Asia's Privacy Reform Bills: Variable Speeds

Graham Greenleaf

[2021] *UNSWLRS* 62
(2021) 171 *Privacy Laws & Business International Report* 26-29

UNSW Law
UNSW Sydney NSW 2052 Australia

Asia's privacy reform Bills: Variable speeds

Graham Greenleaf, Professor of Law and Information Systems, UNSW Sydney, Australia

(2021) 171 *Privacy Laws & Business International Report* 26-29

Never before have there been so many draft laws and Bills in Asian jurisdictions awaiting finalisation and enactment. The jurisdictions with the most important changes to existing drafts are China and Sri Lanka. Brunei becomes the latest Asian country with a data privacy draft law. However, there are also developments in countries in north-east Asia, south Asia and south-east Asia. Some countries, however, are in the 'slow lane' in moving reform forward, particularly India and Indonesia, where major reform Bills have languished for more than a year – due partly to COVID 19 disruptions.

Developments in reforms (if any) in all 26 countries in Asia are noted at least briefly in this article. The overall picture is that Asia is undergoing a more intense transformation of its data privacy laws than any other region of the world at present.

China: 2nd draft of PIPL requires platform oversight bodies

The National People's Congress Standing Committee (NPC-SC) released, on 29 April 2021 for a month's public consultation, a '2nd Deliberation Draft' of the *Personal Information Protection Law of the PRC* (draft PIPL),[1] the first draft of which was released in October 2020. The first draft has been analysed previously,[2] and the purpose here is to identify any significant changes in the second draft.

The most important addition is a requirement on each Internet platforms to establish its own supervisory body in relation to personal information, one that is independent of the platform itself (new art. 57). This will apply not only to China-based social media and search engine giants, but also to any international platforms such as Facebook and Google which fall under the extra-territorial scope of the law (art. 3) because they handle information about persons within the PRC, for purposes of marketing products or services to them, or analysing their conduct, or for other as-yet-unspecified purposes. Any such foreign-based platforms falling under the law must 'establish special institutions or designated representatives within the territory of the PRC responsible for handling matters related to the protection of personal information' (art. 53), and advise the supervisory bodies of their identities.

Article 57 requires that 'Personal information handlers that provide foundational Internet platforms, have a huge number of users or a complex operational model shall perform the following obligations:

(1) Establish an independent body comprised mainly of external personnel to conduct oversight of personal information handling activities;

[1] The English translation by China Law Translate is the source of any quotes in this article.

[2] G. Greenleaf 'China issues a comprehensive draft data privacy law' (2020) 168 *Privacy Laws & Business International Report*, 1, 6-10. <https://papers.ssrn.com/abstract_id=3795001>

(2) Stop providing services to products or service providers on the platform that handle personal information in serious violation of laws and administrative regulations;

(3) Periodically publish 'public social responsibility reports on the protection of personal information, and accept societal oversight.'

There is no definition of 'foundational Internet platforms', how 'huge' user numbers must be, or what a 'complex operational model' requires. Also undefined are what 'oversight' requires, or whether 'societal oversight' is to come only from the independent body. In any case, the combination of sections 53 and 55 implies that foreign platforms would not be able to operate their independent oversight solely from outside China.

Other changes in this 2nd draft include:

- 'Convenient and easy methods for **withdrawing consent'** must be provided. Any such withdrawal does not affect the validity of previous transactions' (art. 16).
- The rights of **deceased persons** in relation to their personal information 'are to be exercised by their close family' (art. 49). No time limits are stated. No right of the deceased to give testamentary directions on this topic is stated.
- Cross-border transfers can be legitimated by an approved contract between sender and receiver (art. 38), but the 2nd draft is being interpreted to mean that **standard contract clauses** to be developed by the Cyberspace Administration of China (CAC) should be used.
- Legitimate grounds of processing without user consent are expanded slightly, to include processing of **publicly available personal information** to a reasonable extent (art. 13(5)).
- The **burden of proof** of no fault where there is harm to interests related to personal data is placed on the data controller (art. 68).

Elsewhere in north-east Asia

Significant changes are underway elsewhere in north-east Asia, except in Taiwan and Macau.

