do so. In Asia, until recently, South Korea was the only Asian jurisdiction allowing payment of compensation by a DPA (the specialized mediation **(p.515)** bodies or a ministry where a complaint is found to be justified. It is a routine part of data protection enforcement in South Korea, though payments are small, and the proposed settlement may be rejected by either party (who may then go to court). Over the past four years, 76 per cent (242) of cases where mediation resulted in a finding in favour of the complainant resulted in payment of damages as part or all of the remedy. Vietnam has specific provisions allowing compensation, but examples of such payments are not known. The Philippines now allows its DPA (when established) to order such payments, with no maximum limit specified. The other jurisdictions have no such provisions (Japan, Taiwan, Hong Kong, Singapore, Macau, Malaysia), though some allow compensation to be sought via the courts (discussed below). A unique South Korean element is that company privacy officers have a function of providing 'remedial compensation' before matters ever get to a DPA: compensation is built into the South Korean system at all levels.

Mediation—by DPA or third party referrals

All DPAs in Asia attempt to mediate to find a mutually acceptable solution to complaints. For example, Hong Kong's DPA states that in recent years about 10 per cent of complaints are resolved by mediation, although this function is not mentioned in its law. South Korea's law makes heavy use of mediation, first through informal mediation carried out at ministry level (designated by the law), but if that fails, through recommendations to an independent body created specifically for that purpose, the 'Personal Information Dispute Mediation Committee'. The functions of this Committee resemble arbitration, but the results can be accepted or rejected by the parties. Vietnam's e-commerce and consumer laws encourage mediation. The Philippines DPA has a specific function of seeking to enable settlements through use of alternative dispute resolution (ADR), which seems to imply that third party ADR may be used. Singapore's DPA may, with the consent of both parties, refer a dispute to third party mediation, or may direct either party to attempt to resolve a dispute in a way it considers appropriate.

'Name and shame' publication of decisions

Where respondents to successful complaints (i.e. parties in breach) may be named in public reports and thus press releases, this is a significant sanction in itself (as distinct from the transparency function of reporting). The Hong Kong DPA has led the way in

naming the respondents whenever 'section 48(2) reports' of breaches are published, using this adverse publicity as a sanction. On average seven such reports per year since 2011 have been published. Macao also has explicit provisions which treat publication of details of breaches (and specify newspaper publication and notices required), with named respondents, as an additional punishment. South Korea has provisions with similar effect. Macau and South Korea have used 'name and shame' less often than Hong Kong. In other jurisdictions the legislation is ambiguous. For example, the Philippines DPA has a specific power to 'prepare reports' and publicize them where it deems appropriate. China requires that violations must be logged by the telecommunications management organs in the 'social credit register' of a regulated entity, and published. Vietnam uses a similar technique, in that once a business receives notice of a complaint from the ministry, it only has 10 days to reply before it goes on the 'name and shame' list on the ministry website, and before administrative sanctions can be brought against it. Similar adverse publicity can follow a ministry inspection. It seems that Japan's ministries never use 'name and shame', unless a **(p.516)** respondent has already been 'outed' by the media. Other laws do not make any provision for such a sanction (Malaysia, Singapore, India).

Appeals from DPA decisions

All Asian jurisdictions with DPAs allow appeals from their decisions. Japan and Taiwan do not have specific provisions for appeals from ministry decisions, but those decisions are not based on individual complaints in any event. In Taiwan, administrative review of such decisions is common. In Malaysia the right of appeal against decisions of the DPA is defective, in that only respondent companies are given a right of appeal, not complainants (although, inconsistently, complainants can appeal against the DPA's refusal to investigate their complaint).

In Hong Kong, appeals are to the Administrative Appeals Board, a general administrative law tribunal, not one specifically for data protection matters, and there is no further appeal to the courts. Appeals occur frequently. In South Korea, appeals to the courts (not to another tribunal) may be made against DPA decisions. In Macau, appeals against DPA actions or decisions are to the Administrative Court, but on issues of fundamental rights there may be appeals direct to the Court of Final Appeal. Singapore allows appeals to a specialist Data Protection Appeal Panel on any grounds (law, facts, or remedies). There is also a limited right of appeal from an appeal committee to the courts, initially to the High Court, on a point of law, or from a direction as to the amount of financial penalty, but not on questions of fact. No appeal provisions are specifically provided in relation to decisions of the Philippines DPA.

In India the supposed appeals body (Cyber Appellate Tribunal) stopped functioning before India's data privacy Rules commenced, and has not re-started. In Japan there are no specific provisions for appeals against ministerial orders, but it does not matter because Ministers never make orders. Nor is there an explicit right of appeal in Taiwan, but companies can and do seek administrative review. In China and Vietnam there is also a general right of appeal against administrative decisions.

3.4. Criminal offences

The FRA found that in almost all EU countries, a variety of criminal sanctions and penalties can be imposed by judicial bodies:[9]

> In serious enough cases, criminal proceedings can be initiated for violations of data protection legislation. As the research demonstrates, there are a number of possible outcomes once court proceedings have been initiated: the courts can issue warnings; publicise any judgment made; prohibit an individual from managing the processing of data in the future; and compel those responsible for the violation to undertake community service.
>
> In addition, in all EU Member States the courts can impose fines, issue prison sentences or combine both. The size of the fine or length of the prison sentence is set out in national legislation and varies between Member States. Much like the civil and administrative procedures in place, the sentence will be affected by whether the violation involves natural persons or legal entities.

The maximum fines that can be imposed in EU countries vary greatly, from US$12,000, up to US$415,000 (€300,000) in France, and no maximum imposed on UK courts.[10]

(p.517)

Table 18.4 Maximum fines in Asian legislation, by DPA/ministry or by a court

Jurisdiction	Admin fine US$	Court fine US$
China (PRC)	$82,500	None
Hong Kong SAR	None	$13,000
Japan	None	$3,000
India	None	$8,000
Korea	$50,000	$100,000
Macau SAR	$10,000	None
Malaysia	None	$100,000
Philippines	None	$45,500
Taiwan	$15,000	$33,000
Singapore	$790,000	$80,000
Vietnam	None	None

Across Asia, other than compliance orders by DPAs (without other penalties), criminal prosecutions are one of the most commonly used means of enforcement. Every jurisdiction has some criminal offences in its legislation, although not necessarily for breaches of all provision of the data privacy law. Criminal offences in the criminal code are often used in Taiwan and Macau, and in China, instead of using offences located in the data privacy laws themselves. In Hong Kong, criminal prosecutions have been used in the past because of a lack of other enforcement mechanisms. Table 18.4 compares the

maximum fines (for a single breach) allowed in legislation in Asia, either as an administrative fine by a DPA or a ministry, or by a court.

In comparison with Europe, the potential financial penalties able to be awarded either administratively or by a court are low, with the exception of Singapore's provision for administrative fines. Outside Europe, higher potential fines are becoming more common, with Australia's 2012 amendments to its law allowing for a maximum fine by a court of $US1,590,000.

Offences involving breaches of principles

Malaysia is unusual in that breaches of any one of the seven principles in the Act constitutes an offence carrying a maximum fine of US$100,000. However, in most Asian jurisdictions, a breach of the principles in the Act is not an offence in itself: there must first be an enforcement order issued by a DPA or ministry, and non-compliance with that order. The maximum fine for contravention of an enforcement notice in Hong Kong is about US$13,000, but in practice the highest fine in 2012 was only US$1,300. Repeated or successive similar non-compliance is now subject to a US$65,000 maximum fine. In Japan there must first be a breach of a ministerial order to attract criminal penalties (with fines only up to US$3,000) but no such orders have ever been made. Some breaches of an enforcement notice in Singapore's Act—essentially those showing a dishonest intent—may constitute offences, resulting in fines ranging from US$4,000–80,000 for organizations or US$4,000–8,000 for individuals, with lesser penalties for wrongful access to, or alteration of, personal data.

However, in some jurisdictions breaches of some specified principles constitute offences (a broad range in the Philippines), or damage to individuals triggers an offence (Taiwan), without need for breach of an enforcement order. Similarly, Macau's law specifies a wide range of offences that may be carried out by controllers, processors, or third parties. In Taiwan, breaches of the principles in the Act, where damage is caused to another, can result **(p.518)** in fines up to about US$6,700, or to US$33,000 where there is intent to profit or gain other benefits. Penalties increase by 50 per cent where offences are committed by civil servants. As yet under the new Act there have only been prosecutions in what are essentially domestic matters, with small fines. In the Philippines, the maximum penalties of two million pesos (US$45,500), and imprisonment for up to five years, are mandatory where the personal information of more than 100 persons is affected. In South Korea the maximum fine for 'normal' breaches is US$100,000, but extraordinarily high penalties ('surcharges') are being added by new amendments where resident registration (RR) numbers or commercial sales of data are involved.

Offences involving data theft and third parties ('trafficking')

Data protection laws used to deal only with breaches of privacy principles, and offences, by data controllers or processors. However, offences by third parties involving wrongful acquisition, sale, or purchase of personal data ('trafficking' in personal data) have been added to most new or revised data privacy laws in Asia. New Hong Kong offences for disclosing personal data obtained from a data controller carry penalties up to US$13,000.

The Philippines offences include many that may be committed by third parties, and include unauthorized access to personal information and providing such access. Malaysia's offences include sale or purchase of personal data. Both mainland China and Vietnam have passed laws criminalizing third party personal data disclosures during 2009. Some such offences which may be committed by third parties are clearly needed in any comprehensive data privacy law.

3.5. Access to judicial remedies by data subjects

In the EU, courts are able to issue compliance orders and injunctions in relation to breaches of data privacy laws:

> In five EU Member States, courts can issue an order demanding that access be granted to specific data; 10 Member States use orders for the controller to rectify, erase or cease the processing of specific data; and in four Member States the courts are able to order that relevant third parties or the public be informed of any violation or subsequent court judgment.[11]

In most EU member states, according to the FRA, 'judicial authorities can award damages for violations, although guidelines on award amounts vary'.[12]

> With regard to civil and administrative procedures, most of the EU Member States explicitly recognise the ability to award compensation in the form of damages. Several Member States report that non-pecuniary compensation can also be granted. Whereas some Member States set out in domestic legislation the amount of compensation that can be awarded, often it is left to judges to develop an accepted range of both pecuniary and non-pecuniary damages through national case law. Again, the amounts awarded vary greatly between Member States. Austria for instance, sets an upper limit of €20,000 for non-pecuniary damages, but the range of cases in other Member States suggests that awards of compensation are often much lower, ranging from €300 to €800 in Finland, up to €600 in Sweden, and from €1,200 to €12,000 in Poland.

(p.519) The potential range is therefore a low US$415 (Finland) to a high US$15,600 in Poland, with Austria's US$27,600 being an outrider. Actual payment ranges are not stated. However, the FRA found that compensation was not a major motivating factor for complainants:[13]

> The complainants and non-complainants interviewed defined the damage from data protection violations as psychological and social. They described emotional distress, offence, insecurity or damage to reputation as well as impact on their relations with other people. Fieldwork participants also reported financial damages but less frequently. Financial compensation was not a motivating factor to seek redress for the fieldwork participants. Instead, most complainants and non-complainants say they sought redress to ensure that similar data protection violations do not recur.

In Asia there is a right to seek compensation through court actions in most data privacy

laws (Hong Kong, Macau, Singapore, South Korea, Taiwan, China, Vietnam, and possibly India), and equivalent rights may also arise under the Civil Code in some civil law jurisdictions (Macau, Taiwan, South Korea) but not in common law jurisdictions. In the Philippines the Act only provides for compensation actions when an offence has occurred, but actions may also be possible under the Civil Code. Vietnam's e-commerce and consumer laws appear to provide that any breaches of the privacy principles can potentially result in a claim for compensation through the courts. China's laws are specific that there is a right to compensation, but not yet clear on how it may be pursued, though it is likely that this could occur under the tort law.

In South Korea complainants pursue compensation before the civil courts, not before a DPA or specialist tribunal. Data controllers have the onus of proof of lack of 'wrongful intent or negligence'. Also, to reduce the damages payable, they have the onus of showing 'compliance with the Act' and 'non-negligence of due care and supervision'. Other jurisdictions do not have pro-complainant procedural rules to this extent.

Singaporean complainants who have suffered 'loss or damage directly as a result of a contravention' of those principles applying to individuals have a right of private action before a court to obtain injunctions or damages. It is not clear whether it is necessary for the complainant to prove ab initio (despite a prior finding by the DPA) that there is a contravention before the court can consider the question of compensation. This would be a significant disincentive to actions. In Hong Kong, a similar provision allowing a civil action for compensation before the courts, has not resulted in any compensation being paid since the law has operated, nor has any claim proceeded to a full hearing. However, the 2012 amendments allow matters to be heard in the District Court, reducing the likelihood of costs being awarded against plaintiffs. Additional provisions make it easier for a plaintiff to prove in court matters that have already been investigated by the DPA.

In Malaysia there are no provisions by which complainants may seek compensation for damage: the DPA cannot award damages, data subjects cannot seek compensation in court proceedings under the Act, and Malaysia has not developed a tort of invasion of privacy. In Japan complainants also have no avenue through which to obtain compensation (except ex gratia), because the courts have as yet refused to allow breaches of the data privacy law to found a cause of action, and the civil law is under-developed and will only provide compensation for some types of breaches.

While compensation actions through courts are possible in most jurisdictions, in some it is known they have not occurred (Hong Kong, India), in others it is as yet too early (Singapore and the Philippines), and otherwise it is difficult to obtain examples of cases and amounts typically paid (Macau, Taiwan, South Korea).

(p.520) Litigation assistance to complainants

The FRA found that in the EU, merely providing a legal right to compensation before a court was rarely sufficient:[14]

> Most interviewees worry about the lack of legal assistance available. Judges and

lawyers interviewed noted that there are too few data protection professionals; they also recommended training and more specialisation in data protection law. This lack of data protection experts was also a problem in looking for and trying to access interviewees during the fieldwork. People also raised concerns over the lack of financial and human resources available to DPAs and intermediary organisations specialised in the area of data protection. Many individuals reported difficulty in obtaining information about procedures and insufficient knowledge of remedies.

As a result of the 2012 amendments to the Hong Kong Ordinance, their Commissioner can assist complainants to obtain evidence from respondents (by questions and answers) in order to prepare a compensation claim and governing the admissibility of such answers as evidence in court. There is no provision for other DPAs in Asian jurisdictions to intervene in civil court cases on behalf of plaintiffs.

4. Systemic methods of enforcement, and assisting compliance

There is limited provision of systemic enforcement measures to prevent or deter breaches of privacy principles in Asian data privacy laws, both old and new. They have had some impact through the more established laws, particularly in South Korea, in Macau, in various ways in Hong Kong, and through quasi-mandatory guidelines in Japan and Taiwan. Systemic measures to encourage and assist compliance, such as education facilities, advice hotlines, and advisory guidelines are more common, and will not be discussed in detail.

Table 18.5, with the same structure as Table 18.2, compares jurisdictions, and each of the various systemic compliance measures is discussed below.

Table 18.5 Table of systemic measures to enforce or assist compliance

Jurisdictions*	Aim	CN	HK	IN	JN	KR	MA	MY	PH	TW	SN	VN
Systemic enforcement measures												
DPA/ministry inspection/audit	PRE	X	√	X	X	√	√	√	X	X	X	√
Independent audits required	PRE	X	X	√	X	X	X	X	X	X	X	X
Privacy Impact Assessments required	PRE	X	X	X	X	√	X	X	X	X	X	X
Data user registration (comprehensive)	DET	X	X	X	X	X	X	X	X	X	X	X
Data user registration (selective)	DET	X	√	X	X	X	√	√	X	X	X	X
Data protection officer required	PRE	X	X	√	X	√	X	X	X	X	X	X
Measures to assist compliance												
Issuing advisory Guidelines		X	√	√	√	√	√	–	√	√	√	X

Approval of codes of conduct	X	√	X	X	X	√	√	√	√	X	X
Educational functions	√	√	X	X	√	√	√	√	√	√	X

(*) Jurisdictions: CN = China; HK = Hong Kong SAR; IN = India; JN = Japan; KR = South Korea; MA = Macau SAR; MY = Malaysia; PH = the Philippines; TW = Taiwan; SN = Singapore; VN = Vietnam.

(p.521) 4.1. Systemic compliance measures

Singapore, and the Philippines do not have any explicit systemic compliance measures in their legislation. Nor do Japan and Taiwan, but their ministry-based enforcement model would lend itself to ministries having such powers as part of their general supervisory functions in an industry. Whether they are used in relation to data privacy would, however, be difficult to establish. Similar considerations apply in China and Vietnam.

Data protection officers

South Korea is the only Asian jurisdiction to yet require a data protection officer with extensive and onerous obligations, defined qualifications for appointees, and defined independence of action. India has a requirement for a data protection officer to be appointed, but without the specific qualifications and obligations as in South Korea, and it is ambiguous when and whether data subjects can complain to such a person.

