ASEAN'S TWO SPEED DATA PRIVACY LAWS: SOME RACE AHEAD

GRAHAM GREENLEAF

(2017) 147 *Privacy Laws & Business International Report* 25
[2017] *UNSWLRS* 70

UNSW Law
UNSW Sydney NSW 2052 Australia

ASEAN's two speed data privacy laws: Some race ahead

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

(2017) 147 *Privacy Laws & Business International Report* 25-28

The ten ASEAN (Association of South East Asian Nations) member states include some of the world's most rapidly-developing economies, and have high ambitions for economic integration. The ASEAN Economic Community (AEC),[1] established in 2015, has as one of its e-commerce objectives[2] the development in 2016-2025 of a 'coherent and comprehensive framework for personal data protection', including 'Regional Data Protection and Privacy Principles'.

By 2014 five of the ten member states had enacted data privacy laws: Singapore, Malaysia, the Philippines and, to a lesser extent, Indonesia and Vietnam. Since then, there have been significant developments in all five countries, including strong enforcement actions in both Singapore and the Philippines in the past year, and new legislation in Indonesia and Vietnam. However, there have been few developments since 2014 in the other five, so that overall, there is limited progress toward the 'coherence' which is the aim of the AEC.

The Philippines

The Philippines National Privacy Commission (NPC) has taken a very activist approach to carrying out its duties in its first year of operation. The most obvious indicator of this is that, following the massive data breach by the Commission on Elections (COMELEC) in March 2016, the NPC found[3] that the Commission on Elections (COMELEC) violated the Data Privacy Act and recommended the criminal prosecution of COMELEC Chairman J. Andres D. Bautista. No prosecution has yet commenced. One of the databases involved in the security breach contained sensitive personal data on over 75 million voters, a database on persons banned from holding firearms, with nearly 900,000 personal records, and another with data on 1,267 COMELEC employees, which the NPC describes as 'making the incident the worst recorded breach on a government-held personal database in the world, based on sheer volume.' The NPC alleges 'willful and intentional disregard of his duties as head of agency, … tantamount to gross negligence' by Bautista. Among numerous sections of the *Data Privacy Act* allegedly breached, s.26 penalizes accessing sensitive personal information due to negligence, imposes imprisonment from 3 to 6 years and a fine from US$10,000 to US$80,000 and exposes public officers to disqualification from public office for double the term of imprisonment.

The NPC also ordered that COMELEC must, within short time-frames, appoint a Data Protection Officer, conduct an agency-wide Privacy Impact Assessment and a Privacy

* Assistance with information for this article has been provided by Andin Aditya Rahman, Sonny Zulhuda, and Clarisse Girot. All responsibility for content remains with the author.

[1] ASEAN Economic Community (AEC) website <http://asean.org/asean-economic-community/>

[2] *ASEAN Economic Community 2025 Consolidated Strategic Action Plan*, February 2017 <http://asean.org/storage/2012/05/Consolidated-Strategic-Action-Plan-endorsed-060217rev.pdf>; Endorsed by the AEM and AEC Council on 6 February 2017.

[3] NPC Case No. 16-001 (Philippines), 28 December 2016; For a summary by the NPC, see < https://privacy.gov.ph/privacy-commission-finds-bautista-criminally-liable-for-comeleak-data-breach/>.

Management Program and a Breach Management Procedure within three months, as well as observing the Implementing Rules and Regulations (IRRs) and Circular on Security of Personal Data in Government Agencies.

The NPC has started investigating a second complaint against COMELEC, involving a data breach of a database held by a regional office concerning 55 million individuals. It has issued an interim compliance order[4] that COMELEC should erase all copies of this database in all offices, unless it can secure them appropriately, and that all individuals affected by the breach must be notified, individually in one location, and by newspaper advertisements otherwise.

The NPC has not yet published results of any other investigations, so it is not yet known how its approach will translate into it dealings with private sector organisations, but these first complaints should help induce businesses to take the Act and the NPC seriously.

The NPC is engaging internationally, obtaining accreditations as a full member of the International Conference of Data Protection and Privacy Commissioners (ICDPPC), and as an observer to the Council of Europe Convention 108 Consultative Committee.