- **Japan** enacted amendments in 2020 to its *Protection of Personal Information Act 2003.* Most of these have the effect of bringing Japan's law more into alignment with the EU's GDPR, and will assist Japan later in 2021 when the European Commission reviews its 2019 Decision in favour of the 'adequacy' of Japan's data protection system. Some of the reforms were rather technical, but others were substantive: a) mandatory data breach notification; b) increases in penalties to US$1M (but only for fraudulent breaches); c) more notice required for cross-border transfers; and d) new categories of 'Pseudonymized Information' and 'Personal Related Information' intended to facilitate 'big data' processing.

  In mid-2021 a complex suite of Bills have been introduced into the Diet, to unify all Japan's data privacy laws (concerning private sector, public sector, independent administrative organs and perhaps local government) under a common set of principles, and under the authority of the Personal Information Protection Commission (PIPC). Once again, the main aim is to facilitate data sharing, and an Act establishing a Digital Agency has already been enacted. The effect on renewal of 'EU adequacy'

remains to be seen. All of this has some similarities to the Korean reforms of 2020. Japan intends to apply for a new EU adequacy Decision covering all sectors, once this is done.

- **South Korea** and the European Commission have announced that they have completed negotiations concerning Korea's adequacy application. It is expected that the Commission will publish a positive draft Decision during June 2021. In 2020, Korea enacted sweeping changes to its data privacy laws,[3] bringing both the public sector and those parts of the private sector regulated by the Korean Communications Commission under the authority of the Personal Information Protection Commission (PIPC). The PIPC was given all enforcement powers in relation to all sectors, under the *Personal Information Protection Act* (PIPA). This overcame the main deficiency in Korea's data protection structure, namely that the PIPC did not have the necessary jurisdictional scope, nor the enforcement powers, to be regarded as an independent regulator for GDPR purposes. Part of the agreement between Korea and the European Commission is that the PIPC will enact Supplementary Rules on five issues that the PIPC has powers to enact and enforce, simultaneous with the EU Decision. A summary of the draft Rules is available.[4] Since it obtained enforcement powers previously only held by the Korean Communications Commission, the PIPC has fined Google US$6M, the largest fine in an Asian jurisdiction. PIPC has also fined a Korean AI company US$92,000, for eight breaches of PIPA, including for misuse of millions of personal emails by using them for machine learning training of an AI 'chatbot'.[5]

- In **Hong Kong**, the Constitutional and Mainland Affairs Bureau and the Privacy Commissioner for Personal Data (PCPD) jointly proposed in a Personal Data Privacy Ordinance (*PDPO) Review Paper* (January 2020) a rather minimal reform Bill (the first since 2012) which would include mandatory data breach notification to the PDPO; an end to the flawed system where breaches of the Ordinance could not result in penalties, but only a breach of PDPC compliance notices; higher penalties; and direct regulation of data processors. A Bill is not yet available. In April 2021 the government proposed additional legislation to criminalise 'doxxing', which would include disclosure of any personal data under the Ordinance, with intent (or recklessness) to threaten, intimidate or harm a person or their family, with few defences and severe penalties including imprisonment.

Sri Lanka's latest 'final draft': Fine tuning

An earlier 'final draft' of Sri Lanka's Personal Data Protection Bill, in December 2019, was reviewed in a previous issue of PL&B, and found to be one of the strongest Bills proposed in an Asian country, except for weaknesses in the independence and enforcement powers of its DPA.[6] Over a year later, after reviews by various government and legal profession committees,

---

[3] KB Park, HK Ko and S Chae 'Korea amends Personal Information Protection Act' (2020) *Privacy Laws & Business International Report 163*, February 2020 pp.21-23.

[4] Bae, Kim and Lee LLC 'EU and Korean data protection authority announce successful conclusion of adequacy talks: Grant of adequacy decision for South Korea expected in coming months' *BKL Legal Update* 21 April 2021.

[5] Jasmine Park 'South Korea: The First Case Where the Personal Information Protection Act was Applied to an AI System' *Future of Privacy Forum*, 21 May 2021 <https://fpf.org/blog/south-korea-the-first-case-where-the-personal-information-protection-act-was-applied-to-an-ai-system/>

[6] G. Greenleaf 'Advances in South Asian DP laws: Sri Lanka, Pakistan and Nepal' (2019) 162 *Privacy Laws & Business International Report*, 22-25. <https://papers.ssrn.com/abstract_id=3549055>

a new 'final draft' has been released by the Legal Draftsman's Department, and has gone to the Cabinet of Ministers in March 2021.