Audits or inspections

DPA inspections or compliance audits of personal data systems can be required in Hong Kong, South Korea, Macao, and Malaysia. In Hong Kong the DPA has powers to carry out formal inspections of personal data systems, but has only done so and published reports (which are very detailed) on four occasions. Instead, the DPA carries out informal 'compliance checks' (220 in 2012–13, mostly in the private sector). Malaysia's DPA has power to carry out inspections, and regulations have been made concerning the records that must be kept. In China and Vietnam, periodic inspections, and publication of their results, are the main means of systemic enforcement. In India, compliance with the security principle probably requires independent audits, but the Rules are ambiguous.

Registration or notification systems

Registration systems are uncommon in Asia, and comprehensive registration schemes are not found. Registration of data controllers in particular categories considered to be of higher risk can be required in Hong Kong and in Macau. In Malaysia, the registration scheme is primarily a revenue-raising device. In no Asian jurisdictions is a cancellation of registration used as a punitive enforcement measure equivalent to cancellation of a 'licence to process data'. The Hong Kong DPA has postponed implementation of a selective registration scheme in four major industry sectors until it is clear what approach the EU is going to take, but only on the basis that data controllers in these sectors are expected to implement voluntary 'accountability' measures. While China does not have a data privacy registration system, suspension or termination of business operations, websites, or licences are among the range of administrative sanctions that can

result from either complaints or periodic inspections.

Macau has a notification (quasi-registration) system, requiring notification to its DPA within eight days of most automated processing of data, or processing of sensitive data, unless an exemption from notification is obtained. It also has a 'prior checking' system where particular types of processing are illegal without prior DPA authorization, but this has only been applied to the public sector as yet, except in relation to 'interconnections' of data (data matching). These are the only such requirements in Asia as yet.

(p.522) Privacy impact assessments (PIAs)

Privacy impact assessments (PIAs) can be required in South Korea, but only for public sector entities. No other Asian jurisdiction yet has specific provisions for privacy impact assessments of potentially dangerous systems. Macau's 'prior checking' system could be used in a similar fashion. A number of PIAs were carried out in relation to Hong Kong's development of its smart ID card, and one was made public. PIAs have not become a common practice in Hong Kong, or elsewhere in Asia.

Codes of conduct

Where a DPA issues codes of conduct which are not merely advisory but have some legal effect, this is a form of systemic regulation because it makes the application of general privacy principles more precise for a particular industry sector, and therefore makes clearer what standards data controllers in that industry sector must observe. There are many different ways in which codes can be developed, and enforced. They lead to argument about whether specific codes improve or degrade the effectiveness of regulation.

Under Macau's provisions for codes (as yet unused), DPA approval only means it is the DPA's opinion that the code is lawful, but it has no legal effect on what a court might decide. The Hong Kong DPA may issue codes as to how the law may be complied with by a particular sector or in relation to a particular activity. Non-compliance does not itself amount to a contravention of the law, but in legal proceedings it is admissible in evidence and raises a rebuttable legal presumption against the data controller concerned. Compliance with a code does not automatically constitute compliance with the law. Only two codes have been issued, on ID cards and numbers, and on credit reporting. The Philippines DPA will be able to approve codes, which may include private dispute resolution mechanisms, but the relationship between codes and the Act is unstated, and raises the risk that consumers will lose their statutory rights. The Malaysian DPA will also be able to do so, and approved codes will carry penalties for non-compliance. In Japan and Taiwan, ministry guidelines for particular sectors are to some extent like statutory Codes of Conduct in other jurisdictions, because of the regulatory powers that ministries exercise in each sector. Extensive use of them is made in both countries.

Openness of processing procedures required

Where jurisdictions implement the OECD 'openness principle' requiring data controllers to provide information about data processing practices to any person who enquires (including NGOs or the media), and not only to data subjects, this should operate as a

systemic measure acting as a deterrent against non-compliance. Hong Kong is a rare example of a jurisdiction implementing such a provision in relation to its private sector, though it can in effect be provided by FOI/RTI laws in relation to the public sectors of other countries that have them (South Korea, Japan, and India).

4.2. Measures to assist compliance and exercise of rights, and resources

No attempt is made in this study to comprehensively document the various ways in which DPAs and ministries take positive measures to assist data controllers to comply with their legal obligations, or to assist data subjects (consumers and citizens) to exercise their rights. That is a sociological study which would be valuable, but beyond the scope of this book. **(p.523)** However, it is important to emphasize that such measures are extremely important, as the theories of responsive regulation stress (see Chapter 3, section 4.2). Established DPAs such as in Hong Kong or in South Korea (by the Korea Internet & Security Agency (KISA) before the current DPA) invest a significant proportion of their resources in very creative ways to assist both data controllers and data subjects to understand their obligations and rights. Finally, although no comparisons are made here, it is obviously necessary that a DPA, or the relevant sections within a ministry, must have sufficient resources to carry out both enforcement activities and actions to assist compliance, otherwise legal provisions may be empty gestures.

5. Transparency—the evidence of enforcement

The relationship between responsive regulation and transparency in the operation of sanctions (reactive or systemic) is discussed in Chapter 3, section 4.3. Two main forms of transparency were identified: (i) publication of case studies and (ii) publication of statistics concerning outcomes and remedies.[15] Such publication may be required by law, or may simply be a practice adopted by a privacy enforcement authority. Such transparency may be provided by a DPA, or by ministries, but is far more likely to provide effective transparency where published centrally, and with consistency, and so is much more likely to be provided by a DPA rather than scattered across ministries (as a comparison of Japan or Taiwan with, say, Hong Kong or Macau illustrates).

Table 18.6, which has the same structure as earlier tables in this chapter, is accompanied by a brief comparison of each type of transparency measure. Where a provision in a law makes coverage doubtful, ‘no’ (X) is indicated. Where it is too early to assess, this is indicated by a dash (–).

5.1. Complaint case studies

Details of selected complaints investigated by Hong Kong’s DPA have been published on its website since the late 1990s, usually in enough detail to explain the main legal issues and the DPA’s response, at an average rate of almost 20 per year until 2009, with ‘catch up’ for 2010–13 ongoing. Macau has the highest rate of publication of complaint summaries of any Asian jurisdiction, publishing summaries of 28 per cent of complaints investigated during its first six years. South Korea also publishes very considerable numbers of complaint

Table 18.6 Table of transparency measures in Asian laws and practices

Jurisdictions*	Aim	HK	IN	JN	KR	MA	MY	PH	TW	SN
Publication of DPA decisions authorized	DET	√	?	X	√	√	X	X	X	X
Publication of DPA decisions required	DET	X	X	X	X	X	X	X	X	X
Published (selected) anon case studies	DET	√	X	X	√	√	–	–	X	–
Case studies of systemic enforcement	DET	√	X	–	√	√	–	–	X	–
Statistics of enforcement outcomes	DET	√	X	√	√	√	–	–	X	–

(*) Jurisdictions: HK = Hong Kong SAR; IN = India; JN = Japan; KR = South Korea; MA = Macau SAR; MY = Malaysia; PH = the Philippines; TW = Taiwan; SN = Singapore.

(p.524) summaries, but only a few are translated into English. The International Privacy Law Library allows the complaint summaries and appeal decisions of 10 DPAs to be searched together, including from Hong Kong, Macau, and South Korea.[16]

The DPAs in Singapore, Malaysia, and the Philippines have not yet handled any complaints, so their practices are as yet unknown, and only the requirements of the law can currently be considered. Singapore's law is unclear, and does not state that the DPA can publish decisions it makes. Appeal committees must notify the DPA, as well as the parties, of their decisions and reasons, but nothing is said about publication.

The publication of complaint summaries by ministries in Japan and Taiwan has been non-existent, one of the main failures of their ministry-based system of enforcement. No case studies of any value have been published in Japan, nor any court decisions. Under Taiwan's new Act, its Justice Ministry has not taken on any coordinating role in publishing complaint case studies. However, there are quite a few reported cases in the courts, from which that aspect of the Act's operation is more transparent. In India there is nothing to report.

5.2. Complaint outcome statistics

Reporting of remedial outcomes is the weakest aspect of the reporting practices in Asian jurisdictions, and probably in others as well. The Hong Kong DPA, though admirable in other aspects of transparency, does not report remedial outcomes in a sufficiently informative way, but has stated it intends to do so in future. Macau's DPA publishes statistics of the number of complaints resulting in sanctions but little more than that. Japan's Cabinet and its Consumer Agency have at various times made efforts to publish some enforcement statistics, but they are not very informative. Taiwan publishes very little.

5.3. Reporting systemic enforcement

Macau's DPA publishes considerable details of various types of systemic enforcement, particularly authorization decisions concerning data matching, data exports, and similar

matters. Hong Kong's DPA publishes detailed reports as a result of any formal inspection, and publishes briefer details in its annual report of more informal 'compliance checks'. There is no systemic enforcement to report in Taiwan, Japan, or India.

6. Privatized enforcement: Codes, seals, PETs, and other co-regulation

While industry self-regulation (and co-regulation) normally plays a significant role in theories of responsive regulation, neither form has had a very encouraging record in 40 years of privacy regulation. That may be in part because of a lack of transparency in such systems, which impedes appreciation of success, but lack of transparency is a fatal defect in self-regulation or co-regulation because it equates to 'trust us' in situations of clear conflict of interest. Self-regulation has the onus of proof. So do government regulators who deflect complainants to industry-run schemes.

(p.525) 6.1. Privatized enforcement and DPA 'pass the parcel' provisions

Japan's attempt to create private sector complaint handling bodies by statute is a failure, with nothing known of how any of them have ever handled complaints (if they have). No other jurisdiction has gone down that unsupervised dead end.

The laws of various countries allow DPAs to refuse to investigate a complaint, or to 'pass the parcel' to another body after commencing investigation. These laws may sometimes result in a more expert complaint body in a particular sector taking over a complaint, and possibly one with enforcement powers equivalent to or stronger than the DPA. However, there is usually no prohibition on DPAs referring complaints to bodies with weaker enforcement powers (or perhaps ones which have been captured by the industries they regulate), with no requirement that the data subject agrees to the referral.

6.2. Privacy seals

There is little evidence of any of the privacy seal systems in Asia providing any benefits to consumers, though they may provide some benefits to the companies holding them. Japan's PrivacyMark is the most long-established in Asia, and has very high take up among data controllers. This is influenced by the fact that it is, in effect, compulsory to hold one in order to obtain local government contracts, which may reduce and compromise its credibility. No instances of a company having its PrivacyMark revoked have occurred, reducing the credibility of its only major sanction against members. It has procedures for third party investigation of complaints. Very little evidence of the effectiveness of the system is published.

Taiwan's TPIPAS DP Mark and South Korea's new Personal Information Protection Level Certification Management System (PIPL) Mark are informed to some extent by Japan's PrivacyMark, but are in their early stages of development, so conclusions are premature. In South Korea companies and government agencies are now eligible to apply for certification under PIPL. Certification will provide benefits for companies including reduced supervision and potentially reduced penalties. India has a system of smoke and mirrors operated by the Data Security Council of India, which purports to be a data protection system but has no provision for complaints by data subjects.

6.3. APEC's Cross-Border Privacy Rules (CBPR)

In Chapter 19 it is explained that the Asia-Pacific Economic Cooperation (APEC)'s Cross-Border Privacy Rules (CBPR) system is not yet operating for any Asian country, and that when and if it does operate, it will be something like a series of 'mini safe-harbours', probably for the primary benefit of US companies. It will be a form of co-regulation, but possibly one with no credibility or utility.

7. Conclusions—responsive regulation?

The recent increase in the number of privacy laws in Asia, and reforms of existing laws, means that there are now ample examples of regulatory options to compare in the Asian context. However, only a few Asian jurisdictions have had data privacy laws in operation for long enough for their effectiveness in practice to become apparent.

(p.526) 7.1. A regulatory toolkit in theory

Inspection of Table 18.2 at section 3.1 indicates that South Korea, followed by Macau, has the widest range of enforcement mechanisms. Each jurisdiction's laws have been in force for long enough for assessment of their use to be possible. Following the 2012 reforms, Hong Kong's DPA has a much broader range of enforcement measures, adding some bite to the current Commissioner's insistent bark. Singapore has a variety of potentially strong enforcement mechanisms, notably the 'million dollar fine'. The Philippines also has a wide range of measures, in theory. It will take some years from 2014 before an assessment of either law can be made concerning whether the sanctions are used and used effectively.

The Malaysian law is lacking almost any enforcement measures, and those it has suffer from the same deficiencies as the pre-reform Hong Kong law. Japan's law has negligible enforcement measures, and even those are not being used. Taiwan's reformed Act is considerably better than that, but the ministries have made little use of the enforcement measures as yet. India has some ambiguous measures, but they are not used.

7.2. A track record of effective regulation?

Of those jurisdictions whose laws have been operative long enough for them to have a track record, Japan, Taiwan, and India (the three ministry-based models of enforcement) share the 'wooden spoon' award for inactivity and non-responsive regulation.

Despite its previously defective toolkit, the Hong Kong DPA has vigorously and publicly attempted to make the maximum use of all enforcement measures in its possession in recent years, particularly the 'name and shame' approach. In a very small jurisdiction, Macau's DPA has used a range of quite different powers consistently and vigorously. South Korea's DPAs and ministry agencies, including KISA, the Personal Information Dispute Mediation Committee (PIDMC), and the Korean Communications Commission (KCC), now supplemented by the Personal Information Protection Commission (PIPC), have in combination been effective in a much larger jurisdiction than either Hong Kong or Macau. Further comparison is unnecessary, because all three of these DPAs satisfy the basic criteria for responsive regulation (though only recently in Hong Kong's case), even

though all have room for improvement on each criterion:

> (i) a diverse range of regulatory measures ('toolkit'), sufficient to allow graduated responses to breaches of different forms of seriousness, and to complement reactive measures with systemic measures and with incentives;
> (ii) a track record of actually using all the enforcement measures available to them;
> (iii) a reasonable degree of transparency in regularly publishing details of the complaints they investigate and resolve, and the remedies that result.

'Responsive regulation' is therefore alive in Asian privacy regulation, even if it is not yet 'state of the art'.

7.3. Ministry-based privacy regulation appears to have failed

Japan, Taiwan, and India produce little that can be recognized as enforcement of their laws, irrespective of how strong or weak the principles in their laws may be. At this point, they are the three regulatory failures in Asian privacy, and they are the three examples that **(p.527)** only include ministry-based enforcement. The three success stories are the three longest-established DPAs (although South Korea is a mixed model). The three new DPAs—Singapore, Malaysia, and the Philippines—are not yet active, and so have not been able to falsify (or support) the hypothesis that it is ministry-based enforcement that is a major problem for effectiveness of data privacy laws.

Notes:

([1]) European Union Agency for Fundamental Rights, *Access to data protection remedies in EU Member States* (FRA, 2013).

([2]) Christopher Kuner, *European Data Protection Law* (2nd Edn., Oxford University Press, 2007), pt. 1.G 'Enforcement of the Law', pp. 50–7; see also Appendix 13 'Selected enforcement measures'.

([3]) These results may be underestimates for some jurisdictions, if other laws provide the attribute.

([4]) Graham Greenleaf, 'Scheherazade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories' (2014) 23(1), *Journal of Law, Information and Science* <www.jlisjournal.org/abstracts/greenleaf.23.1.html>, section 'The Prevalence of DPAs'.

([5]) Which is in part a reflection of the 'democratic deficits' in the semi-democratic regimes: see Chapter 1, section 5.2.

([6]) EU FRA, *Access to data protection remedies*, p. 8.

([7]) EU FRA, *Access to data protection remedies*, p. 21.

([8]) EU FRA, *Access to data protection remedies*, p. 21.

([9]) EU FRA, *Access to data protection remedies*, p. 22. Fine ranges are given for many other countries as well.

([10]) EU FRA, *Access to data protection remedies*, p. 22.

([11]) EU FRA, *Access to data protection remedies*, p. 22.

([12]) EU FRA, *Access to data protection remedies*, p. 21.

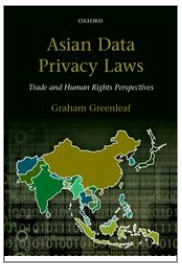
([13]) EU FRA, *Access to data protection remedies*, p. 7.

([14]) EU FRA, *Access to data protection remedies*, p. 8.

([15]) As distinct from publication of workload statistics, which have other useful transparency benefits but say little about the effectiveness of enforcement.

([16]) International Privacy Law Library (World Legal Information Institute) <http://www.worldlii.org/int/special/privacy/>.

