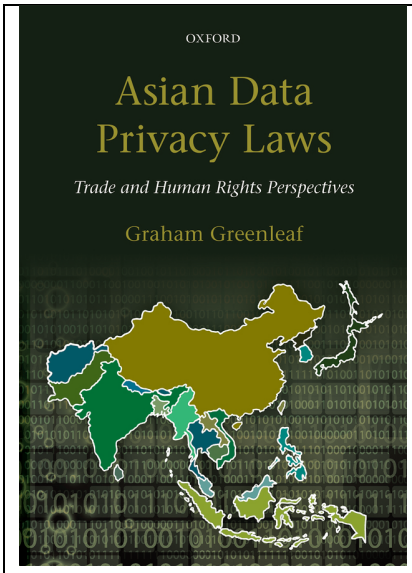

2017-2018 **Further Update** to

Graham Greenleaf's ***Asian Data Privacy Laws – Trade and Human Rights Perspectives***

(Oxford University Press, 2014; Paperback edition 2017)

In July 2017 I published on SSRN an update[1] from mid-2014 to mid-2017 of my *Asian Data Privacy Laws – Trade and Human Rights Perspectives* (Oxford University Press, 2014), to accompany the publication of the paperback edition in July 2017. Purchase details and reviews of the book are on the OUP website.[2]

This further update aims to cover developments to 31 August 2018. Most of the contents are abstracts of my articles in *Privacy Laws & Business International Report (PLBIR),*[3] from which the details of what is abstracted here can be found. I recommend subscription to PLBIR if you wish to keep up-to-date with developments in Asian data privacy laws.

Graham Greenleaf
Professor of Law & Information Systems, UNSW Australia
Asia-Pacific Editor, Privacy Laws & Business International Report (PLBIR)
10 September 2018

Contents (by region and country)

[1] *2014-2017 Update to Graham Greenleaf's Asian Data Privacy Laws* <https://papers.ssrn.com/abstract_id=3000766>

[2] OUP website: https://global.oup.com/academic/product/asian-data-privacy-laws-9780198810094?lang=en&cc=au

[3] PLBIR website https://www.privacylaws.com/Publications/int/.

International agreements

Free Trade Agreements (FTAs)

Japan, Malaysia, Singapore and Vietnam are signatories to the *Comprehensive Regional Trans-Pacific Partnership* free trade agreement (CPTPP FTA), the successor to the failed TPP, which imposes significant limitations on the ability of parties to enact data export restrictions or data localisation requirements, beyond those found in the GATT. Korea, Indonesia, the Philippines and Thailand are not signatories to the CPTPP FTA, although they are entitled to accede to it because they are APEC members. So is China, but very unlikely to sign.

Greenleaf, Graham, Looming Free Trade Agreements Pose Threats to Privacy (2018) 152 *Privacy Laws & Business International Report*, 23-27

Free trade agreements (FTAs) don't include requirements to strengthen data privacy laws, other than by vague and unenforceable gestures. While many FTAs are quite benign to privacy, others may be toxic to domestic privacy laws which impose restrictions on cross-border data transfers, but the toxicity varies. The European Union has made it clear that 'EU data protection rules cannot be the subject of negotiations in a free trade agreement', although existing EU rules can be reflected in FTAs.

In 2018, the threats to privacy legislation posed by FTAs have suddenly become more real. In February the US reiterated complaints against Chinese legislation restricting personal data exports, under the WTO's General Agreement on Trade in Services, (GATS, 1995). In March, a FTA was signed by 11 Asia-Pacific countries (including neither the US nor China) which has much stronger anti-privacy provisions than GATS: the revised 'Comprehensive and Progressive Trans-Pacific Partnership' (was the TPP, now the CPTPP). The US is now considering re-joining TPP, after the Trump administration initially pulled out. Two other Asia-Pacific FTAs are under re-negotiation (NAFTA) or negotiation (RCEP).

This article compares the approach being taken in each of these three FTAs (insofar as is known), and the GATS, and the potential effects of these agreements on data privacy laws. It concludes that, after decades during which free trade agreements have been a potential threat to privacy, the potential has now come much closer to reality. The anti-privacy virus is out of the bottle, with its effects already felt in a bilateral FTA and likely to be replicated in NAFTA. Whether the potentially more powerful RCEP agreement will follow or perhaps abandon this direction is unpredictable, as is the future extent of the US's influence.