The changes to the Bill are matters of detail, there are no major structural changes from the previous draft. Some details, such as the deletion of the 'right to be forgotten', are significant.

Scope The extra-territorial extent of the Act remains similar to that of the GDPR, except that it now refers to '*specific* targeting' or '*specifically* monitoring' data subjects in Sri Lanka. It is not clear that this wording will narrow the scope of the extra-territorial extent. However, the Data Protection Authority (DPA) may determine the circumstances under which such specific targeting or monitoring may occur (s. 2). Unless the DPA does so, this provision will have no effect.

The Act will not apply to 'non-personal data' (defined as 'data other than personal data'), which is tautological since the Act only applies to 'personal data' (s. 2(3) and (4)). The previous exclusion of 'irreversibly anonymized' data probably still applies.

Obligations of controllers The conditions for lawful processing (s. 5, Schedule 1) now include definitions of 'public interest' and 'legitimate interests', but these provide limited and expected grounds for processing, except perhaps one allowing political parties to collect personal data for electoral purposes. Data minimisation is weakened somewhat by deletion of the requirement that data controllers ensure that processing is 'not excessive' (s. 7).

The application of the obligation of private sector controllers to appoint a Data Protection Officer (DPO) is no longer subject to the discretion of the DPA, based on the 'nature or magnitude of the processing activity' (now s. 20). Details of the educational requirements for DPOs, and their responsibilities, are now provided (s. 20(2)-(5)).

Rights of data subjects The terminology usually associated with the 'right to be forgotten' ('the personal data is no longer necessary for the purposes for which such personal data was collected or otherwise processed') has been deleted from the right to erasure provision (s. 16). Data subject rights therefore seem to be considerably diminished. The scope of the 'automated processing' provisions are further narrowed by a definition of 'automated processing' to mean 'processing that does not involve any manual processing' (s. 47).

Data Protection Authority and sanctions The intention to recycle some existing government-controlled public authority as the DPA continues in this draft, but the clause making it 'responsible for all matters relating to data protection' has been deleted. This is desirable, because it was false: the Minister retains considerable powers. Annual Reports by the DPA are now required (s. 28(5)).

The provisions in the Bill concerning administrative fines and other sanctions remain unchanged.

The scope for exceptions to be made to the Act has been narrowed, by deletion of the vague ground of 'other essential objectives of the interest of the general public (s. 35).

The ability of the Minister to make Orders to 'remove difficulties' that arise under the Act has been extended so that it now applies for five years after the Act comes into operation (s. 46).

Elsewhere in South Asia

In South Asia there are no proposals for data privacy laws in Bangladesh, the Maldives or Afghanistan, and no changes to the existing limited laws in Bhutan and Nepal.[7] Developments are slow in the two largest countries of the region, India and Pakistan.

- **India**'s *Personal Data Protection Bill 2019*[8] remains under examination by a 30 member Joint Committee of Parliament, which on 20 May 2021 was given an extension of time to submit its Report, at the request of the ruling Bharatiya Janata Party (BJP), until the monsoon session of parliament (July to August- September).

- **Pakistan**'s *Personal Data Protection Bill 2020*[9] has not yet been submitted to Pakistan's federal Cabinet. In April 2021, the Sindh High Court directed the responsible federal Ministry 'to expedite the consultative process' so that the Bill could go to the Cabinet and the legislation process commence, and to report back to the Court in a month.[10]

A draft privacy Order for Brunei Darussalam

Brunei is one of the world's few remaining absolute monarchies, and the only one in Asia (Bhutan having transitioned to a constitutional monarchy). The Sultan has complete legislative powers, assisted by an advisory Legislative Council. It has a dual common law and Sharia law legal system, and its common law courts maintain a reputation for independence. Brunei citizens have no constitutional rights, and until now there are no legislative protections of privacy. [11] There is a non-enforceable Data Protection Policy that applies to the public sector.