University Press Scholarship Online
Oxford Scholarship Online



Asian Data Privacy Laws: Trade & Human Rights Perspectives
Graham Greenleaf

Print publication date: 2014
Print ISBN-13: 9780199679669
Published to Oxford Scholarship Online: December 2014
DOI: 10.1093/acprof:oso/9780199679669.001.0001

International Developments—Future Prospects for Asia

Graham Greenleaf

DOI:10.1093/acprof:oso/9780199679669.003.0019

[–] Abstract and Keywords

This chapter discusses the developments concerning global or regional data privacy agreements and instruments likely to affect Asian countries in future. The overall picture is one of continuing competition for global influence over the shape of data privacy developments, and their trade and human rights implications. The issues are usually more complex than a simple 'USA v Europe' divide. The main international developments considered are: APEC (Asia-Pacific Economic Cooperation)'s Cross-Border Privacy Rules system (CBPRs); the 2013 revision of the OECD (Organisation for Economic Co-operation and Development) privacy Guidelines, and its 'globalization'; the Council of Europe Convention 108 'modernization' and 'globalization'; the proposed EU data protection Regulation; United Nations developments including the surveillance resolution and proposed new International Covenant on Civil and Political Rights (ICCPR) protocol; and the possibility of law reform in the USA. Discussion of the strengthening of global privacy standards, and five prospects for global or regional agreements, conclude the chapter.

Keywords: data protection, privacy, Asia, APEC CBPR, OECD, United Nations, UN, European Union, Council of Europe, USA

1. Introduction

Whereas Chapter 2 discussed existing agreements and instruments that have already shaped the data privacy landscape in Asia, this chapter discusses the developments concerning global or regional data privacy agreements and instruments likely to affect Asian countries in future. The overall picture is one of continuing competition for global influence over the shape of data privacy developments, and their trade and human rights implications. Although on many important issues the USA tends to be on one side and European institutions (and most European countries) on the other side, the issues are usually more complex than a simple 'USA v Europe' divide, and the positions of many (perhaps most) countries cannot be so simply classified. Many international developments in data privacy law, and their consequences, remain unresolved at the end of 2013, including the continuing implications of the disclosures triggered by Edward Snowden.

1.1. The global surveillance context after Snowden

After the attacks on New York City on 11 September 2001 (often referred to as '9/11'), there were many claims that 'everything is different', including in relation to the protection of privacy. New laws authorizing expanded surveillance were enacted, particularly the 'homeland security' legislation in the USA. There was little realization of just how 'different' the surveillance practices of some countries had become since 2001, until information about such practices were revealed by Edward Snowden and others, commencing in 2013 and **(p.530)** continuing. Surveillance practices by the USA, the UK, their 'Five Eyes' partners in espionage (Australia, New Zealand, and Canada), and various other countries have been shown to have gone far beyond what was known or expected. The 'Snowden revelations', as they are referred to here, have been summarized in part by *The Guardian* newspaper,[1] which played a major role in bringing them to light, as follows:[2]

> The Snowden files reveal a number of mass-surveillance programs undertaken by the NSA [the USA's National Signals Agency] and GCHQ [the UK's Government Communications Headquarters]. The agencies are able to access information stored by major US technology companies, often without individual warrants, as well as mass-intercepting data from the fibre-optic cables which make up the backbone of global phone and internet networks. The agencies have also worked to undermine the security standards upon which the internet, commerce and banking rely.
>
> The revelations have raised concerns about growing domestic surveillance, the scale of global monitoring, trustworthiness of the technology sector, whether the agencies can keep their information secure, and the quality of the laws and oversight keeping the agencies in check

As a result of the continuing Snowden-instigated revelations, it may be the case that many attitudes to privacy protection, and the desire to react against surveillance practices, may be 'different' after 2013. This reaction is not likely to be in the direction of 'you have zero privacy anyway, get over it' suggested by Scott McNealy of Sun Microsystems in 1999.[3] Although it is far too early to be sure of their final form, some of the international reactions against unchecked state surveillance have included increased interest in the UN becoming more involved in privacy issues (section 4.1 of this chapter), and a reduction or slowing down of cooperation on privacy issues between the USA and various European Union (EU) countries and institutions.

The Snowden revelations have caused many to reconsider the use of so-called 'cloud-based services' for personal data. Some countries are legislating or considering legislation to require servers containing the personal data of their citizens to be based in their country. This poses a significant threat to providers of cloud-based services. Some Asian countries, including Indonesia[4] and Vietnam, are already moving to require local servers, usually in relation to government services. Others, such as South Korea and India,[5] are moving to build 'local clouds'. The details of such legislation and proposals are beyond the scope of this book. A United Nations Conference on Trade and Development (UNCTAD) review of cloud-specific law, policy, and regulation in developing countries[6] argues that 'while the nature of TDFs [transborder data flows] has evolved way beyond that imagined some 40 years ago, concerns about the potential erosion or circumvention of national privacy protections remain at the forefront of the policy response to cloud computing'.[7] It **(p.531)** concluded that 'developing countries could benefit from implementing strong domestic privacy regimes' and '[a]ligning such laws with leading international legal instruments [such as] the Council of Europe [data protection] Convention'.[8] It is clearly in the current interests of the USA to use its economic and political power to dissuade as many countries as possible from taking such steps, and in that context international agreements which prevent them from taking such steps may become important. Since the first development of international agreements on data privacy in the early 1980s there has been a constant struggle between the objectives of privacy protection and free flow of personal information, and there is no sign that this conflict is yet resolved. From 2014 onward, the significance of international agreements affecting data privacy is likely to intensify.

2. APEC's Cross-border Privacy Rules (CBPR) system

The most discussed new development with potential direct effect on at least some Asian countries is the Asia-Pacific Economic Cooperation (APEC) Cross-border Privacy Rules (CBPR) system (abbreviated as 'CBPRs' by APEC), which has been under development at least since 2007, after the APEC Privacy Framework was completed in 2005.[9] As outlined in this chapter, whether APEC CBPRs will, or should, have any long-term impact is still very uncertain. However, the proponents of APEC CBPRs present it as having a major role in the Asia-Pacific, and in transfers of personal data between Europe and the Asia-Pacific, so it needs to be examined in considerable detail.

2.1. Operation of APEC CBPRs

Official documentation of how the CBPR system is supposed to work is available on the CBPRs site.[10] The CBPRs System Documents section includes documents establishing the system, concerning APEC economy participation, and concerning

Accountability Agent participation.[11] The proposed operation of the system may be summarized as follows:

1. An APEC economy must first have 'laws and regulations…the enforcement of which have the effect of protecting personal information consistent with the APEC Privacy Framework,' to be able to participate in the APEC Cross-border Privacy Enforcement Arrangement (CPEA) (see Chapter 2, section 6.4), an organization of privacy enforcement authorities (PEAs).[12] The CBPRS Joint Oversight Panel (JOP), consisting of representatives of three economies with two-year terms,[13] issues a Findings Report on each application to participate. This is not a process by which an independent body makes a substantive determination that the economy does have a law meeting the **(p.532)** required APEC Framework standard. It is more like a requirement that the applicant economy puts forward a 'self-assessesment' that it does meet the required standard.[14]
2. A privacy enforcement authority (PEA) (a 'public body that is responsible for enforcing information Privacy Law, and that has powers to conduct investigations or pursue enforcement proceedings') from the APEC economy notifies the CPEA Administrators of its intention to participate in the CPEA, and provide information confirming its powers etc.[15] Similarly, the JOP does not make an independent substantive assessment that the proposed PEA does have the required powers; the economy concerned is in effect required to document a 'self-assessment' that it does have these powers.
3. A 'designated APEC government delegate' in the APEC economy informs APEC's ECSG of its intent to participate in the CBPR; that it has a PEA that is participating in the CPEA; and that it intends to appoint an Accountability Agent (AA).
4. An economy can nominate, or forward an application from, an organization in the economy concerned (or subject to its jurisdiction) to be an Accountability Agent (AA), to CBPR's Joint Oversight Panel (JOP). A PEA can also be nominated to be an AA. The application must provide details attested by the organization as to how it meets the Accountability Agent recognition criteria, and demonstrate how it will meet CBPR Program Requirements in assessing companies applying for certification, monitoring compliance by them and dealing with complaints against them.
5. The JOP conducts 'a review of the required documentation' to check that the AA recognition criteria appear to be met. The extent to which the JOP actively investigates whether the AA applicant does what it claims, or even whether the JOP is thorough enough in ensuring all recognition criteria are met, has been questioned by civil society organizations (see discussion of TRUSTe application later in this chapter). The JOP makes a recommendation for approval of the AA application to the APEC Electronic Commerce Steering Group (ECSG), and if no economy objects within a specified period of time it is considered approved.[16] The AA approval is only for one year, with re-application required annually according to the same process, except that the JOP is required to consider any complaints against the AA received from businesses, consumers, or others.[17] This process is also being tested in 2014 by a civil society organization in relation to TRUSTe's renewal.
6. The AA, once approved, may accept applications from companies within the jurisdiction of the economy from which it comes, to certify that those companies comply with the requirements of the CBPR system. This is only in relation to personal data 'that they have collected or received that is subject to cross-border transfer to other participating APEC economies'.[18] APEC CBPR does not apply to any other data held by a company, though they are 'encouraged' to apply the same company policies to it.[19] There is no CBPR mechanism for consumers to know whether particular items of their personal information fall within the 'subject to export' qualifying criterion.
(p.533) 7. The AA is to 'verify' an applicant company's self-certification of the compliance of its policies with the AA's programme requirements. The company's policies must be regarded as confidential by the AA. There is, therefore, no mechanism by which external parties can assess either before or after certification whether a company has accurately stated its policies in order to obtain certification. Complaints can only be made in individual cases about non-compliance with CBPR requirements.
8. CBPR certification does not change (or substitute for) a company's obligations to comply with all local legal requirements in the economy in which it is located.[20] In particular, any local restrictions on exports of personal data still apply.
9. The AA does not certify that the company complies with local data privacy laws of the economy concerned, only with its CBPR requirements[21] (which will often be lower). So a consumer cannot know if a CBPR-compliant company is in fact 'law abiding'.
10. An AA is required to investigate complaints made to it against a company it has certified, and to remove the certification of companies that fail to remedy breaches of the programme requirements within a reasonable time. The AA is required to refer a breach which has not been remedied in a reasonable time to an appropriate PEA 'so long as such failure to comply can be reasonably believed to be a violation of applicable law'.[22] This leaves considerable discretion to the AA. An AA is not required to have the ability to impose financial penalties on companies in breach,[23] and there is no requirement to be able to award compensation to consumers. Therefore, the only additional remedy that the CBPR offers consumers is that a company might have its certification removed or that a PEA might be asked to investigate a possible breach of a law.
11. AAs are required to 'release anonymised case notes ("on a selection of resolved complaints illustrating typical or significant interpretations and notable outcomes") and complaint statistics'.[24] None have yet been released. This transparency, if made effective,[25] could be a strong point of APEC CBPRs.
12. Discussions continue concerning extension of the application of the CBPR to processors in addition to controllers to whom it applies at present.[26]

2.2. Effect of CBPR certification on a company

Companies considering the business case for CBPR accreditation (with its attendant and ongoing costs) need to appreciate how

limited are the effects of being accredited by an AA: **(p.534)**

> (i) Certification only means that the company, in relation to its operations in one APEC economy, claims to deal with personal information it receives in accordance with the APEC Framework. But this only need apply to data it imports.
> (ii) Such certification has no effect on the same company in its operations in other APEC economies. Certification would need to be obtained separately in each country to which data was to be transferred.
> (iii) Certification does not in itself mean that personal data can be transferred from any other APEC economy. The law in each other economy must permit such transfers. At this stage, no laws in APEC economies clearly provide that exports to APEC CBPR-compliant companies are allowed.
> (iv) There is not, and will not be, any such thing as 'APEC wide' certifications allowing companies to receive information from any APEC economy. This would require the laws in all 21 APEC economies to allow such transfers. If such transfers are not prohibited under existing laws, then APEC certification adds nothing in relation to whether the data can legally be exported.[27]
> (v) For the same reasons, APEC CBPR certification cannot have any direct effect on the ability of companies to import personal data from countries outside APEC.
> (vi) As yet, there is no 'mutual recognition' or 'interoperability' of CBPR certification by regional organizations outside APEC, such as the EU. Any notion of full 'interoperability' with EU Binding Corporate Rules (BCRs) is illusory,[28] and partial consistency so as to reduce the paperwork in obtaining 'double certification' under both EU and APEC systems is the best that is likely to be achieved.[29] To the extent that this occurs, it may make the CBPRs more attractive.
> (vii) If a company is based in a country which already has a data privacy law that meets or exceeds the low standard of the APEC Privacy Framework, there should be no benefit to that company in obtaining CBPR certification.

Given the complexity and the essentially 'multi-bilateral' nature of the APEC CBPR processes, any company considering applying for certification would need to consider carefully both the business case (initial and ongoing annually) for certification, and the benefits to its customers. Potential certification customers are being given a very different, possibly misleading, message.[30]

2.3. Operation of APEC CBPRs to 2013

APEC CBPRs, like any other form of regulation, cannot simply be assumed to be credible and effective. In addition to its professed standards (considered in the previous section), the operation of the regulatory system in practice must be examined to determine whether it **(p.535)** credibly upholds and enforces those standards. APEC CBPRs is not yet in full operation, but the initial operation of any institution is often a major determinant of its future path, and so is examined here for APEC CBPRs.

By the end of 2013, three of the 21 APEC economies, including one in Asia, had reached different stages in becoming participants in the CBPR system. Announcements of each step in an economy's participation are on the CBPRs website.[31] The USA is the only applicant to have yet completed the process to be a participant, having completed to the satisfaction of the Joint Oversight Panel (JOP) the required documents (i) confirmation from its 'designated APEC government delegate' that it would be a participating economy, (ii) the appointment of a privacy enforcement authority (the Federal Trade Commission) which notifies its intent to participate in the APEC CPEA (Cross-border Privacy Enforcement Arrangement) system, and (iii) the nomination and approval of TRUSTe as an AA for the USA (June 2013). Mexico has confirmed that its data protection authority is a participant in the APEC CBPEA, and the JOP has made a positive Findings Report,[32] which steps are sufficient for it to be 'participating' even without an AA being approved.[33] Japan has done similarly, but it has nominated 16 PEAs because it does not have a single data protection authority,[34] and it has also not yet proposed any AAs.

The US company TRUSTe has been approved as an Accountability Agent for the USA by the JOP.[35] The civil society representative at the following APEC Data Privacy Subgroup meeting was very critical of what he saw as the JOP's 'rubber stamp' approval of TRUSTe's application:[36]

> It is unfortunate that it was left to civil society volunteers to question the JOP assessment of the TRUSTe application for recognition as an AA. We are pleased that a number of economies took up some elements of our critique. This appears to have led to some specific modifications to the application (and consequently to the JOP's report) but also to many assurances about future changes and TRUSTe practices, which the JOP has taken on trust. We consider that the changes and assurances (even if subsequently delivered) fail to address the most serious criticisms, and we cannot understand how the JOP, and member economies, can be satisfied that the application met the recognition criteria.
>
> International civil society believes that approval of TRUSTe as an Accountability Agent has seriously undermined the credibility of the CBPR system. It is a very unfortunate precedent, setting a low bar for other applicants for AA recognition both in the US and in other economies.

A civil society submission to the JOP[37] had argued that TRUSTe's application, which JOP had initially proposed to approve,[38] had many deficiencies, including that TRUSTe's **(p.536)** program standards/requirements, failed to meet at least 21 of APEC's programme requirements,[39] that it restricted monitoring and certification to online activity (whereas APEC criteria required all activity to be monitored and protected), that it failed to address questions of conflict of interest, that it was incomplete because some information was withheld as supposedly 'commercial in confidence', and that it proposed to hide APEC case notes or statistics in larger result sets. The JOP's final approval[40] required TRUSTe to address some of these criticisms, including monitoring non-online activities, and separating complaint reporting. It did not address the criticism that 21 programme

requirements were missing, except to require TRUSTe to post online TRUSTe's requirements and the JOP approval of them. TRUSTe's approval is only for one year. How the JOP handles the complaint that a civil society organization has made to it in 2014 concerning continuing and additional alleged breaches by TRUSTe will be a test of the credibility of CBPRs.

The significance of this description of the first AA approval process is not only that the civil society view that TRUSTe fails to meet APEC requirements to an extent exceeding what the JOP and what APEC member economies should accept. It is also that the only reason any of these issues (including those that the JOP required TRUSTe to address) came to light at all, is the coincidence that a civil society representative was part of one of the member economy delegations and obtained information in time to allow civil society to attempt to intervene in the initial AA approval procedure. There is no external or critical perspective built in to these CBPRs processes (except it is allowed in AA certification renewal). This first example does not indicate that any scrutiny will be provided by member economies. The TRUSTe approval as an AA calls into question whether a proposed AA's application could ever be refused by the JOP. If that is questionable, then what credibility can the whole CBPRs process have?

In 2013 three US companies were certified by TRUSTe as CBPR-compliant. No details of the basis of any of these certifications are available, and there is no requirement for there to be any opportunities for third party inputs. The responsible officer of the first company certified[41] described in an interview the certification process and stressed how little work was required on the company's part to obtain certification.[42] There is too little transparency and credibility in the CBPRs processes in their operation as yet.

2.4. Criticisms of APEC CBPRs

There will always be a ready supply of praise for APEC's CBPRs from companies with a commercial interest in being certified, or acting as AAs, and from economies that wish to attract personal data business. There are, however, very few critical voices, partly because very few people outside these circles have access, during CBPRs approval processes, to documents that allow critical views to be formed, and very few critical inputs are allowed.