APEC Framework and CBPRs

G. Greenleaf 'Notes on APEC Framework and CBPRs' (unpublished) May 2018

- All APEC members have endorsed the *APEC Privacy Framework*, a largely '1980s' standard based on the OECD Guidelines, as revised in 2013, but with some additional weaknesses, particularly its 'accountability' principle of allowing data exports subject to 'due diligence'. There are no enforcement mechanisms (Greenleaf, 2014, pp. 33-37). This endorsement does not carry any legal obligations with it – it is not a treaty. However, the Framework is the foundational standards on which the APEC CBPRs is based, and as such they are standards well below those of the GDPR (or the Directive).

- No Asian country (except Japan) is as yet a full participant in the *APEC Cross-Border Privacy Rules* system (APEC CBPRs),[4] as only the US and Japan have appointed 'Accountability Agents' (AA). Both South Korea and Singapore have formally advised their intention to participate, and had their participation approved,[5] but participation is inoperative until they appoints an AA, and the AA certifies companies as compliant. The Philippines, Vietnam and Australian governments have also stated intentions to participate Reasons why APEC CBPRs is a deceptive and flawed system are in Greenleaf, 2014, pp. 531-38.[6] At present, the privacy dangers of APEC CBPRs in ASEAN countries are still unrealised.
- Some APEC countries are participants in APEC's *Cross Border Privacy Enforcement Arrangement* (CPEA**),**[7] a form of cooperation between DPA and PEAs which has no adverse privacy aspects (see Greenleaf, 2014, pp. 48-9).
- A Joint APEC–EU Working Group stated by APEC to be on 'Promoting Interoperability between the APEC–EU Privacy Rules Systems' has existed since 2012, and 'agreed to continue discussions in Papua New Guinea in 2018'. In 2017 it 'explored options for collaboration and a future work plan—including discussing mechanisms established under the GDPR such as certifications and codes of conduct' (see history of Working Group.[8]) In 2014 the Working Group produced 'a common referential for the structure of the EU system and the APEC system',[9] but this document must be treated with much scepticism (even before the GDPR) as being any type of pointer toward EU-APEC 'interoperability' (see Greenleaf, 'A House of Cards', 2014).
- The EU will not accept, for any country that is to receive a positive adequacy assessment, that EU-origin personal data is able to be export to CBPR-compliant companies. See the Japan section concerning the closing of the 'Japanese back door'.

EU GDPR

Greenleaf, Graham, " 'GDPR Creep' for Australian Businesses But Gap in Laws Widens" (2018) 154 Privacy Laws & Business International Report 1, 4-5

Australia's privacy protections are not regarded as 'adequate' by the European Union, under the 1995 Directive, despite occasional misapprehensions that they are. There has been some strengthening of Australia's Privacy Act 1988 in the decade since the EU last examined the question of the adequacy of Australian law, but the most significant gaps have not since been plugged. However, as the EU's General Data Protection Regulation (GDPR) entered into force on 25 May 2018, the distance between Australian and EU data privacy protections may be greater than it was under the Directive. This article considers the 'gaps' remaining between the GDPR and Australian law, and whether they are likely to be significant for the question of adequacy, if and when it arises again.

---

[4] <http://www.cbprs.org/>

[5] <http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx>.

[6] See also G. Greenleaf, 'APEC's Cross-Border Privacy Rules System: A House of Cards? (2014) 128 *Privacy Laws & Business International Report*, 27-30 < https://ssrn.com/abstract=2468782 >

[7] <http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx>

[8] <https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group>).

[9] <http://www.apec.org/~/media/Files/Groups/ECSG/20140307_Referential-BCR-CBPR-reqs.pdf>

North-East Asia

China

Greenleaf, Graham and Livingston, Scott, 'China's Personal Information Standard: The Long March to a Privacy Law' (2017) 150 *Privacy Laws & Business International Report* 25-28.

A recommended standard entitled 'Information Security Techniques - Personal Information Security Specification' (the 'Standard'), was circulated by China's National Standardization Committee in late 2017, and provides the most detailed specifications yet for how Chinese authorities will interpret and apply existing data privacy laws to private and public-sector entities. [Authors' Note: The Standard was officially released on 29 December 2017, after publication of this article, and will become effective on 1 May 2018.]