On 12 May 2021 Brunei's Authority for Info-communications Technology Industry (AITI) launched a public consultation on its draft *Personal Data Protection Order* (PDPO), with a detailed consultation paper. [12] Submissions close on 16 June 2021. AITA has been designated by the Ministry of Transport and Communications to be the 'Interim Data Office' to develop the new law. It will apply to the private sector only (commercial and non-commercial organisations). The consultation paper cites numerous influences on the formation of the PDPO, including the GDPR, national laws, various international agreements, and various ASEAN initiatives. However, the strongest influence clearly is Singapore's data protection law, although Brunei is not following every aspect of it.

The target date for the start of implementation is the end of 2021, but with a 'sunrise period' of two years from enactment before the Order comes into force. The Order will also have a

---

[7] G. Greenleaf 'Advances in South Asian DP laws: Sri Lanka, Pakistan and Nepal' (2019) 162 *Privacy Laws & Business International Report*, 22-25. <https://papers.ssrn.com/abstract_id=3549055>

[8] G. Greenleaf 'India's data privacy Bill: Progressive principles, uncertain enforceability' (2020) 163 *Privacy Laws & Business International Report*, 1, 6-9. <https://papers.ssrn.com/abstract_id=3572620>

[9] G. Greenleaf 'Pakistan's DP Bill: DPA will have powers but lack independence' (2020) 165 *Privacy Laws & Business International Report*, 20-23. June 2020 <https://papers.ssrn.com/abstract_id=3667396>

[10] Jamal Khurshid 'Personal data protection bill: SHC directs federal IT ministry to expedite consultative process' *The News*, 21 April 2021 <https://www.thenews.com.pk/print/823538-personal-data-protection-bill-shc-directs-federal-it-ministry-to-expedite-consultative-process>

[11] For Brunei's political and legal systems, see G. Greenleaf *Asian Data Privacy Laws* (OUP, 2014), pgs. 390-392.

[12] AITA *Public Consultation paper on Personal Data protection For The Private Sector In Brunei Darussalam* <https://www.aiti.gov.bn/SiteCollectionDocuments/Event/PCP_PersonalDataProtectionPrivateSector_20052021_final2.pdf>

'grandfathering clause' (sic) so that in relation to personal data collected before the Order comes into effect, the law will not apply in relation to ongoing uses of existing data for the same purpose for which it was collected. Other uses, or disclosures, will need to comply with the Order. In addition, existing contractual arrangements with third parties in relation to use and processing of personal data will remain valid.

'Personal data' is defined conventionally in terms of 'identifiability'. 'Sensitive data' is not separately defined, similar to the approach taken in Singapore's law. Various exceptions to the law's obligations are specified, including information on employees and business contact information. Deceased person's information will be protected for ten years. There is some extra-territoriality, because the PDPO will apply to any organisations collecting, using or disclosing personal data in Brunei. 'Data intermediaries' (processors) have reduced obligations. Any existing legal provisions will prevail over those in the PDPO (as in Singapore).

The obligations of data controllers are explicitly based on the APEC Privacy Framework (ie. based on the 1980 OECD privacy Guidelines), but go beyond them in a few respects: requirement to appoint a Data Protection Officer (DPO); prohibition of collection by unfair means; a data portability right; data retention limitations; data breach notification; and a right to withdraw consent.

Various versions of 'deemed consent' have been borrowed from Singapore's 2020 amendments, including 'notice and opt-out', thus weakening consent requirements. However, consent is invalid if in response to a demand for information beyond what is reasonably required for provision of a product or service. Overall, the data minimisation and purpose limitation requirements are reasonably strong. Data export limitations will not be based on the protections provided in the recipient destination, but instead on an undefined obligation on the exporter to ensure 'appropriate measures are taken'. Data subject rights have many, potentially over-broad, exceptions.

There will be a designated 'Responsible Authority' to oversee the PDPO. It may resemble a DPA, but it cannot be independent, because that would be inconsistent with the Sultan's absolute powers. It may issue administrative fines for intentional or negligent breaches of the PDPO up to a maximum of US$750,000, or 10% of the annual turnover of the offender in Brunei. Fines must 'provide sufficient deterrence' as well as motivating compliance. An individual or organisation aggrieved by a decision my appeal to an Appeal Committee, the decision of which is final, with no appeal to the courts. There is an individual right of action to the courts, which may grant relief by injunction, declaration or damages as it sees fit.