The following criticisms may be made of the whole CBPR system:

1. A combination of CBPRs processes and standard APEC processes exclude any significant critical participation as of right, and often as of fact. There is no provision for external inputs into the key questions of (a) whether an economy's law does allow **(p.537)** enforcement of the APEC Privacy Framework, (b) whether a proposed PEA has powers to do this, and (c) whether there are substantial objections to a proposed AA approval. There are no procedures to invite written inputs, or even to make 'outsiders' aware in advance that decisions are being made (although this is predictable when annual AA renewals are required). Civil society organizations are refused attendance at APEC Privacy Sub-group meetings,[43] though their members may occasionally be present as part of an economy's delegation. Without any right of submission or attendance, decisions on these key matters occur without the inconvenience of a dissenting civil society voice, or other voices.[44]
2. The benefits to consumers of APEC CBPRs are very slight. It does not apply to all personal data held by a certified company, only that which is to be exported. Customers are not told which data this might be. The only 'remedy' an AA is required to provide is termination or suspension of a company's certification.
3. The CBPRs processes do have some transparency, but it is primarily in making available documents after decisions are made by JOP. There is no transparency concerning company applications for certification. The transparency of complaint processes remains to be demonstrated. To be fair, APEC processes are not alone, among international privacy bodies, in lacking sufficient transparency.
4. CBPRs only requires that companies certified under it meet the standard of the APEC Privacy Framework's 'OECD-Lite' Principles, including undisclosed company interpretations of the dangerous APEC 'harm', 'consent', and 'accountability' principles. It is arguable that this is too low a standard to be in the interests of consumers in APEC economies, or on which to base any 'interoperability' with European or other regional systems with higher standards.
5. CBPRs may develop in practice to be a series of 'mini safe harbours' between US companies and the non-US countries that decide to accept APEC CBPR as an acceptable basis for data exports from companies in their countries to US companies (often, to US-based cloud service providers). Will APEC CBPR's predominant purpose be to allow data transfers from willing APEC countries to US-based certified companies, despite US privacy laws having such limited scope?
6. The only example of a similar scheme in operation is the US-EU 'Safe Harbor' scheme, which has been 'put on probation' by the European Commission because of multiple failures,[45] and its future is uncertain. TRUSTe provides an EU Safe Harbor certification mark under the scheme, but along with other trustmark providers it is alleged to have failed to ensure that certified companies are actually complying with the Safe Harbor requirements. In 2013 more than 400 complaints were sent to the US Federal trade commission regarding 'false claims' of Safe Harbor membership. More than 25 per cent of these false claims had links with trustmark providers.[46] The US Federal Trade Commission is taking enforcement steps in relation to some of these complaints,[47] and a number of consent agreements have been made as a result of **(p.538)** breaches.[48] The reasons for failure of 'Safe Harbor' processes, and the parties responsible for them, need to be examined for their implications for APEC CBPRs, but that is beyond the scope of this work.
7. It is difficult to see why any non-US APEC countries that have their own data privacy laws will find any use in CBPRs to obtain data transfers to their countries, when they can rely on the protection provided by their own laws (unless data import exemptions apply). It is also questionable whether there are any APEC member countries without extensive data

privacy laws for their private sectors that would have companies with significant needs for personal data imports.

There are two overall themes in the above criticisms. The first is to question the transparency and credibility of the CBPRs processes, in the absence of any inbuilt critical input. The second is to ask whether the overriding function of CBPRs will be to protect personal data exports to the USA, while offering consumers in Asian countries no protection of value in return.

APEC CBPRs is part of a larger global agenda. The USA and its allies may aim for 'interoperability' of APEC CBPRs with non-APEC countries and regional blocs (including those in Asia, as well as Europe and elsewhere), to overcome the problems of data export restrictions in other countries' laws. This could be done via negotiated agreements with blocs like the EU, or by requiring this as part of free trade agreements, perhaps including use of the 2013 OECD Guidelines in non-OECD countries (see section 3.1 of this chapter).

3. Changes to existing international data privacy instruments

The revision of the OECD Privacy Guidelines was completed in 2013. The revisions of the Council of Europe Data Protection Convention 108 and the EU Data Protection Directive remain unfinished. These revisions all have major implications for the future of data privacy developments in Asia.

3.1. Revised OECD privacy Guidelines 2013

From 2011–13 an expert group including non-government experts, convened by the OECD's Working Party on Information Security and Privacy (WPISP), and chaired by Canada's Privacy Commissioner, considered the revision of the Guidelines and prepared a report.[49] 'On the basis of the work by the expert group, proposed revisions were developed by the WPISP and approved by the Committee for Information, Computer and Communications Policy (ICCP), before final adoption by the OECD Council'[50] of the 2013 Guidelines and Supplementary Explanatory Memorandum.[51] The final revisions were therefore a matter of intergovernmental negotiation, and matters on which the expert group had little **(p.539)** say. Last-minute changes to both the Guidelines and the Memorandum, which weakened them substantially, were such that one of the expert group members has described it as a 'procedural hijack'.[52]

The revised Guidelines do not change the core 'Principles of National Application' at all from the 1980 version (see Chapter 2, section 3.1). All OECD members, except Turkey and the USA in relation to its private sector, have implemented the 1980 Guidelines in legislation. What is the point of the 2013 revision if all it does is preserve a standard that almost every OECD member exceeds? What is its relevance to Asia, given that there are only two OECD members in Asia (South Korea and Japan)? One answer is that the 2013 Guidelines are aimed at least as much at countries that are not (or not yet) OECD members, arguably with a result that can be used to limit the extent that they can implement restrictions on data exports. Along with other new weaknesses, there are also some improvements to the Guidelines, relevant to both OECD members and non-members. These changes are now explained.

The (non-revised) OECD principles—'Let's do the time warp, again'

The Expert Group proposed that the eight Basic Principles of National Application in the 1981 Guidelines should be unchanged (as they were), not because they were regarded by participants as satisfactory, but because 'no clear direction emerged as to what changes might be needed', meaning that there was no possibility of obtaining consensus within the expert group.[53] The OECD's Privacy Principles therefore remain frozen at 1981 levels, as if nothing (including the EU Data Protection Directive) had occurred in the intervening 32 years. Even though this may have been strategically necessary, in order to salvage even the 1981 Principles, this result ignores the fact that the overwhelming majority of the 101 data privacy laws enacted globally by 2013 embody considerably higher data privacy standards than the 1981 (and now 2013) Guidelines.[54] The Privacy Principles in the OECD Guidelines now represent little more than the maximum that the USA will accept in an international agreement. Meanwhile, the USA continues to fail to enact its own comprehensive data protection law. Even the idea that there should be some time limit on how long personal data is held was deferred by the OECD for further study,[55] despite being a common feature of almost all data privacy laws for the last 30 years.[56]

Stronger aspects of the 2013 Guidelines

The 2013 Guidelines are in some important respects stronger than the 1981 Guidelines, particularly in relation to enforcement. A new Part Three, 'Implementing Accountability', recommends inclusion of a 'privacy management programme' with specific requirements, **(p.540)** including that data controllers must be prepared to demonstrate the programme, particularly to enforcement bodies. Mandatory data security breach notification is also required, to enforcement authorities, and to data subjects where they are likely to be affected. These changes can be seen as reinforcing the OECD's 'accountability' principle and 'security' principles, and also as strengthening enforcement. The inclusion of these two principles in the 2013 Guidelines makes it easier to argue that these principles are now part of the normal global standards for data privacy laws.

The 2013 Guidelines add recommendations that countries should establish 'privacy enforcement authorities' with sufficient resources and expertise to exercise their powers effectively and make impartial decisions (but without requiring 'independence'). It is also recommended that countries should 'make public the details of their observance' of the Guidelines and 'encourage the development of internationally comparable metrics'. The explanatory materials clarify that this includes publication of complaint statistics and similar matters than can improve policy-making, particularly if done in internationally consistent fashion.[57] This is a valuable inclusion.

'Globalization' of the OECD Guidelines—a global weakening of data export restrictions?

The 1981 Guidelines could be adopted only by OECD member countries, and they only attempted to regulate relationships between OECD members, a small group of economically advanced countries. The 2013 Recommendation by the Council 'invites non-Members to adhere to this Recommendation and to collaborate with Member countries in its implementation across borders'. Given this Recommendation, it would seem that any references to a 'Member country' in the text of the Guidelines should be read as a reference to 'an adhering country' whether or not a member, otherwise adherence would mean nothing.[58] Thus any country, including the 25 non-members of the OECD in Asia, can now adhere to the Guidelines by a simple declaration. This is the first sense in which the Guidelines have been 'globalized'. It may mean that the OECD Guidelines will now be promoted as one of the alternative global privacy standards. This is beneficial insofar as it functions to encourage countries without data privacy laws to adopt such laws to a consistent minimum standard.

However, the potential danger in this development is that the 2013 Guidelines attempt, though a series of subtle steps, to limit the extent to which any countries that endorse the Guidelines (whether OECD members or not) can then impose limitations on data exports to any other countries. At the same time, these steps also convert what was previously a 'minimum standards' agreement into something closer to 'maximum standards' in relation to data export restrictions.

Once a country (OECD member or not) has adhered to the 2013 Guidelines, the 'Basic Principles of International Application' require that an adhering country 'should refrain from restricting transborder flows of personal data between itself and another country' where one of two conditions are met. The reference to 'another country' (meaning any other country in the world) is in itself a major change, because the 1981 Guidelines only imposed restrictions on data flows between member countries, leaving OECD countries **(p.541)** free to do what they liked in relation to other countries. This is the second sense in which the 2013 OECD Guidelines are 'globalized'.

There are two conditions (in Article 17) that may prevent any further restriction of data exports, if either is satisfied by any other country which has announced its adherence to the Guidelines. They are: '(a) the other country substantially observes these Guidelines' (but that 'observance' need not, according to the Guidelines, be by legislation) or '(b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines'. Requirement (b) in effect rules out any export restricts based solely on the destination of a data export, and requires that other types of safeguards (e.g. binding corporate rules, standard contract clauses) must be allowed. This is not necessarily very different from what is required by Article 26 of the EU Data Protection Directive (or the revised Convention 108). The important thing is that it will apply to any country adhering to the Guidelines.

A difficult question, on which they Guidelines are ambiguous,[59] is whether adhering countries can impose conditions on data exports where they consider special protection is needed, such as in relation to classes of sensitive data, or exports for the purpose of particularly sensitive types of processing. If the restrictive interpretation is correct (which is not certain), the upshot of these changes is that any country adhering to the Guidelines (OECD member or not) must allow data exports to any other country adhering to the Guidelines (OECD member or not) on the basis set out in Article 17, and no more restrictive than that.

None of these aspects of 'globalization' of the Guidelines are mentioned in the Supplementary Explanatory Memorandum, and are generally not remarked upon by commentators. Their significance has not been recognized.

Other changes that weaken the Guidelines

The 1981 Guidelines required members to 'take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a member country, are uninterrupted and secure'. This is now completely removed from the 2013 Guidelines, which in light of the Snowden revelations (see section 1.1 of this chapter) is a very convenient result for the USA, UK, and some other governments, and a very poor result for other countries and their citizens.

Although the 2013 Guidelines say explicitly that member countries 'should…adopt laws protecting privacy', this is not as straightforward as it sounds. It is arguable that the Guidelines, as a whole, weaken the importance of implementation by legislation, in favour of non-legislative approaches.[60] However, these are only non-binding Guidelines, so it is **(p.542)** also possible that legal hair-splitting about terminology is less important than the apparent encouragement of legislation.

The future significance of the OECD Guidelines in Asia

The various changes to the 2013 Guidelines that strengthen them, may have a unifying effect on both new laws and reform of existing laws, just as the 1980 Guidelines have had, in helping to create the minimum standards largely common to privacy laws across the world. Data breach notification and accountability requirements on data controllers will probably become more prevalent. However, just as the 1980 Guidelines did not result in much uniformity in approaches to data exports, the effect of the ambiguous export provisions in the 2013 Guidelines is equally uncertain. 'Improving interoperability among privacy frameworks' has effectively become a goal of the Guidelines through inclusion in its recitals, as well as being one of the guidelines,[61] giving a clear indication of the agenda of some OECD members, most clearly the USA. The overall result is that the OECD Guidelines will continue to play a role, but an increasingly political one, as the flagship for a lower global standard of privacy protection. Comparing the 2013 Guidelines with the view that the proposed EU Regulation will be the new 'gold standard' for global privacy, one proponent described the Guidelines as 'a more modest and probably more realistic avenue in a globalized world',[62] but that is not a universal view, nor one I share.

3.2. 'Globalization' and 'modernization' of CoE Convention 108

The Council of Europe (CoE) Data Protection Convention 108[63] and its Additional Protocol have not been of direct importance in Asia until now, but have played an indirect role in establishing both the 'basic' and 'European' standards for data privacy principles (see Chapter 2, section 3.2, and Chapter 3). However, they are now being 'globalized', or opened to accession by non-European countries that meet the standards of the Convention, including Asian countries. They are also being 'modernized', at the same time as the EU is making efforts to strengthen the Directive (perhaps by a Regulation). This section examines both developments, and their implications for Asian countries.

'Globalization' of CoE Convention 108

Since 1981, Article 23(1) of CoE Convention 108 has provided for accession by states outside Europe,[64] but the Committee of Ministers had not invited any state to accede for **(p.543)** the first 25 years of the Convention's life.[65] After some prompting by the international data protection commissioners,[66] since 2008 the CoE has actively sought non-European accessions[67] and attempted to explain its advantages. In 2011, the CoE Secretariat published a very short and formal description of the accession process (the 2011 'Note').[68] Uruguay and Morocco were the first non-European countries to apply to accede. Uruguay has completed all requirements and formally became a party to the Convention in October 2013. Morocco has not yet completed all requirements. These first two examples of the accession process are reasonably transparent (more so than APEC CBPR or EU 'adequacy' processes') and adhere to the standards of the Convention. They provide a guide to other non-European countries that maybe interested in acceding.[69]

Advantages and disadvantages of accession for Asian countries and citizens

There are significant potential advantages for Asian countries (and other non-European states) in acceding to Convention 108 and the Additional Protocol. These fall into three categories. In relation to EU countries, non-European states obtain a guarantee of free flow of personal data from the EU country (unless the EU country derogates from Convention 108 on that point). An adequacy finding from the EU under the Directive does not give them this. Because Convention 108 already has 46 existing ratifications, the advantages are significant from the outset. While Convention 108 accession will not automatically lead to a finding of 'adequacy' by the EU, it is hard to see the EU denying a finding of adequacy to a non-European state that accedes to the Additional Protocol as well as the Convention.[70] In relation to other non-EU countries that are parties to the Convention, mutual obligations of free flow of personal data arise between them, unless either derogates because of the other's lack of a data export restriction. The principal advantage of accession, therefore, is a guarantee of free flow of personal data from 46 EU and other European parties, and from any other non-European parties that accede.

Then there are more general advantages: it is only a modest step towards a stronger international data protection regime, not a radical one; it involves voluntary acceptance as an equal party to a treaty of obligations concerning data, rather than what might be seen as the unilateral imposition of a standard by the EU; the Cybercrime Convention shows that it is not unprecedented for a global treaty to emerge from Europe; and it avoids the necessity **(p.544)** for individual countries to make decisions about which other countries have privacy laws that are 'adequate' or 'sufficient' to allow personal data exports to them. Depending on how long it takes the Committee of Ministers to make decisions, and whether those decisions are perceived to be fair and not unduly political, it could be a more attractive process than applying for an 'adequacy' finding to the EU Commission, and sufficient in practice even though not technically a substitute for that.

However, there are also potential downsides for Asian countries, and their citizens, in accession. The principal one is that being a party to the Convention involves a commitment that personal data exports to other member states will not be prevented. Is every existing CoE member a safe destination for personal data exports? Will the CoE continue to insist on high standards for new members? Also, all other member states are obliged to have laws which protect the data of foreigners that are exported there, but can these protections be enforced? In all probability, cross-border enforcement cooperation between privacy enforcement authorities (PEAs) will be of some value. Enforcement by one state against another is of no value to individual data subjects. Citizens of European states can (indirectly) take actions to enforce their rights in another European state in the European Court of Human Rights,[71] but non-Europeans do not have an equivalent enforcement avenue. The 'modernization' process (next discussed) is also considering how to improve enforceability of Convention obligations.

These are the same problems as are found with any agreement that aims to achieve free flow of personal data in return for an agreed minimum level of protection. Comparisons with how citizens of Asian countries could protect themselves under the OECD Guidelines or the APEC CBPRs are legitimate, but are not likely to leave CoE Convention 108 worse for the comparison, particularly since the standard of protection it is attempting to provide is inherently higher than that of the OECD or APEC with their outdated 1980s standards.