Singapore

In April 2016 Singapore's Personal Data Protection Commission (PDPC) published its first nine enforcement decisions since its Act came into force in July 2014, and in little over a year has published details of 27 enforcement actions, including 22 in 2016.[5] The first case reported in April 2016 involved a US$35,000 (Singapore $50,000) fine, [6] and while none have matched that, there has been one US$17,500 fine, and three US$7,000 (Singapore $10,000 fines), plus some lesser fines. About 75% of findings involve failures to provide reasonable security arrangements, and most others involved disclosures of personal information in breach of disclosure limitation obligations, which were not justified by consent or other defences. Security failures by data intermediaries occurred frequently. The data privacy principles in Singapore's Act are at the less onerous end of the spectrum,[7] but these cases make clear that there are many points where businesses cannot assume that the PDPC will adopt a broad and pro-business interpretation.[8]

The PDPC has issued an update to Chapter 3 'Anonymisation' to its Advisory Guidelines.[9] Since the Guidelines use 'anonymisation' to refer to de-identification processes which 'can be reversible or irreversible' they must be read with considerable care, because, as the

---

[4] Compliance Order dated February 13, 2017; see < https://privacy.gov.ph/npc-starts-probe-comelecs-2nd-large-scale-data-breach-issues-compliance-order/>.

[5] PIPC (Singapore) 'Data Protection Enforcement Cases' <https://www.pdpc.gov.sg/commissions-decisions/data-protection-enforcement-cases.>.

[6] G Greenleaf, Graham, Singapore Starts Privacy Enforcement: Fines for Lax Security (May 30, 2016). (2016) 141 Privacy Laws & Business International Report, 1, 4-6.

[7] G Greenleaf 'Singapore's Personal Data Protection Act 2012: Scope and Principles (with so Many Exemptions, it is only a 'Known Unknown') (2012) 120 Privacy Laws & Business International Report, pgs 1, 5-7.

[8] For a more detailed analysis see Ken Chia and Celeste Ang 'Data Privacy Enforcement Trends', 13 January 2017 <http://www.bakermckenzie.com/en/insight/publications/2017/01/data-privacy-enforcement-newsletter/>

[9] PDPC (Singapore) *Advisory Guidelines on the PDPA for Selected Topics,* revised 28 March 2017 <https://www.pdpc.gov.sg/docs/default-source/advisory-guidelines---selected-topics/ch-3---anonymisation-(20170328).pdf?sfvrsn=2>

Guidelines say with considerable understatement 'reversibility of the specific process used would be a relevant consideration … when managing the risk of re-identification.'[10]

PDPC Commissioner Tan Kiat How has mentioned that PDPC would start setting up a TrustMark for data privacy in Singapore in 2017, and that they were 'seriously looking into' joining the APEC-CBPRs.[11]

Malaysia

Malaysia's Personal Data Protection Commissioner (PDPC) is perhaps the first in world to publish a draft 'White List' of jurisdictions to which the Commissioner considers personal data may be transferred. Section 129(1) of the PDPA provides that: 'A data user shall not transfer any personal data of a data subject to a place outside Malaysia unless to such place as specified by the Minister, upon the recommendation of the Commissioner, by notification published in the Gazette.' Section 129(3) provides various exemptions, on which companies transferring data out of Malaysia may otherwise rely and must now rely. The Act does not set out criteria on which the Commissioner must base his decision.

The PDPC has published a Consultation Paper[12] which proposes policies which will guide it in making recommendations to the Minister under s129(1), together with a draft *Personal Data Protection (Transfer Of Personal Data To Places Outside Malaysia) Order 2017* ('Draft Order'). The PDPC refers to three criteria which it says it considered in drawing up its White List: (i) 'Places that have comprehensive data protection law (can be from a single comprehensive personal data protection legislation or otherwise a combination of several laws and regulations in that place)'; (ii) 'Places that have no comprehensive data protection law but are subjected to binding commitments (multilateral/bilateral agreements and others)'; and (iii) 'Places that have no data protection law but have a code of practice or national co-regulatory mechanisms'. Other than what can be implied from the words 'comprehensive data protection law' (which could just mean that it applies to all parts of the private sector), these criteria have no substance: the standard of data protection required is not stated, whether relative to the standard in Malaysia's law or any other standard.

Based on these rather slim criteria, the draft Order by the Minister simply lists the jurisdictions which the Commissioner would recommend that the Minister could declare. They are: (1) the EEA member countries (including EU countries); (2) the US; (3) countries that have received positive EU 'adequacy' assessments; (4) Asian and Pacific regional countries: Australia; Japan; Korea; China; Hong Kong; Taiwan; Singapore; and The Philippines; and (5) the Dubai International Financial Centre (DIFC). Macau is missing, surprisingly. This is not a politically courageous list. The US does not fit within any of the criteria supposedly applied. It is also dubious concerning China, given that the right of subject access is not yet clear in its laws.[13] The other standard being applied here appears to be political expediency.

Some commentators have welcomed Malaysia taking this initiative: 'given that the growth of advanced, high tech economies in the region is likely to be aided by moves towards

---

[10] PDPC (Singapore) *Advisory Guidelines*, [3.1].

[11] Tan Kiat How 'Breakfast with the Commissioner' presentation, Singapore Business Federation, Privacy Awareness Week 2017 <https://www.pdpc.gov.sg/news/Events/page/0/year/2017/month/All/breakfast-with-commissioner-(paw-2017>.