We have assessed the data privacy provisions of the 2016 Cybersecurity Law as 'China's most comprehensive and broadly applicable set of data privacy principles to date', going beyond the five main laws and regulations dealing with data privacy enacted from 2011-14, but that it is still missing several common elements found in other jurisdictions' data privacy laws, such as explicit user access rights, requirements on data quality and special provisions for sensitive data, as well as no specialist data protection authority (DPA). The omission of the first of these -- explicit subject access rights -- means that China's law does not yet include one of the most fundamental elements of a data privacy law.

In this article, we examine the additional elements the Standard brings to our understanding of the 2016 Cybersecurity Law, and whether it advances China on its long march towards a national data privacy law. Our overall conclusion is that the Standard is an important step forward in the evolution of China's data privacy protections because of its comprehensive scope; the potential breadth of its definition of 'personal information'; inclusion for the first time of extra protections for 'personal sensitive information'; explicit inclusion of a right access; collection minimization, and appeals against automated processing. This article discusses a draft Standard, from which the final Standard may diverge.

The most significant implications of this Standard for businesses operating in China are:

● Its application to all private sector organisations involved in 'personal information processing', whether customers, employees or others.

● The definition of 'personal information' could potentially be interpreted more broadly than under some European or similar laws, even if it is not intended to be broader that the full scope of EU definitions. Therefore, considerable care must be taken in any use of any data relating to a person, at least until the approach of Chinese authorities is clear.

● The definition of 'personal sensitive information' is both open-ended, but also with named categories much broader than in many other laws, thus requiring great care.

● The suggested obligations in relation to subject access, minimum collection of data, and restrictions on automated processing, because these are not found in other laws.

Japan

Draft adequacy Decision by EU Commission

Since the article below was written, the Commission has issued a draft adequacy Decision concerning Japan:

- European Commission – Press Release 'International data flows: Commission launches the adoption of its adequacy decision on Japan' Brussels, 5 September 2018 <http://europa.eu/rapid/press-release_IP-18-5433_en.htm>
- Other documents including draft Adequacy decision (minus Schedules I and II) <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en>

The draft Decision does not seriously address any of the issues raised in the article below. Other EU institutions (EDPS, EDPB, LIBE Committee) will form their views on what the Commission is proposing. Perhaps NOYB and the CJEU will do so in due course.

Greenleaf, Graham *'Japan's Proposed EU Adequacy Assessment: Substantive Issues and Procedural Hurdles'* (2018) 154 *Privacy Laws & Business International Report*

On 17 July 2018 the European Commission announced that it had successfully concluded with Japan 'their talks on reciprocal adequacy', and that the Commission would adopt its adequacy finding once 'relevant internal procedures are complete'. The draft decision is not yet available.

This article commences by noting seven such procedures, and the numerous EU bodies that could have a substantive influence on the final decision, including the European Data Protection Board (EDPB) and the LIBE Committee of the European Parliament. The draft 'Supplementary Rules' by Japan's DPA (the PIPC), on which the decision is substantially based, is explained, and four aspects of them which will benefit European data subjects are set out.

The article then examines the following issues which EU bodies will need to consider: (i) the transparency of adequacy assessment processes; (ii) the applicability of the decision to Japan's public sector; (iii) whether some personal information transferred from the EU might fall outside Japan's definition of what is protected; (iv) whether the enforcement of Japan's data privacy laws does or can meet the standards of the GDPR; (v) whether, even though the Commission is preventing APEC-CBPRs compliance being a basis for onward transfers, its proposed replacement with an almost entirely consent-based mechanism is protective enough; and (vi) whether a law where the key elements of adequacy can benefit only Europeans can be 'essentially equivalent'.

The path to the EU's decision on whether Japan's privacy protections are adequate has many rivers to cross.

[Some of these criticisms were set out at greater length in an earlier article, below, which prompted the EU Commission's decision to block the 'Japanese back door'.]

Greenleaf, Graham, "Questioning 'Adequacy' (Pt I) – Japan" (2017) 150 Privacy Laws & Business International Report, 1, 6-11

Assessments by the European Commission of whether non-EU countries provide an 'adequate' level of data protection so as to enable a positive EU decision under Article 25 of the 1995 data protection Directive ('adequacy decisions') usually receive little discussion while the process is underway. The criteria which have been used within the EU for the

assessment of adequacy derive partly from the Directive itself, from the Schrems decision, and from the opinions of the Article 29 Working Party (A29WP). A simplified version of these complex criteria commences this article. [Note: This article was written before the Article 29 Working Party's 'Adequacy Referential (Updated)' (November 2017) was available, but it makes no substantive difference to this article.]