The 'modernization' process

The Convention and Additional Protocol are undergoing revision (referred to as 'modernization'). In November 2012, the Consultative Committee of the Convention submitted its final proposals[72] for 'modernization' of the Convention[73] to the Committee of Ministers for amendment or adoption.[74] A draft Explanatory Report, to be prepared by the Convention 108 Bureau, is not yet available publicly. Three general observations can be made about the proposals. First, many changes will make the 'globalization' of Convention 108 more effective, both in terms of the procedures for accession of new members, and in terms of providing post-accession mechanisms to ensure that the Convention is in fact being **(p.545)** complied with by the parties to it. This is particularly so with the provisions that, in effect, absorb the Additional Protocol into the Convention (requiring a data protection authority (DPA), data export restrictions, and access to the courts), so that it is not possible to

accede to one without also acceding to the other. Second, some aspects of the proposals will help the Convention 'keep pace' with stronger provisions likely to be included in the proposed EU Regulation. Third, it will become clearer that the standards required for a non-European country to accede to the Convention differ from those by which the EU assesses the 'adequacy' of a non-EU country's data protection provisions. That being said, it remains unclear whether 'adequacy' is a suitable standard by which to measure data export restrictions.

Strengthened content of the Convention

The Consultative Committee's proposed changes to the Convention can only be summarized here, but detailed analysis is elsewhere available.[75] Significant proposed changes to the Convention's existing standards (see Chapter 2, section 3.4) include expanded categories of sensitive data; data breach notification requirements; and rights concerning automated processing. Many aspects of enforcement are proposed to be strengthened: privacy enforcement authorities must assist complainants no matter where they reside (very relevant to Asian accessions); verifiable 'accountability'; risk analysis of intended data processing (including 'privacy by design' and 'privacy by default' principles); and protections modifiable to accommodate the level of risk. The data protection principles proposed for the revised Convention are therefore considerably stronger than those in the 2013 OECD Guidelines, but sharing some of their stronger enforcement aspects. They may end up being comparable to those in the proposed EU Regulation (discussed in section 3.3 of this chapter).

Data export restrictions: 'modernization' at risk

The guarantee of free flow of personal data between its parties which, the Convention provides, is only justifiable if it is coupled with an obligation on parties not to export personal data to organizations in non-party states, unless the protection of privacy continues to be guaranteed. As elsewhere, data export provisions have been the most contentious aspect of the Consultative Committee's recommendations.[76] The Additional Protocol to the existing Convention requires that data exports ('transfers') can only be allowed if 'an adequate level of protection' is provided. In 2012 the Consultative Committee was adhering to 'adequacy' as the touchstone for export limitations.[77] However, its final proposals refer instead to 'an appropriate level of personal data protection based on the principles of the Convention' and it is uncertain whether the Explanatory Report will add clarity to this. There are strong reasons to consider 'appropriate' protection to be an unsafe term, at least from the perspective of the data subject's interests.[78]

(p.546) Asian countries and the 'modernized' Convention

In the modernized Convention, the Consultative Committee proposes that the Committee of Ministers will only invite accessions after obtaining the Committee's Opinion. The Committee has made proposals dealing with the evaluation of candidates for accession, periodic evaluations of all parties' compliance with the Convention, and the measures that should be taken in event of non-compliance.[79] All of these are important to Asian countries considering accession. The evaluations of both candidates and compliance would be carried out by a committee of probably six members of the Consultative Committee.[80] An open process is proposed, very different from EU 'adequacy' evaluations,[81] to increase confidence in the quality of the Convention and its processes.

3.3. Proposed EU reforms and 'third generation' principles

The EU has, since 2011, been considering proposals from the Commission to reform the Data Protection Directive, possibly by replacing it with a Regulation. The main point that needs to be made about the proposals for this study is that there is no indication that the EU is proposing to reduce its standards on any significant issues. While the timing and content of the reform is still very uncertain, there is little to be gained from lengthy discussion here. However, if anything resembling the content of the drafts under discussion is included, this will constitute (in conjunction with a 'modernized' CoE Convention 108), a 'third generation' of data privacy principles. At least 15 new elements can be identified as possible components of such enhanced principles:[82] more explicit consent (opt-in) requirements, and obligations to prove same; more explicit requirements of data minimization at collection; a 'right to be forgotten', possibly including obligations on intermediaries to inform third parties; a right to data portability, including a right to obtain a copy of personal data in a portable format; regulation of automated 'profiling'; demonstrable implementation of privacy principles (stronger 'accountability'); implementation 'by design'; implementation 'by default'; liability of local European representatives of a processor; mandatory data breach notification; the ability to require privacy impact assessments; data protection officers required; more specific requirements in relation to data exports; EU rules to apply to extraterritorial offering of goods, services, or monitoring; and a right to online subject access. Some of these elements are already found in some Asian data privacy laws, as discussed in Chapter 17.

The enforcement provisions after reform of the Directive may also set a much stronger standard. If it is a Regulation, not a Directive, that means that the same law will apply in all EU member states, not that the laws of EU member states will have to be modified to **(p.547)** approximate to a standard (as with a Directive). Other reforms may include a 'lead DPA' in the state in which a company has its headquarters, required to consult about penalties with the EU Data Protection Board (successor to the Article 29 Working Party), and fines for breaches of the Regulation of 2 per cent or more of a company's 'annual worldwide turnover'. Any reforms such as these are likely to influence developments in countries outside Europe.

4. Other possible sources of international agreements and standards

There are other 'known unknowns' in the international arena which could have significant effects on the development of data privacy in coming years. These include the involvement of the United Nations, and the role of trade and intellectual property treaties. The other, somewhat unlikely, element is the possibility of a change of domestic law in the USA.

4.1. Proposals for UN initiatives concerning data privacy

The United Nations has until now, only been a minor participant in international data privacy developments, with its most relevant engagements being the 1989 'General Comment no. 16' on Article 17 of the International Covenant on Civil and Political Rights 1966 (ICCPR) by the Human Rights Committee (see Chapter 2, section 4.1) and the 1990 General Assembly Guidelines (see Chapter 2, section 3.5). Prospects for its greater involvement have increased but should not be exaggerated. However, in 2013 there were two developments.

New ICCPR Article 17 protocol proposed by the ICDPPC

The International Conference of Data Protection and Privacy Commissioners (ICDPPC) has, in recent years, passed a series of resolutions at its annual meetings in favour of development of a new international data privacy treaty, preferably one based on their own 'Madrid Declaration'.[83] At the 35th Conference in Warsaw (September, 2013) the ICDPPC, clearly influenced by the Snowden revelations, resolved:[84]

> to call upon governments to advocate the adoption of an additional protocol to Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which should be based on the standards that have been developed and endorsed by the International Conference and the provisions in General Comment No. 16 to the Covenant [of the UNHRC] in order to create globally applicable standards for data protection and the protection of privacy in accordance with the rule of law.

The USA's FTC abstained.[85] The resolution noted the existence of CoE Convention 108, but refrained from endorsing it as the desirable global instrument.

(p.548) The UN Resolution concerning state surveillance

Closely related to the above proposal is the UN General Assembly resolution 'The right to privacy in the digital age',[86] passed by consensus in response to the Snowden revelations. This is the first time that the UN General Assembly has paid serious attention to privacy issues since it passed its 1990 Guidelines (see Chapter 2, section 3.5). After amendments to obtain consensus adoption, the resolution was relatively mild, primarily affirming that rights that exist in the offline context also exist online. It does reaffirm that the right to privacy in ICCPR Article 17 exists in part because 'the exercise of the right to privacy is important for the realization of the right to freedom of expression and to hold opinions without interference, and one of the foundations of a democratic society'. The resolution also requests the UN High Commissioner for Human Rights (UNHCHR) to prepare a report on the protection of privacy in the context of 'mass scale' domestic and extraterritorial data surveillance and interception, with recommendations.

Privacy as a human right is therefore likely to remain on the UN agenda for the moment, but it is difficult to see a concrete result emerging, unless the UNHCHR picks up the ICDPPC proposal to develop a new protocol under Article 17 of the ICCPR. Article 17 improvements would seem to be within the remit of the UNHCHR and the terms of the resolution.

4.2. Free trade and intellectual property agreements

Some countries are attempting to use free trade agreements as a means of nullifying the effectiveness of national laws limiting exports of personal data, but as yet it has not worked, the European Union has confirmed that it will not include data protection issues in trade negotiations with the USA.[87] India has also been attempting to include what it calls 'data secure status', meaning 'a finding of adequacy', in trade negotiations with the EU, but without success (see Chapter 15).

If countries continue to enact laws requiring personal data to be stored on local servers (see section 1.1 of this chapter), this could trigger actions under trade agreements by cloud service providers, or host countries such as the USA, on the basis that this constitutes a disguised restriction on trade in services contrary to GATS (see Chapter 2, section 5.1). In EU–US trade negotiations the USA is reported to have proposed prohibition of requirements in EU countries for local data storage.[88]

4.3. The USA and the forgotten 'Consumer Privacy Bill of Rights'

If the USA did enact national legislation concerning data privacy, its economic and political power would make that law equivalent to an international standard, and give more meaning to the notion of 'interoperability'. But there is little sign that this will occur. The Obama administration 'Framework' initiative,[89] including the 'Consumer Privacy Bill of **(p.549)** Rights' (CPBR), announced in early 2012, appeared to represent a new level of serious consideration of privacy protection by a US Administration. The CPBR, compared against the OECD privacy Guidelines, was good on the less important privacy principles, but defective on all the key elements.[90] Since its release in February 2012, little has been heard of the CPBR. It has been reported that 'the Obama administration has been working on legislation to boost online privacy safeguards for consumers' in 2013, but the reports have no more substance than statements that the administration is trying to build support in Congress for measures that are not finalized.[91] Other parts of the administration continue to add to calls for legislation, such as a 2013 report by the Government Accountability Office (GAO) which concluded that there ought to be a 'comprehensive federal law governing the collection, use and sale of personal information by information resellers'.[92] In addition, the extent of constitutional limitations on the scope of data privacy laws in the USA is not yet settled, but they may be significant.[93]

As in the past three decades, it seems that for the near future, the key element of US personal information policy will be negative: to prevent the constantly increasing number of countries that do have data privacy laws from applying those laws to prevent exports of personal data to the USA. The fact is that the USA has no comprehensive data privacy laws of its own, and provides inadequate protection to foreigners' personal data, just as it does to the personal data of its own citizens. The problem

is exacerbated by the increasing worldwide distrust of what both US government agencies and US companies (particularly those involved in social media) do with personal data that comes within their reach.

5. Conclusions

Few conclusions may be drawn from this chapter's survey of new developments in international instruments and standards, other than to observe the strengthening of some standards, and the likelihood of continuing conflict between competing standards.

5.1. The strengthening of privacy standards

As Part II of this book has shown, the privacy principles in domestic laws in Asia are strengthening in almost all jurisdictions within recent years. Within a few years, it seems that the privacy principles of both the EU and CoE will also be stronger, but to an uncertain extent. Although there is no indication that the APEC Privacy Framework will change, even the 2013 OECD Guidelines have some significant additional requirements in relation to data breach notification and 'privacy management programmes'. Global privacy principles are becoming stronger, but at different speeds. The European standards will also strengthen in relation to enforcement measures, as have the OECD Guidelines, but much more so.

(p.550) ### 5.2. Five prospects for a global (or regional) data privacy agreement

Although domestic privacy standards, and enforcement mechanisms continue to strengthen, no resolution has been found to the issues around data exports. The combination of the much greater increase in demand for mobility of personal data, and the continuing increase in the number of countries with data privacy laws, almost all of which have some provisions restricting data exports, means that a uniform global approach (or even a regional approach) to data export issues becomes more desirable over time. There are five alternatives that deserve mention, though none seems likely to provide an answer in the short term:

(i) *A regional treaty (not possible)*—In Asia, one answer which is not on the table is a regional agreement for a data privacy standard, such as exists within Europe and is under consideration by the African Union (and already present in the Economic Community of West African States (ECOWAS) sub-region). As discussed in Chapter 2, there is no 'Asian Union', and even within the Association of Southeast Asian Nations (ASEAN) sub-region such a development is not possible. APEC's Privacy Framework is non-binding and that will not change (see Chapter 2, section 3.3), and at sub-regional levels the same can be said of ASEAN and the South Asian Association for Regional Cooperation (SAARC) (see Chapter 2, section 2). There is no likelihood of even APEC wide adoption of CBPRs (section 2 of this chapter).

(ii) *'Globalization' of CoE Convention 108*—The mechanisms for Asian and other non-European countries to accede to Convention 108 are now functioning (section 3.2 of this chapter), albeit slowly. There are both advantages and disadvantages in accession. The advantages to European countries in the success of globalization to include non-European parties are also substantial.[94] The prospects for Convention 108 becoming a 'global' agreement, at least to the extent of including a substantial proportion of significant countries both within and outside Europe, could be reasonable in the medium term, but only if the CoE becomes more adept at promoting membership, and perhaps only if the EU decides to support the idea. Because it has 46 existing members, all economically developed countries, there are immediate benefits to any new members, so it is not starting from scratch. But the process of accession requires a serious commitment.

(iii) *'Globalization' of the 2013 OECD Guidelines*—In contrast to accession to CoE Convention 108, any country can simply announce that it will adhere to the 2013 OECD Guidelines, but there are no specific advantages which arise from doing so, because the obligations arising from adherence apply to all other countries with which it deals. Any advantages flow simply from the adherence of others, not from its own adherence. Nevertheless, in a contest for global influence, there is likely to be some contest for membership, and a possibility that the USA will promote OECD adherence, because that will advance its own interests, and may reduce the likelihood of CoE Convention 108 becoming more of a global standard.

(iv) *A UN treaty (remains unlikely)*—Another alternative is a new global treaty, built from scratch under the auspices of the UN. Such an approach, although called for by the international conference of data protection authorities,[95] is not realistic, both **(p.551)** because such a UN process would take many years, and because there is no possibility of agreement concerning standards.[96] There are occasional academic calls for such a treaty, with one version proposing the UN Guidelines of 1990 as a starting point, with 'only' a new UN institution to be added to it, and for a treaty to emerge from a process of successive amendments of the Guidelines.[97] The addition of a new Protocol to the ICCPR might prove more feasible.

(v) *'Interoperability' between 'Frameworks'*—The EU and APEC are attempting to 'map' APEC's CBPRs with the EU's BCRs, to determine what commonalities they have, and what differences. The Article 29 Working Party *Opinion 02/2014* has shown that the differences are considerable. The US approach of 'interoperability' between these different 'Frameworks', with each accepting the standards and procedures of the other as sufficient to allow data exports, is an unrealistic goal. On the other hand, agreements between Europe and the ECOWAS bloc in West Africa, or the MERCOSUR countries in Latin America, if they were to occur, might create 'interoperability' at a higher 'European' standard, and place this issue in a different perspective. An undue focus solely on EU–APEC relations may be distorting.

Notes:

([1]) One of the most convenient and authoritative collections of information is *The Guardian*'s 'The NSA Files' <http://www.theguardian.com/world/the-nsa-files>.

([2]) *The Guardian*'s 'The NSA Files', section 'The story in a nutshell'.

([3]) 'Sun on privacy: Get over it' (*Wired*, 26 January 1999) <http://www.wired.com/politics/law/news/1999/01/17538>.

([4]) Regulation concerning Electronic System and Transaction Operation (Regulation 82 of 2012, Indonesia): art. 17(2) says: 'Electronic System Operators for the public service is obligated to put the data center and disaster recovery centre in Indonesian territory for the purpose of law enforcement, protection, and enforcement of national sovereignty to the data of its citizens.' Further regulations may be made under art. 17(2).

([5]) UNCTAD, *Information Economy Report 2013—The Cloud Economy and Developing Countries* (UNCTAD, 3 December 2013), pp. 58–60 <http://unctad.org/en/PublicationsLibrary/ier2013_en.pdf >. (See also the draft bill in South Korea: Bill for the development of cloud computing and protection of users.)

([6]) See Chapter V, UNCTAD, *Information Economy Report 2013.*

([7]) UNCTAD, *Information Economy Report 2013*, p. 68.

([8]) UNCTAD, *Information Economy Report 2013*, p.76.

([9]) Graham Greenleaf, 'Five Years of the APEC Privacy Framework: Failure or Promise?' (2009) 25 *Computer Law & Security Report*, pt. 6 'Cross-Border Privacy Rules (CBPR) and the "Pathfinders"', <http://ssrn.com/abstract=2022907>.

([10]) CBPRs website <http://www.cbprs.org/default.aspx>. CBPRs documents were previously on APEC's Electronic Commerce Steering Group (ECSG) website, <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.aspx>; under 'Cross-Border Privacy Rules (CBPR)'.

([11]) These documents are on the CBPRs site at 'Cross Border Privacy Rules System' <http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx>.

([12]) 'A PE Authority is any public body that is responsible for enforcing information Privacy Law, and that has powers to conduct investigations or pursue enforcement proceedings. It can be a national or sub-national authority. "Privacy Law" is defined in the CPEA as the laws and regulations of an APEC economy, the enforcement of which have the effect of protecting personal information consistent with the APEC Privacy Framework': *CPEA Fact Sheet*.

([13]) See JOP 'Charter' and 'Protocols' in CBPRs System Documents.