[12] PDPC (Malaysia) *Personal Data Protection (Transfer Of Personal Data To Places Outside Malaysia) Order 2017*, Public Consultation Paper (PCP) No. 1/2017.

[13] G Greenleaf, G and S Livingston 'China's Cybersecurity Law – also a data privacy law?' (2016) 144 *Privacy Laws & Business International Report*, 1-7

interoperability, Malaysia's open commentary on the adequacy of other data protection laws in the region is a welcome step forward'.[14] The problem is that this interoperability would be of the lowest common denominator (the US and China), and few other countries with data privacy laws are likely to agree.

Since mid-2016, three Codes of Practice have been registered in Malaysia: PDP Code of Practice for Utilities Sector (Electricity); Code of Practice on PDP for the Insurance and Takaful[15] Industry in Malaysia; and PDP Code of Practice for the Banking and Financial Sector.

Otherwise, apart from collecting registration fees, there is nothing on the PDPC website to indicate that the Commissioner takes any steps to enforce the Act, such as reports of investigated complaints.

Indonesia

Although Indonesia does now have a data privacy law meeting minimum international standards,[16] work continues on a more comprehensive law which includes, among other things, a data protection authority. A Draft *Bill on Personal Data Protection* was prepared in 2015 by the House of Representative, and the circulated by the Ministry of Law and Human Rights for discussion between all government institutions to ensure that there is no conflict between it and other sectoral rules. As a result of the plenary meeting of the Indonesian legislature held in early 2017, a new version of the Draft Bill ('2017 draft Bill') is available.[17] These processes are taking place earlier than observers had anticipated, considering that the Bill was not included in the House of Representative's priority list for new legislation.

Some features of this new draft include: its scope covers both Indonesian citizens and foreign citizens in Indonesia; there is comprehensive coverage of both private and public sectors, and some extra-territorial coverage; the principles included are extensive, including for example data breach notification to individuals; entitlement to claim compensation from a court for any infringements; and personal data transfers outside Indonesia based on both the consent of the data subject and the law recipient country providing 'an equal level of protection', or based on contract or international agreements, or an exemption from the Commission. An independent Commission is established to administer the law; to investigate and adjudicate on infringements; to conduct mediation between parties, with agreed results of mediation being enforceable; and to impose administrative penalty sanctions of at least US$75,000 (and up to 25 times as much). It is a strong and comprehensive draft Bill of international standard.

Vietnam

Vietnam's Law on Cyber-Information Security, which came into effect on 1 July 2016, has probably the most comprehensive set of data privacy principles yet found in a Vietnamese law,[18] but still lacks regulations to clarify its enforcement. Amendments to the Penal Code

---

[14] Mark Parsons, 'Malaysia publishes draft "White List" for personal data exports' Hogan Lovells, Hong Kong, 27 April 2017 < https://www.hoganlovells.com/en/publications/malaysia-publishes-draft-white-list-for-personal-data-exports>.

[15] A type of Islamic insurance, where members contribute money into a pooling system in order to guarantee each other against loss or damage.

[16] Andin Aditya Rahman 'Indonesia enacts Personal Data Regulation' (2017) 145 *Privacy Laws & Business International Report*, 1.

[17] Rancangan Undang-Undang tentang Perlindungan Data Pribadi **(**2017 Indonesian draft Bill, in Bahasa – select '.docx') <http://www.peraturan.go.id/rancangan-undang-undang-tentang-perlindungan-data-pribadi.html>

[18] Christian Schaefer and Graham Greenleaf 'Vietnam's Cyber-Security Law Strengthens Privacy… A Bit' (2016) 141 *Privacy Laws & Business International Report*, 26-27 <https://ssrn.com/abstract=2824405>.

were drafted, and planned to come into force at the same time, to impose specific 'criminal penalties for violations relating to cyber information and cybercrime' which previously had to be fitted under 'more traditional crimes, such as theft or fraud', but 'its implementation has been postponed indefinitely … due to the large number of errors discovered in the code'.[19]

Other ASEAN members

There have been no significant data privacy developments since 2014 in Thailand, Cambodia, Laos, Brunei or Myanmar. Thailand, which was proceeding toward a law up to 2014, has been ruled by a military junta since mid-2014, with few privacy protections. [20] There is little sign of a draft *Personal Information Protection Act* being enacted, although it is being reviewed by numerous government and legislative bodies, [21] but there are quite a few sectoral regulations.[22]

APEC CBPRs and/or CoE 108: internationalisation options

APEC's Cross-border Privacy Rules system (CBPRs) has had no impact on ASEAN countries as yet. None of the seven ASEAN countries which are APEC members have formally taken any of the steps to join CBPRs. Although a report prepared by Vietnam in late 2016 claimed that the Philippines 'planned to join', and Singapore and Vietnam were 'considering' doing so, no letter of intent from any of these countries has yet appeared on the APEC CBPRs website.[23] Malaysia was reported to have 'no plan to join', and the other ASEAN countries had no laws enabling them to do so.[24]

Some ASEAN countries are also considering another option: both Indonesia and the Philippines have become observers on the Consultative Committee of Council of Europe data protection Convention 108, and might be eligible to accede to it. Singapore, Malaysia and Vietnam would not be eligible because their data privacy laws do not cover their public sectors.