It is therefore unusual that both Japan and South Korea made public in 2016 that they were applying for positive adequacy assessments by the EU, and that general comments about these assessments progressing have been made by the Commission and by representatives of the two countries. Japan and the EU are considering simultaneous findings of adequacy, which Japanese law also allows. Even more unusual is that Korea decided to make its own 'Self Assessment' of the adequacy of its data protection in 2016, and then updated it in 2017 after changing the scope of the assessment sought. This article considers Japan's application, and Part II will consider that of Korea.

It is not the purpose of these articles to suggest what the Commission's conclusions should be, or might be, in the case of either country. Any proper assessment of a country's claims to adequacy of data protection is likely to take hundreds of pages, not a short article. Nevertheless, there needs to be public discussion of the strengths and weaknesses of the data protection offered by candidate countries, prior to any assessment being made, because of the importance of such decisions for both international trade, and for the protection of human rights. There also needs to be critical consideration of the quality of the decisions made by the EU bodies involved, once they are made, and analysis of what can be learned from them in relation to future assessments.

This article discusses three of the issues which the EU will have to take into account in its assessment of Japan's application:

(i) The definition of 'personal information' in Japan's legislation includes two 'carve-outs'. It only includes data which 'which can be readily collated with other information and thereby identify a specific individual'. Its 2015 amendments exempted a new concept of 'anonymously processed information', prescribing measures of anonymisation potentially different from those accepted in the EU.

(ii) Japan's restrictions on personal data exports include an exception designed to allow compliance by exports to overseas businesses (at present, only in the US) certified under the APEC Cross-border Privacy Rules system (CBPRs). The issue raised for the EU is whether this would allow onward transfer of personal data originating from the EU, without providing adequate protection.

(iii) Prior to enactment of slightly expanded enforcement powers, and creation of a data protection authority (DPA) in 2015, Japan's data privacy laws had received negligible enforcement. These new enforcement measures have only been in effect since May 2017, so it is therefore an issue that there has as yet been no time for the Japanese system to demonstrate the extent to which they will actually be used, that the failures of past enforcement have been reversed, and that compliance with the requirements of the Directive can be demonstrated.

How EU institutions address these issues is important for this and all future adequacy assessments, both under the Directive and under the GDPR.

Korea

New amendments to Korea's Network Act

Since the article below was written, Korea has enacted legislation (passed 30 August 2018; in effect March 2019) concerning the second set of issues discussed in the article below, and some other issues relevant to an EU adequacy assessment of Korea. The key amendments will have these effects (see article for some issues):

- Foreign online business with sufficient nexus with Korea must **designate a local agent** (similar to EU GDPR art. 27). However, local agent **will be liable** for ensuring compliance by foreign business with Korean law (and foreign business will also be liable for breaches by agent). May also apply to **foreign transferees** of data. Nexus with Korea will be based on scale of business, by users or revenue (to be decided) and (probably) lack of a Korean office.
- Data exports will still depend on (high standard) **consent** of data subject (3% penalty), and **onward transfers** to 3rd country now have same protections. Some exceptions.
- Data exports require **protective measures** (now the responsibility of the agent), including data breach notifications. Presidential Decree will further define measures.

For details, see Bae Kim and Lee LLC 'Korean data law amendments pose new constraints for cross-border online services and data flows' 5 September 2018 <https://www.lexology.com/library/document.ashx?g=c4fa0a24-43a5-43a8-a925-082d84c1f17e>

In relation to the first issue discussed, Korean government websites continue to include translation of the PIPA (the general data privacy law) which differ in whether 'easily combined' is included in the definition of 'personal information'. Not so for Network Act.

Whether changes made to date will satisfy EU adequacy requirements is unclear.

Greenleaf, Graham 'Questioning 'Adequacy' (Pt II) – South Korea' (2018) 151 Privacy Laws & Business International Report.

[The first part of this article summarised the criteria and procedures by which the European Union has assessed the 'adequacy' of data protection in third countries, and considered, in light of those criteria, some issues which could arise in relation to Japan's current application.]