([14]) See the JOP Findings concerning the USA (2012) and Mexico (2013), in CBPRs System Documents.

([15]) See Chapter 2, section 6.4 for details. The CPEA website is at <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx> and details of the CPEA arrangements are at <http://aimp.apec.org/Documents/2010/ECSG/DPS1/10_ecsg_dps1_013.pdf>.

([16]) *APEC CBPR System—Policies, Rules and Guidelines* (APEC, undated), para. 33.

([17]) *APEC CBPR System—Policies, Rules and Guidelines* (APEC, undated), para. 37.

([18]) *APEC CBPR System—Policies, Rules and Guidelines* (APEC, undated), para. 8.

([19]) *APEC CBPR System—Policies, Rules and Guidelines* (APEC, undated), para. 8, fn. 10.

([20]) *APEC CBPR System—Policies, Rules and Guidelines* (APEC, undated), para. 43.

([21]) *APEC CBPR System—Policies, Rules and Guidelines* (APEC, undated), para. 45.

([22]) *APEC Accountability Agent Recognition Criteria* (APEC, undated), criterion 14.

([23]) JOP determination of TRUSTe AA application, 2013.

([24]) *APEC CBPR System—Policies, Rules and Guidelines* (APEC, undated), p. 15; *APEC Accountability Agent Recognition Criteria* (APEC, undated), criteria 10(g) and 10(h).

([25]) APEC's JOP initially agreed to allow TRUSTe to publish statistics on larger sets of data, not only APEC-related complaints, which would have 'buried' the APEC data. After criticisms from civil society organizations, they reversed this: APEC CBPRs JOP 'Recommendation Report on APEC Recognition of TRUSTe' (JOP, 18 June 2013), pp. 15–16.

([26]) Nigel Waters, 'APEC Cross Border Privacy Rules System Awaits Final Component' (Privacy International, 5 March 2013) <https://www.privacyinternational.org/blog/apec-cross-border-privacy-rules-system-awaits-final-component>.

([27]) *APEC CBPR System—Policies, Rules and Guidelines* (APEC, undated), para. 43 states that 'the CBPR System is intended to

provide a minimum level of protection', and it could do so by providing some protection in the importing country to consumers from the exporting country.

([28]) Put very briefly, one reason is that the EU's Binding Corporate Rules (BCRs) are solely about intra-company transfers of data, whereas APEC's CBPRs is primarily about inter-company transfers of data (but can also be used intra-company). In the EU, Standard Contract Clauses (SCCs) are used for inter-company transfers.

([29]) *Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross-Border Privacy Rules submitted to APEC CBPR Accountability Agents* (Article 29 Working Party, 28 February 2014) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp212_en.pdf>.

([30]) Statements are made promoting APEC CBPR to companies such as 'For unrestricted flow of personal information across borders while establishing meaningful protection by your customers, TRUSTe is your APEC endorsed, data privacy solution' <http://www.truste.com/products-and-services/enterprise-privacy/apec-accountability>.

([31]) 'News' (CBPRS, undated) <http://www.cbprs.org/GeneralPages/LatestNews.aspx>.

([32]) JOP Findings Report regarding Mexico's intent to participate in the CBPR system (16 January 2013) <https://cbprs.blob.core.windows.net/files/JOP%20Findings%20Report%20-%20MEXICO.pdf>.

([33]) 'About the APEC CBPR system' (CBPRs, undated) <http://www.cbprs.org/GeneralPages/About.aspx>.

([34]) JOP Findings Report regarding Japan's intent to participate in the CBPR system (25 April 2014) <https://cbprs.blob.core.windows.net/files/Japan_Final_Report.pdf>.

([35]) CBPRs JOP, 'Recommendation Report on APEC Recognition of TRUSTe' (JOP, 19 February 2013, as amended 18 June 2013); see also other documents concerning appointment of TRUSTe as Accountability Agent (APEC ECSG, 2013) <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.aspx>; Other documents included are; 'TRUSTe—Annex B: Accountability Agent Recognition Criteria Checklist'; and 'TRUSTe—Annex C: APEC Cross-border Privacy Rules System Program Requirements Map'.

([36]) Nigel Waters, 'The APEC Cross Border Privacy Rules System: A Civil Society Perspective' (Privacy International, 6 July 2013) <https://www.privacyinternational.org/blasts/the-apec-cross-border-privacy-rules-system-a-civil-society-perspective>.

([37]) *Comments on JOP Recommendation submitted to ECSG Chair, 19 February 2013* (submitted to JOP by Nigel Waters, 11 March 2013).

([38]) CBPRs JOP, 'Recommendation Report on APEC Recognition of TRUSTe' (JOP, 19 February 2013).

([39]) It claimed TRUSTe failed to meet APEC requirements at all (13/21), or failed to fully meet them (8/21).

([40]) CBPRs JOP, 'Recommendation Report on APEC Recognition of TRUSTe' (JOP, 19 February 2013, as amended 18 June 2013).

([41]) IBM, 'IBM Becomes First Company Certified Under APEC Cross Border Privacy Rules' (IBM, 12 August 2013) <http://www-03.ibm.com/press/us/en/pressrelease/41760.wss>.

([42]) Laura Linkomes, 'IBM First to Receive APEC's CBPR Certification' (2013) 126 *Privacy Laws & Business International Report*, pp. 17–19.

([43]) An application by Privacy International to be an observer was rejected early in APEC's processes.

([44]) Waters, 'The APEC Cross Border Privacy Rules System: A Civil Society Perspective'.

([45]) Laura Linkomes, 'Fate of US Safe Harbor to Be Decided by Summer 2014' (2013) 126 *Privacy Laws & Business International Report*, pp. 6–8.

([46]) Chris Connolly, 'EU/US Safe Harbor—Effectiveness of the Framework in relation to National Security Surveillance' (Evidence presented to the Committee on Civil Liberties, Justice and Home Affairs, European Parliament (LIBE Committee), 7 October 2013) <http://www.europarl.europa.eu/document/activities/cont/201310/20131008ATT72504/20131008ATT72504EN.pdf>.

([47]) US Federal Trade Commission, 'Privacy Enforcement and Safe Harbor: Comments of FTC Staff to European Commission—Review of the U.S.–EU Safe Harbor Framework' (12 November 2013) <http://www.ftc.gov/sites/default/files/documents/public_statements/privacy-enforcement-safe-harbor-comments-ftc-staff-european-commission-review-u.s.eu-safe-harbor-framework/131112europeancommissionsafeharbor.pdf>.

([48]) Details of decrees are under 'Topic: Privacy and Security' at Federal Trade Commission Legal Resources <http://www.business.ftc.gov/legal-resources/all/35>.

([49]) *Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines* (OECD, 11 October 2013) <http://www.oecd-ilibrary.org/science-and-technology/privacy-expert-group-report-on-the-review-of-the-1980-oecd-privacy-guidelines_5k3xz5zmj2mx-en>.

([50]) 'OECD Work on Privacy' (OECD, 2013) <http://www.oecd.org/sti/ieconomy/privacy.htm>.

([51]) *2013 OECD Privacy Guidelines and Supplementary Explanatory Memorandum* (OECD, 2013) <http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>. The 2013 Guidelines and the 'OECD Cross-border privacy law enforcement cooperation' have also been re-badged as the 'OECD Privacy Framework': *The OECD Privacy Framework* (OECD, 2013) <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>.

([52]) Nigel Waters, 'Hijacked: The Revised OECD Privacy Guidelines (2013)' (2013) 125 *Privacy Laws & Business International Report*, p. 13.

([53]) Some of these divisions, involving proposals to both strengthen and weaken the 1981 Principles, are indicated indirectly by the 'issues identified for possible further study' in the expert group report; *Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines*, pp. 8–11.

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

([55]) *Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines*, pp. 8–11.

([56]) Greenleaf, 'The Influence of European Data Privacy Standards Outside Europe'.

([57]) The matters discussed here are in pt. 5 'National Implementation' and pt. 6 'International Co-operation and Interoperability'.

([58]) This is because all Guidelines are framed in terms of the obligations of 'Member countries'.

([59]) The 2013 Guidelines still say in art. 6 that they 'should be regarded as minimum standards which can be supplemented by additional measures for the protection of privacy and individual liberties'. How is this consistent with the apparent maximum standards allowed by Art. 17? The phrase 'which may impact transborder flows of personal data' has been added to art. 6, and it appears from the Supplementary Explanatory Memorandum that the intention is to confirm that 'additional measures' under art. 6 can also result in additional restrictions on transborder flows under Art. 17, but this is uncertain and the position is still somewhat ambiguous. In any event, any restrictions on data exports, including additional measures, also have to comply with the Guidelines that they 'should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing'.

([60]) The 1981 Guidelines included in the Recommendations by the Council 'that Member countries take into account in their domestic legislation' the Guidelines, and in the Guideline concerning national implementation, that they 'endeavour to…adopt appropriate domestic legislation' to implement them. However, the 2013 Guidelines drop all of this, with the Council now only recommending that member countries 'implement the Guidelines…through processes that include all relevant stakeholders', and the Guideline concerning national implementation includes in a list of non-legislative measures, 'adopt laws protecting privacy', which have been defined more broadly than specific data protection laws. What this adds up to is that the Guidelines no longer require a commitment to enact data protection legislation implementing the Guidelines. Approaches such as APEC's CBPR, or a scattering of laws such as in the USA, can be more easily argued to suffice.

([61]) Article 21 says countries should support developments that 'promote interoperability among privacy frameworks that give practical effect to these Guidelines'.

([62]) Monica Kuschewsky, 'OECD Privacy Guidelines—What Has Really Changed?' (2013) 126 *Privacy Laws & Business International Report*, p. 1517.

([63]) *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.*

([64]) 'the Committee of Ministers of the Council of Europe may invite any State not a member of the Council of Europe to accede to this convention by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the committee' (Art. 23).

([65]) Graham Greenleaf, 'A World Data Privacy Treaty? "Globalisation" and "Modernization" of Council of Europe Convention 108' in Norman Witzleb, David Lindsay, Moira Paterson, and Sharon Rodrick (Eds.), *Emerging Challenges in Privacy Law:*

Comparative Perspectives (Cambridge University Press, 2014), pp. 93–138, at p. 102 'The quarter-century hibernation of Article 23(1)'.

([66]) 27th International Conference of Privacy and Data Protection Commissioners, *Montreux Declaration—The Protection of Personal Data and Privacy in a Globalised World: A Universal Right Respecting Diversities* (September 2005) <http://www.privacyconference2005.org/fileadmin/PDF/montreux_declaration_e.pdf>.

([67]) In 2009 the CoE's Stockholm Programme explicitly called for the promotion of Convention 108 worldwide: J. Polakiewicz, 'Convention 108 as a Global Privacy Standard?' (Presented at International Data Protection Conference, Budapest, 17 June 2011).

([68]) Council of Europe, Secretariat General, Directorate of Legal Advice and Public International Law (Jurisconsult) Legal Advice Department and Treaty Office, *Note of Information: Accession to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and to its Additional Protocol regarding supervisory authorities and transborder data flows by States which are not member States of the Council* (September 2011) (updating previous publications from at least 1999).

([69]) Greenleaf, 'A World Data Privacy Treaty?' in Witzleb et al. (Eds.), *Emerging Challenges in Privacy Law*, at p. 107 'What we now know about the accession process', and the preceding sections concerning Uruguay and Morocco.

([70]) In practice, a Directive adequacy finding does not even seem necessary: none of the non-EU European countries that are CoE members (and parties to the Convention) have even bothered applying for an adequacy finding. See the table in Greenleaf, 'Scheherezade and the 101 Data Privacy Laws'.

([71]) Article 8 of the European Convention on Human Rights provides rights similar to data protection laws.

([72]) Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (T-PD), *Modernisation of Convention 108: Final Document* (Strasbourg, 29 November 2012) T-PD(2012) 4Rev.3. <http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD%282012%294Rev3E%20-%20Modernisation%20of%20Convention%20108.pdf>.

([73]) Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, item 2 states that the T-PD 'gave a third reading to the proposals for modification of Convention 108, revised by its Bureau following the 28th plenary meeting, and adopted those proposals for transmission to the Committee of Ministers…, and invited the Committee of Ministers to entrust the finalization of the proposals to an ad hoc committee, instructing its Bureau to finalize the draft explanatory report in the light of the discussions'.

([74]) The proposals are to be finalized by an ad hoc committee (CAHDATA) of the Committee of Ministers. The ad hoc committee or the Committee of Ministers as a whole may decide to amend the proposals, so how 'final' they are remains to be seen. The Ad-Hoc Committee on Data Protection (CAHDATA), to include observers from numerous international organizations.

([75]) For a full discussion see Greenleaf, 'A World Data Privacy Treaty?' in Witzleb, et al. (Eds.), *Emerging Challenges in Privacy Law*. Alternatively, see Graham Greenleaf, '"Modernising" Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?' (2013) 29(4) *Computer Law & Security Review*, <http://ssrn.com/abstract=2262296>.

([76]) See Greenleaf, 'A World Data Privacy Treaty?', at p. 129 'Data export restrictions: modernization at risk'.

([77]) Greenleaf, 'A World Data Privacy Treaty?', at p. 129 'Data export restrictions: modernization at risk'.

([78]) Greenleaf, 'A World Data Privacy Treaty?' at p. 129 'Why is adequate not appropriate (and vice-versa)?'.

([79]) Bureau of the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (T-PD-BU), *Information Elements on the Evaluation and Follow-up Mechanism* (Strasbourg, 29 January 2013) T-PD-BUR (2013)02.

([80]) It proposes a mix of government and supervisory authority members, with geographic balance, and a partial rotation of members over six-year terms. The committee would examine the prospective/incumbent Party's legislation, supervisory authority, and the remedies available to data subjects by performing in-person visits and requesting the completion of questionnaires.

([81]) It would involve dialogues with the candidates/parties and interested NGOs would be permitted make to submissions. The committee would prepare a draft opinion and final opinion, for comment by the candidate/party. Both the final opinion and the comments would be made public after transmission to the Convention Committee.

([82]) This summary is derived substantially from an early analysis in February 2012, Christopher Kuner, 'The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law' (2012) *Bloomberg BNA Privacy and Security Law Report*, 6 February 2012, pp. 1–15 <http://ssrn.com/abstract=2162781>.

([83]) The 27th Conference (Montreux) appealed to the UN to prepare a legally binding instrument; 28th Conference (Montréal) called for the improvement of international cooperation; 30th Conference (Strasbourg) proposed and 31st Conference (Madrid) adopted International Standards on the Protection of Data and Privacy (Madrid Declaration); and 32nd Conference (Jerusalem) urged governments to organize an intergovernmental conference to develop a binding international agreement giving effect to the Madrid Declaration.

([84]) ICDPPC, 'Resolution on anchoring data protection and the protection of privacy in international law' (ICDPPC, 35th Conference, Warsaw, 23–26 September 2013) <https://privacyconference2013.org/web/pageFiles/kcfinder/files/5.%20International%20law%20resolution%20EN%281%29.pdf>.

([85]) Sam Pfeifle, 'Data Protection and Privacy Commissioners Release Resolutions on Tracking, Profiling, International Cooperation' (*The Privacy Advisor*, iapp, 25 September 2013) <https://www.privacyassociation.org/>.

([86]) United Nations General Assembly, 'The right to privacy in the digital age' (UN General Assembly, resolution, A/C.3/68/L.45/Rev.1, 20 November 2013).

([87]) European Commission, 'EU-US Trade Agreement—The Facts' (European Commission, 27 February, 2014) <http://trade.ec.europa.eu/doclib/docs/2014/february/tradoc_152204.pdf>.

([88]) Ante, 'US wants to undermine privacy in TTIP negotiations' (ACTA blog, 6 March 2014) <http://acta.ffii.org/?p=2050>.

([89]) *Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy*, The White House, Washington, February 2012.

([90]) Graham Greenleaf and Nigel Waters, 'Obama's Privacy Framework: An Offer to Be Left on the Table?' (2012) 119 *Privacy Laws & Business International Report*, pp. 6–9, <http://ssrn.com/abstract=2187234>.

([91]) Alex Byers, 'White House Pursues Online Privacy Bill amid NSA Efforts' (*Politico*, 7 October 2013) <http://www.politico.com/story/2013/10/white-house-online-privacy-bill-nsa-efforts-97897.html>.

([92]) Government Accountability Office, *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace* (GAO, September 2013); Katy Bachman, 'Government Report Calls For Comprehensive Privacy Law—Consumers should have more information, control over personal data' (*Adweek*, 20 December 2013) <http://www.adweek.com/news/technology/government-report-calls-comprehensive-privacy-law-153996>.

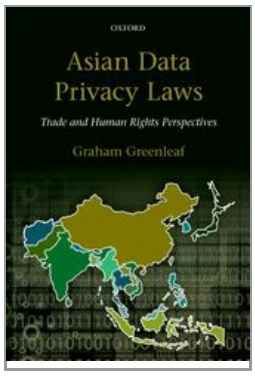
([93]) Greenleaf and Waters, 'Obama's Privacy Framework', section 'How severe are the limits on the USA's ability to protect privacy?'.