RCEP – an ASEAN+ TPP?

The Regional Comprehensive Economic Partnership (RCEP), is a trade agreement covering ten members of ASEAN and six partner countries – China, India, Japan, Australia, New Zealand and South Korea. RCEP is its most likely successor to the defunct Trans-Pacific Partnership (TPP), which posed great dangers to all data privacy laws through its prohibitions on personal data export limitations and data localisation[25]. Whether RCEP contains similar restrictions, or anything else affecting data privacy, is not certain because of the secrecy surrounding drafts and negotiations,[26] but the most recent leaked version of the draft chapter on Trade in

---

[19] Jim Dao, Tu Ngoc Trinh and Waewpen Piemwichai 'Data Security and Cybercrime in Vietnam' 8 February 2017, Tilleke & Gibbins <http://www.lexology.com/library/detail.aspx?g=37d6b3a7-f0aa-4a3f-8688-2e31967b1708>.

[20] Privacy International *State of Privacy – Thailand*, 14 March 2017 <https://www.privacyinternational.org/node/967>.

[21] DLA Piper *Data Protection Laws of the World – Thailand*, 24 January 2017.

[22] Tilieke and Gibbins 'Data security and cybercrime in Thailand', 8 February 2017, Lexology.

[23] APEC 'CBPR system documents' <http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx>.

[24] 'Survey on the Readiness for Joining Cross Border Privacy Rules System – CBPRs', APEC Electronic Commerce Steering Group (ECSG), January 2017 <http://publications.apec.org/publication-detail.php?pub_id=1800>.

[25] Greenleaf, Graham, The TPP & Other Free Trade Agreements: Faustian Bargains for Privacy? 14 February, 2016 (pre-publcation draft) <https://ssrn.com/abstract=2732386>; in Dan Svantesson and Dariusz Kloza *Transatlantic Data Privacy Relationships as a Challenge for Democracy* (European Integration and Democracy series) (Intersentia, 2017).

[26] Jyoti Panday 'RCEP's Digital Trade Negotiations Remain Shrouded in Secrecy', 16 May 2017 <https://www.eff.org/deeplinks/2017/05/rcep-negotiations-remain-shrouded-secrecy>.

Services (August 2015)[27] does not include any provisions concerning these matters. The 18th round of negotiations were held in the Philippines on 2-12 May 2017. Perhaps the fact that the US is not involved in RCEP, unlike the TPP, will produce a better result for privacy.

Other regional developments

ASEAN and the broader Asian region have a number of active multinational business and NGO initiatives concerning data privacy.

The Asian Business Law Institute (ABLI), an initiative of the Singapore Academy of Law, was launched in January 2017.[28] ABLI has initiated a multi-stakeholder project on the convergence of data privacy laws in Asia, and problems resulting from their considerable heterogeneity at present. It is organizing an experts network which will first address the harmonisation of the regulation of international data transfers.

Academics and NGO representatives in the broader Asian region have successfully established the Asian Privacy Scholars Network (APSN), now with over 110 members,[29] many of whom are from ASEAN countries. Founded in 2010, APSN will hold its sixth conference in Hong Kong in September 2017.

Conclusions

Data privacy developments in ASEAN continue to move significantly forward in the Philippines, Indonesia and Singapore, influenced mainly by domestic rather than international factors. But in the region as a whole, data privacy is still moving at two speeds toward the 2025 ASEAN Economic Community (AEC) goals. It is possible that either AEC or RCEP could have a strong regional influence in future years, but there is no sign of that as yet. Nor are there any convincing signs that APEC CBPRs will be significant.

Assistance with information for this article has been provided by Andin Aditya Rahman, Sonny Zulhuda, and Clarisse Girot. All responsibility for content remains with the author.

[27] Bilaterals.org 'RCEP - draft chapter on trade in services' August 2015 <http://www.bilaterals.org/IMG/pdf/services_consolidated_text_-_5aug2015-2.pdf>.

[28] Asian Business Law Institute <http:///www.abli.asia>; ABLI was launched at the initiative of Chief Justice Sundaresh Menon of the Singapore Supreme Court, in conjunction with the International Conference *on 'Doing Business Across Asia – Legal Convergence in an Asian Century',* 21 January 2016.

[29] Asian Privacy Scholars Network (APSN) <http://asianprivacy.org/>.