Korea's data protection system was assessed as the strongest in Asia in 2014, and since then its enforcement aspects have been further strengthened. This article considers two main issues which could arise in relation to the EU's assessment of its adequacy, both of which have some similarity to Japan. Questions concerning the necessary independence and powers of a data protection authority have already led to the application being 'scaled back' to cover only those parts of the private sector subject to the 'Network Act', which is administered by the Korean Communications Commission (KCC).

The first issue is whether 'personal information' has a broad enough scope under the Act. It only applies to information which can a identify a specific individual 'when it is easily combined with other information', so 'easily' excludes some information. Second, a contested set of Guidelines for De-identification of Personal Data, without clear legal status, supposedly allow some personal data to be partially removed from the scope of the Network Act, when followed. These procedures may allow a broader exemption from data privacy laws that would be allowed in the EU.

The second issue is whether Korea's provisions controlling personal data exports, and particularly 'onward transfers' of personal data originally received from the EU, are strong enough. The Network Act currently requires data subjects to be informed of details of data exports before providing consent, but not of the state of the law in the recipient country. It is questionable whether this would satisfy EU requirements. Proposed amendments to the law to require foreign data recipients to do likewise before further exports have questionable enforceability. The proposed amendments also include two new mechanisms under which it is unclear whether data exports may take place which could potentially be used to allow transfers to APEC-CBPRs compliant companies (at present, those in the US) with lower protective standards. Such provisions need clarification in the course of an adequacy assessment.

The two parts of this article illustrate why, while adequacy assessment is not a black box, it is not very transparent in its principles or operation. Consequently, independent analyses need to be made of issues requiring consideration by EU authorities in relation to their assessments of particular countries, as part of more general public debate.

A concluding observations is that the way in which the EU deals with the effect on adequacy of laws facilitating exports to APEC-CBPRs compliant companies may be of great importance to the future of the EU's concept of 'adequacy' as a means of protecting the rights of EU citizens by insisting upon a high standard of data protection in foreign countries where their data will be processed.

South-East Asia

Thailand

Amended Thai draft Bill

An amended version of the draft Bill discussed in the article below has been released, and is subject to public hearings from 5 to 20 September 2018.

See Baker & McKenzie 'New draft Personal Data Protection Bill issued for public hearing – Substantial changes following GDPR' *Client Alert* September 2018 (no URL available), which lists the main changes as:

- 'a shorter transition period from 1 year to 180 days, definitions of personal data, extraterritorial applicability, data subject notification requirements, consent requirements, exemptions for collection of personal data from other sources, explicit consent requirements for sensitive data and new exemptions related thereto, records of processing activities, and the prescribed criminal and administrative fines and imprisonment'
- 'new obligations and concepts … including the data subject's right to data portability and the right to object, consent of minors, representatives of controllers or processors who are not established in Thailand, Data Protection Officers, exemptions from cross-border transfer requirements for transfers within the same business group, and punitive damages'.

The proposed Thai Bill is therefore now closer to the GDPR in many respects, but not in relation to the key weaknesses listed below.

Greenleaf, Graham and Suriyawongkul, Arthit 'Thailand's Draft Data Protection Bill: Many Strengths, Too Many Uncertainties' (2018) 153 *Privacy Laws & Business International Report*, 23-25

Thailand is the most economically significant country in East Asia which does not yet have anything resembling a general data privacy law, but on 22 May 2018, just before the EU's GDPR came into force, a draft Personal Data Protection Bill (PDPB) was approved by the Thai Cabinet for submission to the Council of State and the National Legislative Assembly. After ten years of various draft Bills, there are a number of reasons why the current Bill is much more likely to be enacted. A local factor is that lack of data privacy has recently become very controversial in Thailand because a mobile phone operator, exposed 46,000 customer records (names, addresses, scans of ID cards and passports) but apparently faces no legal consequences. An external factor is the extra-territorial reach of the EU's General Data Protection Regulation (GDPR), in force as of 25 May 2018, which is referred to constantly (although often with exaggeration) by Thai commentators as posing problems for Thai businesses unless Thailand adopts a compatible law. This article critically reviews the PDPB, by reference to the standards of international privacy instruments. It concludes that Thailand's Bill is one of reasonable strength by current global standards, except for its major deficiencies in the independence of its DPA, and the excessive degree of potential exceptions to its operation.

G. Greenleaf 'Notes on the Thai draft Bill compared with the GDPR' (unpublished) May 2018

The above article contains a more detailed assessment, but this summary may be useful. Lack of a reliable English translation makes some conclusions tentative and provisional.