([94]) Greenleaf, 'A World Data Privacy Treaty?', at p. 118 'Advantages for European States in non-European accessions'.

([95]) The Commissioners resolved to appeal 'to the United Nations to prepare a legal binding instrument which clearly sets out in detail the rights to data protection and privacy as enforceable human rights': ICDPPC 'Montreaux Declaration' (2007) <http://privacyconference2012.org/wps/wcm/connect/11fed1804aeb668cb7a3bfa0fea628d8/2005_M2.pdf?MOD=AJPERES>.

([96]) This was shown by the revision of the OECD Guidelines' inability to 'modernize' the OECD Principles of National Application.

([97]) Paul de Hert and Vagelis Papakonstantinou, 'Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?' (2013) 9(2) *I/S: A Journal of Law and Policy for the Information Society*, pp. 271–323.



Asian Data Privacy Laws: Trade & Human Rights Perspectives
Graham Greenleaf

Print publication date: 2014
Print ISBN-13: 9780199679669
Published to Oxford Scholarship Online: December 2014
DOI: 10.1093/acprof:oso/9780199679669.001.0001

Asian Data Privacy Laws—Trajectories, Lessons, and Optimism

Graham Greenleaf

DOI:10.1093/acprof:oso/9780199679669.003.0020

[–] Abstract and Keywords

This final chapter makes an assessment of what effect privacy laws in Asia have had, and what is the apparent trajectory of both privacy laws and their enforcement in Asia. It starts by considering the often-expressed scepticism about the value of data privacy laws, arguing that there is no alternative but to include law as an essential part of the solution to privacy problems. It argues for optimism concerning the trajectory of Asian data privacy laws, because they are, for the most part, only in their early stages of development, and are strengthening rapidly, both in terms of their principles and enforcement. The functions and trajectories of Asian data privacy laws are considered in relation to theories concerning data privacy laws generally. The evidence from Asia concerning the relationships between democracy and data privacy is considered. The conclusion is one of cautious optimism.

Keywords: data protection, privacy, Asia, enforcement, transparency, responsive regulation

1. Introduction—are data privacy laws significant in Asia?

The strengths and weaknesses of the data privacy laws in each jurisdiction in Asia have been examined in detail in Part II, including such evidence as is available of the enforcement of each law, and examples of enforcement. In this final chapter, an assessment is made of what effect these laws have had, and what is the apparent trajectory of both privacy laws and their enforcement in Asia.

1.1. The many forms of pessimism about privacy laws

The appropriate starting point is that there is often expressed scepticism about the value of data privacy laws, not particularly in relation to Asia, but more generally. The Snowden disclosures (see Chapter 19, section 1.1) of state surveillance and the vulnerabilities of the most sophisticated private sector information systems, has combined with the apparently unlimited privacy-disregarding use of personal data for commercial gain, by companies often located overseas, to reduce confidence in any privacy protections to a low point.

This scepticism takes many forms. Technological defeatism or dystopianism is the approach taken by many, who argue that, whatever the merits of privacy as a value, it is futile to attempt to protect it in the face of technological developments in **(p.554)** surveillance.[1] For others, antipathy to privacy as a value is put forward on the basis that it is inefficient because it allows the concealment of the information that others need to make decisions.[2] 'The innocent have nothing to fear' is one less sophisticated variants of

this approach, which maximizes business or government interests in preference to individual privacy interests.

One response to these forms of pessimism about data privacy law is to advocate other forms of privacy protection instead, including voluntary self-regulation and the adoption by consumers of technical self-help methods. These are all useful to some extent; however (see Chapter 1, section 2.5), there is no satisfactory evidence that any of these approaches can provide anything more than minor privacy protection, at least not without legal sanctions backing them up. Legal protections, no matter how unsatisfactory, are still essential to the protection of privacy, so we must persist with them.

A less polemical approach to technological determinism asks whether technologies and bureaucratic practices are necessarily uni-directional, always reducing privacy. Rule notes that 'it appears rare for the trend to go in reverse—that is, for established compilations of personal information to be liquidated', but notes occasions where it has occurred.[3] In Asia we also see examples of surveillance practices put into reverse. Although the process is far from complete, South Korea is winding back the previous all-pervading use of the Resident Registration (RR) number (see Chapter 5). In Hong Kong, the Privacy Commissioner has successfully challenged the intrusive photographic stalking of celebrities by paparazzi. Privacy laws are capable of reversing, or preventing, some aspects of technological loss of privacy. But they have not yet been tested against major new surveillance practices such as data analytics and re-identification.

1.2. It is 'early years' for Asian data privacy laws

It may seem strange to refer to the present as the 'early years' of Asian data privacy laws, because the first examples of such legislation (see Chapter 1, section 3.1) go back a quarter-century to Japan's minor[4] public sector law of 1988. It is not until the Hong Kong legislation of 1995 that there was comprehensive coverage of a jurisdiction's private sector. Further significant private sector legislation occurred in steps over the next decade (South Korea, 2001; Japan, 2003; Macau, 2006). However, Asia's 'privacy revolution'[5] only started in 2011. Since then, very significant new or expanded and strengthened laws or regulations have been brought into force in Singapore, Malaysia, South Korea, Taiwan, Hong Kong, China (five laws), Vietnam, and Indonesia. India can be disregarded (see Chapter 15). Therefore, the bulk of Asia's significant data privacy legislation has been enforceable only since late 2011 at best, or little more than two years at the time of writing. Constitutional and civil law protections in some countries have a longer history of enforcement, but their effect does not compare with specialized data privacy legislation. It is in fact very early days in the substantive history of Asian data privacy laws, and the perspective from even five **(p.555)** years' time is likely to be very different. This book is an attempt to benchmark Asian data privacy laws in their infancy.

1.3. Asian data privacy laws are being enforced

Despite the short history of most laws, it is clear from the studies of each jurisdiction in Part II, and the comparisons and summary in Chapter 18 (see section 7 in particular) that Asian data privacy laws are being enforced, and with increasing effectiveness. Examples

include the Hong Kong DPA vigorously and publicly making the maximum use of all enforcement measures in its possession (despite its previously defective toolkit), particularly the 'name and shame' approach; Macau's DPA has used a range of quite different powers consistently and vigorously; South Korea's combination of DPAs and ministry agencies have been effective in a much larger jurisdiction, through use of mediation, ministry supervision, and other means; and China has made surprisingly strong use of criminal enforcement. Singapore's approach to enforcing its Do Not Call rules may indicate that a similarly strict approach may occur with its data protection rules, in force mid-2014. To this is added the impact of major constitutional law rulings protecting privacy in at least eight Asian jurisdictions, and some enforcement of Civil Code or statutory tort privacy provisions in at least five civil law countries (see Chapter 17, section 2.2 for both). The administrative or criminal fines issued in Asian jurisdictions are not yet as high as in both European countries and the USA in the last few years, but it took decades of enforcement in most of those countries before strong enforcement became common. Nevertheless, stronger privacy enforcement is needed in Asia, commensurate with the financial size and resources of the largest local commercial privacy-invaders, and able to at least contribute to a shared effort to restrain their global cousins.

2. Legitimating or limiting surveillance—functions of Asian data privacy laws

Data privacy laws are found in half the countries of Asia, mainly regulating the private sector. Where they exist we have seen that they are increasingly but still inadequately enforced. It is still necessary to ask what is the function of the laws that are being enforced. Briefly put, do these laws limit harmful data surveillance, contrary to the wishes and interests of those who operate personal data systems, or do they only make such surveillance systems work more efficiently and more effectively, without placing any significant check on their expansion or intrusiveness? Many types of enquiry are necessary to answer this question.

2.1. 'Efficiency' principles vs surveillance limitation principles in Asian privacy laws

One enquiry is to ask, to what extent do Asian data privacy laws include 'surveillance limitation principles' which limit the surveillance capacity of information systems, and not only 'efficiency principles' that make them operate in a more fair manner?[6] The overall answer is that Asian data privacy laws do so to a substantial extent. They implement all of the minimum principles, in an average of 10/11 Asian jurisdictions (see Chapter 17, section 6.1). **(p.556)** Although often imperfectly, they implement the 'finality' principles as well as the 'efficiency' principles. Turning to the European principles, all of which may be regarded as 'surveillance limitation', more than half of Asian jurisdictions compared (see Chapter 17) have implemented the most important European principles: deletion (8/11); minimal collection (7/11); direct marketing opt-out (6/11); data export restrictions based on destination (5/11); 'fair and lawful processing' (5/11); and sensitive data protections (5/11). Asian jurisdictions have therefore substantially implemented these surveillance limitation principles.

Individual Asian countries have also added to or extended principles (see Chapter 17,

section 7.3) in ways which limit surveillance: requiring anonymity in transactions where possible (South Korea); no denial of service (South Korea, Singapore); 'unbundling' of consents (South Korea); segregation of consent and non-consent items (South Korea); marketing requiring opt-in (Hong Kong, South Korea); deletion of data on request (South Korea); and user rights on sale of businesses (South Korea). They have also increased the efficiency of their data privacy laws.[7] None of these innovations are yet widespread, but they indicate how South Korea, in particular, is developing new approaches to limiting surveillance.

2.2. Data protection authorities (DPAs) as legitimators

Another line of enquiry focuses on enforcement resources. Flaherty's 'most important conclusion', a quarter of a century ago, was 'that it is not enough simply to pass a data protection law in order to control surveillance, an agency charged with implementation is essential to make the law work in practice'.[8] Generalized, this is the hypothesis that data privacy laws work better if a specialized data protection authority (DPA) is also created to administer and enforce them. This view appeared to be shared by Bennett and Raab in their description of DPAs as 'a sine qua non of good privacy protection'.[9] Asian experience has so far borne out the views of Flaherty, Bennett, and Raab and many others. The longer-established privacy jurisdictions without DPAs (Japan and Taiwan) have had the least effective data protection laws (see Chapter 18, sections 2.1 and 7.3), and the ministry-based enforcement model now seems to be in retreat in Asia. However, it is 'early days' in this as in other respects, and the track record of the new DPAs in Singapore, Malaysia, and the Philippines, and those proposed in Thailand and Japan, will have to be compared in future with continuing ministry-based enforcement in Taiwan, China, Indonesia, Vietnam, and India. South Korea's model of mixing DPAs with continuing strong ministry powers may remain a special case, or might be followed elsewhere, and its effectiveness is as yet difficult to judge.

However, Flaherty's study of early DPAs led him to a second disturbing conclusion, that DPAs 'are in many ways functioning as legitimators of new technology'.[10] More bluntly, he asked '[a]re we witnessing the emergence of the toothless and blind watchdog?'.[11] Flaherty **(p.557)** was in effect applying Rule's insights about data protection laws to the role of DPAs. The question of whether, viewed objectively, DPAs act as legitimators of surveillance technologies and practices, rather than controlling them, has not gone away. It would take much more detailed studies than the relatively brief accounts of each jurisdiction in Part II to come to any definite conclusions about this. The development of ID and credit reporting codes in Hong Kong early in the history of their law gives some support to 'legitimation' arguments, but there is little otherwise obvious from the histories of the DPAs in Hong Kong, Macau, or South Korea to demonstrate this. Again, it is too early in the history of DPAs in Asia to draw any firm conclusions. It is also a complex question, because it is possible that the mere existence of a DPA may blunt the resistance of civil society to the introduction of new privacy-invasive developments. A new factor, which Flaherty did not have to consider, is that the DPAs in Singapore and Malaysia are specialized bodies but not technically independent of government, and only regulate the private sector. Whether they limit private sector surveillance in those countries remains

to be seen. The extent to which Asian DPAs comply with formal indicia of independence shows a great deal of variation (see Chapter 18, section 2.2), and can be compared against their future performance.

2.3. The Asian surveillance context—uncontrolled national ID systems

The surveillance context in which data privacy laws and DPAs operate in Asia is complex. In Part II it has only been possible to note some of the most obvious aspects of key surveillance systems in each country. The fact that Asia is as yet only 'half democratic' (see Chapter 1, section 5.2) means that some countries have surveillance systems that are far more pervasive and intrusive into everyday life than is common in most Western democracies. Post-Snowden, it would be foolish to say that the surveillance systems of some Western countries are less comprehensive, but that is a comparison beyond this book. One thing that is obvious from the brief discussions in Part II is that chip-based and biometric-based ID systems are extending to every Asian country, but very few jurisdictions are introducing legislation-based privacy controls on their use by either the public or private sectors. The North-east Asian jurisdictions are dealing with this issue to some extent, both through special provisions in their general data privacy laws (South Korea, Hong Kong), and through the general provisions of their law (Macau), as well as through special laws governing the operation of the ID systems (China, Hong Kong, Macau, and Japan). The laws in India and Malaysia are likely to have little effect, and Singapore's law will only do so in relation to private sector uses.

3. The trajectories of Asian data privacy law

3.1. Convergence and divergence of laws

Bennett was primarily concerned in 1992 with explaining the similarities and differences between the data privacy laws that had by then emerged in 'countries with divergent institutional arrangements and cultural traditions' (primarily Sweden, the USA, West Germany, and the UK, but to a lesser extent other OECD member countries).[12] He identified 'five plausible explanations for convergence': the need to respond to common technological issues ('where there is no alternative given the nature of information technology'), emulation (of other countries' laws), elite networking ('common perceptions and **(p.558)** interactions of a cross-national policy community'), harmonization (through authoritative actions by international organizations), and penetration ('a more coercive process where states are forced to conform to legislative action taken elsewhere').[13] His five potential reasons for divergence were: 'the formal structures of the state, the preferences of dominant social groups, the role of political parties in linking social preferences to state institutions, the position and power of bureaucracy, and economic constraints'.[14]

Twenty years later, Bennett's candidates for explaining convergence and divergence all still appear very relevant to Asia. However, in Asia there are wider divergences in history, culture, legal structures, and economic constraints than there were between the countries in his study, and far wider divergences concerning democracy (see Chapter 1, sections 4.1 and 5.2). We would now need to add to the reasons for both convergence

and divergence, the economic force which may be applied by multinational non-state actors (Google, Facebook, etc.), which was not such a factor of significance two decades ago, despite the economic weight of Microsoft and IBM.

Bennett found a high level of policy convergence by around 1990 in the countries he studied, including the USA,[15] with the main drivers of convergence being a common experience of technological change, the growth of an international 'policy community' initially consisting of 'a small network of experts', and parallel analyses in 'the pioneers' Sweden and the USA, which led to the same policy conclusions. These were then shared by a broader West European policy community. However, as these pre-Directive policy conclusions were formalized in the first international instruments (the OECD Guidelines and the Council of Europe Convention), for late adopters in Europe such as the UK and the Netherlands, and for some non-European OECD countries such as Japan and Australia, 'the convergence has resulted from a pressure to conform to international standards for mainly commercial reasons'.[16] Such divergence as there was, particularly in the choice and strength of enforcement bodies, is largely accountable to 'what could be won from entrenched bureaucratic forces', and to some extent to the need for administrative bodies 'that had the potential to be self-financing'.[17]

A detailed analysis of the reasons for convergence and divergence in the dozen Asian jurisdictions which have significant data privacy laws has not been possible in this book. Common technological and social issues and attitudes towards them do create a need for some legal response (as Bennett suggests[18]), but do not determine its form. However, it has been demonstrated that the level of convergence is very high, both in terms of principles (Chapter 17) and enforcement measures (Chapter 18), and that it extends not only to the minimum principles found in international agreements (where it is near-complete), but also to a high extent to the European principles. Correlation is not causation, but it is a reasonable hypothesis (perhaps close to a rebuttable presumption) that the 'pressure to conform to international standards for mainly commercial reasons' identified by Bennett continues to apply to 'late starters' and non-OECD members in Asia, and for the last 20 years has embraced the European Union (EU) Data Privacy Directive as much as the OECD Guidelines. Bennett's other convergence factors are relevant in complex ways: common technological issues (many Asian countries are closer to IT ubiquity than elsewhere), emulation (as much a factor as commercial pressure), elite networking (not obvious **(p.559)** Asia-wide), harmonization (the Asia-Pacific Economic Cooperation (APEC) is not authoritative, and the EU just as influential), and penetration (coercion has not been an option). There has been less divergence of enforcement mechanisms than might be expected given the democratic divergences involved. The factors influencing divergence require far more analysis, but seem to be declining in the face of convergence factors supporting adoption of data protection authorities.