Elsewhere in south-east Asia (ASEAN)

Myanmar, Cambodia and Laos are the three remaining ASEAN member states where there is no known progress on data privacy. In the other jurisdictions, finalising reforms, or bringing them into force, is divided between those in the fast lane (Vietnam, Singapore) and the slow lane (Thailand, Indonesia, Malaysia, and the Philippines).

- **Thailand**'s *Personal Data Protection Act 2019*,[13] due to come into force on 1 June 2021, has now been postponed (for a second time) to 1 June 2022. One reason is that the government has been unable to appoint the required 17-member Personal Data Protection Committee (PDPC) to oversee the Act. There were 200 applicants to fill the ten non-ex-officio positions on the PDPC, and ten were proposed by a selection

[13] G. Greenleaf & A. Suriyawongkul 'Thailand – Asia's strong new data protection law' (2019) 161 *Privacy Laws & Business International Report*, 1, 3-6. <https://papers.ssrn.com/abstract_id=3502671>

committee, but after complaints of lack of qualifications concerning some of them, the Minister asked the Committee to revise the list in consultation with the Council of State.[14] The interim office of the PDPC has been working with the Ministry of Digital Economy and Society to draw up regulations which need to be made under the Act for it to be effective. However, on 4 May 2021, the Ministry of Digital Economy and Society gazetted a notice[15] that requires controllers to observe the security provisions of the PDPA, despite the whole Act not yet being in force.

- **Indonesia**'s *Protection of Personal Data draft law* was submitted by the President to the House of Representatives in January 2020,[16] but there is no known progress since then. The Ministry of Communication and Informatics (MOCI) claims to be taking preparatory steps such as preparing guidelines and regulations.

- **Vietnam**'s proposed *Decree on Personal Data Protection*[17] released for consultation by the Ministry of Public Security (MPS) in February 2021, is intended to be adopted and brought into force by the MPS by 1 December 2021.

- **Singapore**'s first major amendments to the *Personal Data Protection Act* of 2012 were enacted on 2 November 2020, and most provisions entered into force on 1 February 2021.[18]

- **Malaysia**'s *Personal Data Protection Act* of 2010 remains a moribund law, unenforced and useless. After the 2018 election and change of government, a new Minister promised reforms, the DPA called for submissions on 22 reform proposals in February 2020, but no decisions have emerged, and as of August 2020 the Minister said that reforms were 'still in the discussion stage'.

- The **Philippines** has no legislative reform proposals, but in 2021 the National Privacy Commission has concluded a consultation and says it is 'set to impose administrative fines'[19] on the private sector under the *Data Privacy Act 2012*, and in a draft circular 'proposes fines ranging between 0.5% to 5% of the annual gross income of the personal information controller or processor.'

---

[14] Staff 'Delay in panel formation hampers preparedness for Personal Data Protection Act' *Bangkok Post* 20 September 2020 <https://www.bangkokpost.com/business/1989971/delay-in-panel-formation-hampers-preparedness-for-personal-data-protection-act>.

[15] Thailand, Government Gazette 'Standards for Maintaining Security of Personal Data' B.E. 2564 (2021), 4 May 2021.

[16] G. Greenleaf and AA Rahman 'Indonesia's DP Bill lacks a DPA, despite GDPR similarities' (2020) 161 *Privacy Laws & Business International Report*, 1, 3-6. <https://papers.ssrn.com/abstract_id=3769670>

[17] G. Greenleaf 'Vietnam: Data privacy in a communist ASEAN state' (2021) 170 *Privacy Laws & Business International Report*, 1, 5-8. <https://papers.ssrn.com/abstract_id=3874748>

[18] G. Chen and C. Girot 'Singapore DP law amendments: Practical implications' (2021) 170 *Privacy Laws & Business International Report*, 1, 3-5.

[19] NPC, Philippines 'NPC is set to impose administrative fines' 13 May 2021 <https://www.privacy.gov.ph/2021/05/npc-is-set-to-impose-administrative-fines/>