3.2. Converging where? Races to the top or bottom?

In 2006 Bennett and Raab[19] presented their 'main research question' as whether there was a 'race to the bottom', a 'race to the top', or something else, in the global development of data privacy protection. In relation to data privacy legislation, the main

conditions proposed by globalization theories of regulation for a 'race to the bottom'—data mobility and wide national divergences in laws—were present in the case of data protection legislation.[20] Nevertheless, Bennett and Raab found that 'there is clearly no race to the bottom', but nor did they find clear evidence of a 'race to the top', or global ratcheting up of privacy standards. In particular, they considered that the 'general suspicion that the APEC Privacy Principles are intended as an alternative, and a weaker, global standard than the EU' means that they 'may serve to slow and even reverse' the otherwise 'halting and meandering walk' to higher standards which the EU Directive had inspired.[21] They concluded that the most plausible future scenario (the Bennett-Raab thesis) was 'an incoherent and fragmented patchwork', 'a more chaotic future of periodic and unpredictable victories for the privacy value'.[22]

The global history of the adoption, and the standards, of data privacy legislation does not support the Bennett-Raab thesis. Globally, the number of countries with such laws continues to expand rapidly, reaching 101 in 2013 (see Chapter 1, section 2.2), and the standards they adopt are closer to the stronger European standards than the lower minimum standards (see Chapter 3, section 3.2). Much the same applies in Asia in terms of principles adopted (see Chapter 17, section 7). The expansion of the number of privacy laws, and stronger revised laws, gives Asia one of the strongest and most coherent recent histories of rising privacy values. After a decade, the failure of the APEC Privacy Principles to have much significant effect (see Chapter 2, section 3.3 and Chapter 17, section 7.2) shows that they did not have the capacity to 'slow and even reverse' the development of higher standards, contrary to Bennett and Raab's concerns. The APEC Cross-Border Privacy Rules system (CBPRs) seems unlikely to change that (see Chapter 19, section 2).

A variant of the 'race to the bottom' theory of regulatory arbitrage is the 'relocation thesis', that predicts that businesses will relocate some aspects of their business practices to those jurisdictions where data privacy laws are weakest, even if most countries do not 'ratchet down' their legal standards. There is no clear evidence of this in Asia, and it would take complex studies of business practices to test such a thesis. However, as detailed in Part II (and summarized in Chapter 17, section 5) some Asian countries do appear to have versions of 'outsourcing exemptions' (i.e. legislative attempts to apply lower privacy standards in their country to the outsourced processing of personal data received from overseas data controllers).

(p.560) 3.3. Convergence in case-law—Asian privacy jurisprudence?

The high level of similarities in the data privacy laws in Asia open up the potential that DPAs in Asian countries when making and explaining decisions on privacy complaints, might find it valuable to refer to decisions on similar matters in other Asian countries (or other countries), as might tribunals and courts. There is no evidence of this occurring as yet: there is no explicit 'Asian privacy jurisprudence' in evidence at any level. Even constitutional courts in Asia are not known to have made reference to decisions on similar matters (such as telecommunications surveillance or ID cards). As yet, there are too few privacy-related decisions made by courts in Asia, and it has been difficult to find and

compare decisions by DPAs and administrative decisions (including difficulties arising from language issues), but this may change over time.[23]

Rights to appeal against the decisions of DPAs or ministers, either directly to courts or first via Tribunal (see Chapter 18, section 3.3) are available, but they are defective in Malaysia and Hong Kong in not allowing access to the courts (see Chapter 18, section 3.3). Such appeals are essential to ensure high standards of decision-making and transparency by DPAs. Bygrave saw a somewhat different reason for the need for appeals in the 'danger…that the data protection authorities begin to construe the legislation in ways that further the cause of privacy and data protection at the expense of other factors that deserve equal or greater weighting in law'. He hypothesized that '[t]he judiciary, approaching the legislation with relatively fresh eyes and formally unencumbered by a pro-privacy mandate, will tend to be better able to resist such bias'.[24] There are simply not enough privacy decisions from courts in Asia to enable any conclusions about whether courts have made more sense of data privacy laws than DPAs. However, Cheung's study of appeals to the Administrative Appeals Board in Hong Kong found that the Commissioner's decisions were upheld in 87 per cent of cases, from 191 appeals (see Chapter 4, section 2.4).

3.4. Democracy and data privacy

Bygrave observes by that the concept of privacy 'reflects the central importance accorded to privacy as ideal and value in liberal ideology'. 'It is in societies built up to a large extent around liberalism that data protection discourse has flourished', he says.[25] He questions whether data privacy laws can flourish in societies which do not share that ideology. A closely related, but not identical, question is whether there is a relationship between data privacy laws and democracy.

Of the democratic regimes in Asia, 7/12 have significant data privacy laws,[26] in five cases covering the public sectors. Of nine semi-democratic regimes, four have data privacy laws, and in Hong Kong and Macau these cover the public sector but in Singapore and Malaysia they do not. Of six authoritarian regimes, two (China and Vietnam) have data privacy laws, neither of which covers their public sectors (see Chapter 1, section 5.2). In Asia, unlike elsewhere in the world, data privacy laws which cover only the private sector are common, amounting to five of the 13 countries with data privacy laws (including China, Vietnam, **(p.561)** and Indonesia's e-commerce/consumer laws). Of these 13 the correlation between public sector coverage and democracy is high, and almost complete if Hong Kong and Macau (liberal but not fully democratic regimes) are included. Asia therefore seems to be developing two strains of data privacy laws: private sector only in authoritarian and semi-democratic countries; and comprehensive laws in democratic countries and those with clearly liberal value (but a 'democratic deficit'). Whether these tendencies will solidify will be tested by developments in India, Thailand and Indonesia.

There are few signs that the development of data privacy laws in Asia has been influenced by 'Asian values' arguments. The high degree of consistency of the principles in these laws is some evidence of this. One counter-example may be that only half of the

jurisdictions with privacy laws have included special protections for 'sensitive' data, and the definitions of what is sensitive differ between Asian jurisdictions and Europe (see Chapter 17, section 4.7).

3.5. Successful '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).[27] 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'.[28] 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.[29]

Are data privacy laws legal transplants? Data privacy laws originated as a 'Western' notion, with their earliest legislative examples being in North America (1970 and 1974[30]), and in seven western European countries in the 1970s.[31] 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 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 was not for the existence of the OECD Privacy Guidelines. Since the mid-1990s, the EU Directive[32] has been at least as strong an influence as the OECD Guidelines.

(p.562) If data privacy laws are legal transplants, where are they transplants from, other than diffusely from 'the West' (OECD Guidelines) or 'Europe' (EU Directive)? 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?

Assuming data privacy laws are legal transplants, it is necessary to ask whether any of these 'transplant' law are failures because they are only window dressing (i.e. ignored), or whether they are misused to produce consequences contrary to those in their place of origin. The difficulty in giving a satisfactory answer comes once again from how recent are some of the laws. Of the longer-established laws, the details given in Part II show that the laws in Hong Kong, South Korea, and Macau have not been window dressing, or misused for other purposes. Taiwan's previous statute may have been window dressing for OECD purposes, but the new one is in more active use. The most difficult case is that

of Japan, where many aspects of the law and its administration ('enforcement' is not the correct word) seem like ritual observances, with little evidence of tangible results. To say that the other data privacy laws are 'successful' legal transplants is not to criticize them as mere copies of laws from elsewhere. They do have sufficient 'family resemblance' to be easily recognized as 'data privacy laws', but they also have significant differences, customization, and in most cases new and creative elements which develop the family of data privacy laws further.

4. Conclusion—cautious optimism about Asian privacy laws

This book's extended focus on data privacy developments in 26 Asian jurisdictions has demonstrated significant developments at many levels. In half the countries of Asia there are now extensive data privacy laws covering the private and/or public sectors, or at least the e-commerce/consumer sector. In almost all the remaining countries there are developments of importance that may contribute to the eventual enactment of broader data privacy laws, such as East Timor's constitutional protection of personal data, the 'right to information' laws of South Asia, and constitutional, e-commerce, and criminal law provisions in many countries. Serious study of data privacy laws can no longer be limited to Europe, North America, and Australasia, as has often been the case in the past.

Furthermore, Asian developments are often *sui generis* or in advance of developments elsewhere. Examples include an independent panel of experts to conduct mediations and recommend settlements including compensation (South Korea); assistance to complainants to take court actions for compensation claims (Hong Kong); access rights extended to a structured, portable, digital copy of data (the Philippines); an express prohibition of any disadvantage from refusal to provide more than the minimum necessary personal data (Singapore, South Korea); and strict 'unbundling' of various types of consents (Malaysia, South Korea). South Korea is the most active source of data privacy innovation in Asia.

Asia's legal systems are influenced in almost equal parts by the common law tradition and the civil law tradition. Now that the 'ministry-based' model of enforcement is in decline, this common law/civil law distinction is of diminishing significance in relation to specialized data privacy laws. There is still some distinction in that the civil law countries are much more likely to have civil remedies for privacy breaches outside such specialized legislation, in their Civil Codes, and are also more likely to have developed strong constitutional protections for privacy.

(p.563) Commentary from outside Asia often focuses on APEC developments. This book demonstrates that this is largely misguided. The APEC Privacy Framework has had little effect after a decade, and deservedly so because of its voluntary nature, superannuated principles, and absence of enforcement mechanisms. The APEC CBPRs may well have a similar (and similarly deserved) lack of success due to offering data subjects everywhere no tangible benefits, and little but expense to any businesses other than a few based in the USA (see Chapter 19, section 2).

The transparency of the operation of the data privacy laws of Hong Kong, South Korea,

and Macau helps demonstrate that those laws are being enforced. In contrast, Japan's law is opaque, and there are no reasons for confidence that it is enforced. India and Taiwan also lack transparency. This book has argued that, without transparency in enforcement, data privacy laws have little value. Established jurisdictions still need to improve their transparency, and new jurisdictions need to demonstrate they have embraced it.

4.1. 'Big data' and other big unanswered questions

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 networks, and so on—may give them a new urgency, but they have been with us in some form for decades if not longer. Technical and social developments, such as social networks, 'big data' (including data analytics), and cloud computing, arise regularly to pose some genuinely new issues but usually to present pre-existing issues in a far more intensified and privacy-invasive fashion. The examples mentioned do that by orders of magnitude beyond previous practices. These issues are of course global and not particular to Asia, and their resolution is not the focus of this book. Existing data privacy laws are not incapable of dealing with most or all of the privacy issues posed by these practices, but Asian laws have not yet been enforced in relation to them, nor have most outside Asia. When and if this occurs, some businesses relying on these practices are likely to be surprised how extensively their practices conflict with these laws whereas others will know this only too well but continue to resist compliance.

4.2. The continuing fracture—data exports and the future international environment

Personal data exports continue to be the most contentious issue in data privacy, with the least consistency between current international instruments (see Chapter 3, section 3.3). It is probable that the division will remain as wide between the 2013 OECD Guidelines and the two new European instruments currently under revision (see Chapter 19). Both the 2013 OECD Guidelines and the 'globalized' Convention 108 are aiming to become global privacy standards, something that was not the case with either until recently. Both aim to facilitate free flow of personal data across borders in exchange for adherence to agreed privacy standards. Both have considerable deficiencies from the perspective of data subjects, in that they do not provide sufficient guarantees of enforcement. However, Convention 108 has higher standards, peer review regarding which countries can accede, and the starting point of a binding agreement in international law. It is a better start than non-binding guidelines with lower standards and no peer review of who can adhere. The reality of these debates is that they are also predominantly, but not exclusively, about the freedom of US-based companies to 'hoover up' the personal data of people in the rest of **(p.564)** world and process it with few restrictions other than not to make misleading claims or not to have inadequate security (and only then in some sectors). Privacy standards in other countries do not matter much if personal data can be liberated to the US 'safe harbor'. It should not be forgotten that a similar situation prevailed a century ago when the USA was the pirates' harbour of the copyright world, to the despair of authors and countries with 'international standard' copyright laws. National attitudes to laws can do a U-turn with changes in business models, as occurred

with the USA and copyright. The prevailing US model of an Internet where 'the user is the product' is not necessarily permanent.

Data exports are where trade considerations and human rights most clearly collide. This is also an area where data privacy laws in Asian jurisdictions either lack restrictions or do not yet actively enforce them. The question for the future is whether Asian governments or regulators will choose to do more to protect the privacy of their citizens' data.

4.3. Cautious optimism, and a lack of alternatives to law

There is a constant race between business and government practices and their technological advances on the one hand, and privacy regulation on the other. As argued in the opening of this chapter, law is the indispensable form of regulation, no matter what its limitations. In Asia, data privacy laws are still in most places in their infancy, but the number of such laws and their scope is increasing steadily; the principles they apply are relatively consistent, are becoming stronger, and contain innovations; and their enforcement mechanisms are expanding and increasingly being used. In Asia, data privacy laws, or in some cases their enforcement, have not yet caught up with surveillance technologies and practices, but they are necessary, even though (as everywhere) they need to be supplemented with other modes of regulation. There are grounds for optimism, but not overconfidence, that in future they will restore a better balance between the human right of privacy and other interests.

Notes:

([1]) Most memorably stated by Sun Microsystems CEO Scott McNealy in 1999: 'You have zero privacy anyway. Get over it': P. Spengler, 'Sun on Privacy: "Get Over It"', *WIRED Magazine*, 26 January 1999, at <http://www.wired.com/politics/law/news/1999/01/17538>.

([2]) Richard Posner, 'The Right to Privacy' (1978) 12 *Georgia Law Review*, pp. 393–422.

([3]) James Rule, 'Conclusion' in James Rule and Graham Greenleaf (Eds.), *Global Data Privacy Protection: The First Generation* (Edward Elgar, 2008), p. 274.

([4]) That Act did not have significant enforcement provisions until 2003, and is still not known to be enforced: see Chapter 8, section 8.1.

([5]) Graham Greenleaf 'Asia-Pacific Data Privacy: 2011, Year of Revolution?' (2011) 46(3) *Kyung Hee Law Journal*, pp. 289–318 <http://ssrn.com/abstract=1914212>.

([6]) See section 3.4 of Chapter 3 for this distinction.

([7]) Examples are privacy officer required (South Korea); onus of proof on controller (South Korea); data breach notifications to DPA (China, Japan, South Korea, the Philippines, Vietnam); data breach notifications to data subjects (Taiwan, the Philippines, South Korea); right to copy of structured e-data (Malaysia); and data privacy rights transmissible to heirs (the Philippines).

([8]) David Flaherty, *Protecting Privacy in Surveillance Societies* (Chapel Hill, 1989), p. 381.

([9]) Colin Bennett and Charles Raab, *The Governance of Privacy* (2nd Edn., MIT Press, 2006), p. 134; see also Colin Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press, 1992).

([10]) Flaherty, *Protecting Privacy in Surveillance Societies*, p. 384.

([11]) Flaherty, *Protecting Privacy in Surveillance Societies*, p. 385.

([12]) Bennett, *Regulating Privacy*, p. vii.

([13]) Bennett, *Regulating Privacy*, p. viii, and ch. 4.

([14]) Bennett, *Regulating Privacy*, p. viii, and ch. 6.

([15]) That was before the EU Data Protection Directive started to be formulated and the policy divergence between the USA and the European countries became clear (possibly with the UK still somewhat closer to the USA).

([16]) Bennett, *Regulating Privacy*, pp. 221–2.

([17]) Bennett, *Regulating Privacy*, p. 223.

([18]) Bennett, *Regulating Privacy*, p. 150.

([19]) Bennett and Raab, *The Governance of Privacy*, p. xv.

([20]) Bennett and Raab, *The Governance of Privacy*, p. 276.

([21]) Bennett and Raab, *The Governance of Privacy*, p. 283.

([22]) Bennett and Raab, *The Governance of Privacy*, p. 295.

([23]) For example, see the *International Privacy Law Library* (WorldLII) <http://www.worldlii.org/int/special/privacy/> which includes decisions from DPAs in Hong Kong, Macau, and Korea, as well as from many non-Asian sources, and some court decisions from many more such countries.

([24]) Lee Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (Kluwer, 2002), p.16.

([25]) Bygrave, *Data Protection Law*, p. 126.

([26]) India, Japan, South Korea, Taiwan, the Philippines, Indonesia (private sector only), and Nepal (public sector only).

([27]) Hideki Kanda and Curtis Milhaupt, 'Reexamining Legal Transplants: The Director's

Fiduciary Duty in Japanese Corporate Law' in D. Foote, (Ed.), *Law in Japan: A Turning Point* (University of Washington Press, 2007), p. 437.

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

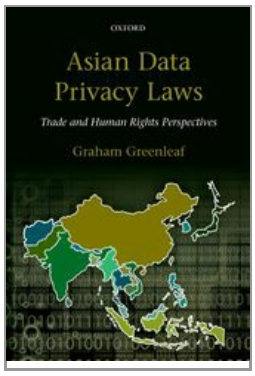
([29]) Kanda and Milhaupt, 'Reexamining Legal Transplants' in Foote, *Law in Japan*, pp. 437–40.

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

([31]) Graham Greenleaf, 'Scheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories' (2014) 23(1) *Journal of Law, Information & Science* <http://www.jlisjournal.org/abstracts/greenleaf.23.1.html>.

([32]) 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 (Official Journal of the European Communities, L 281, 23 November 1995, p. 31 *et seq.*).

University Press Scholarship Online
Oxford Scholarship Online



Asian Data Privacy Laws: Trade & Human Rights Perspectives
Graham Greenleaf

Print publication date: 2014
Print ISBN-13: 9780199679669
Published to Oxford Scholarship Online: December 2014
DOI: 10.1093/acprof:oso/9780199679669.001.0001

(p.565) Index