Key strengths of the PDPB*:*

- Comprehensive scope of all sectors (assuming public sector coverage), with an undesirable complete exception for credit reporting, and for legislative and judicial bodies (rather than by functions);
- Wide extra-territorial application to overseas processing (though differing from GDPR);
- Collection [and processing] has a strong consent basis, with consent able to be withdrawn;
- Exceptions to consent-based processing similar to GDPR;
- Sensitive data protected but not genetic data or biometrics;
- Requirement of regular privacy impact assessments (but is it enforceable?);
- De-identification when retention period expires;
- Data breach notification requirements, to DPA and to data subjects;
- Processors have direct obligations (security; breach notification);
- Transfers to foreign countries must meet a standard of protection, set by the DPA;
- Statutory provisions for compensation for damage;
- Administrative fines by DPA;
- DPA authorised to enter into agreements with foreign DPAs.

Key weaknesses of the PDPB*:*

- Complex administrative/enforcement structure, with no single body identifiable as the DPA carrying enforcement powers;
- Lack of guaranteed independence of the main bodies in the administrative/enforcement structure. Powers of Minister to suspect action of the DPA largely negate independence.
- Exceptions can be made by Ministerial Regulation (to processing without consent; to definitions of sensitive data);
- Standards for foreign transfers are not set by the Act, but by the DPA;
- Administrative fines are manifestly inadequate (up to US$16K only);
- No explicit opt-out provision for direct marketing;
- Lack of a right of appeal against decisions of PDPC or expert Panels.

Indonesia

G. Greenleaf 'Notes on Indonesia's draft Data Protection Law' (unpublished), May 2018

Kementerian Komunikasi dan Informatika (Kominfo), (Minister of Communication and Informatics in English – also sometimes called MOCI) has lead responsibility for the drafting of a comprehensive Data Protection Bill, in consultation with other government bodies. The version discussed below dates from April 2018, and is an internal government version. The following summary is based on an incomplete translation of the Bill which may be unreliable on some points.

[The government subsequently released another, less developed, version for public discussion. It is discussed by Baker & McKenzie in an article dated May 18 2018.[10]]

Key strengths of the Bill (compared with the GDPR)

- The 'personal data' (PD) definition is conventionally based on identifiability;

[10] Baker & McKenzie 'Indonesia: Government Pushes Draft Data Protection Law' *Global Compliance News* May 18 2018 <https://globalcompliancenews.com/indonesia-draft-data-protection-law-20180518/>

- The Act has very broad scope
  - it covers both Indonesian citizens and foreign citizens in Indonesia;
  - there is comprehensive coverage of both private and public sectors,
  - there is some extra-territorial coverage, relating to acts outside Indonesia which have consequences in Indonesia, or harm Indonesia's national interests;
  - there are very few (and expected) exemptions from the whole Act; other exceptions are from specific principles;
  - there is no general exemption for publicly available information;
- 'specific' (or sensitive) personal data includes normal categories (excluding religious beliefs) plus genetics and biometrics ;
- The principles included are extensive, covering all basic principles plus the following:
  - right to request limitation of processing (needs clarification);
  - opt-in to pseudonymous processing;
  - direct marketing requires consent (ie opt-in);
  - data breach notification to individuals.
- Personal data transfers outside Indonesia based on both the consent of the data subject; or the law of the recipient country providing 'an equal or higher level of protection' than Indonesia, or based on contract or international agreements, or an exemption from the Commission.
  - Commission may determine a White List based on strength of foreign laws.
- A Commission (DPA) is established to administer the law, responsible directly to the President;
- DPA may investigate and adjudicate on infringements; to conduct mediation between parties, with agreed results of mediation being enforceable
  - the approach of initial mediation by Commission members, and if that fails, arbitration, with a right of either party to take the dispute to a court, is similar to South Korea;
- Compensation claims may be made to a court, or to the Commission, for any infringements;
- DPA may impose administrative penalty sanctions of at least US$75,000 (1BN rupiah), and up to 25 times as much (25 BN rupiah).
- Criminal offences for many breaches of the Act, the most severe with potential 10 years gaol.

Key limitations of the Bill (compared with the GDPR)

Some of these apparent weaknesses may only be due to a poor translation.

- Concept of 'data owner' rather than 'data subject' may cause problems by confusion of property rights (and thus alienabilty) with data protection rights;
- There is no automatic destruction of PD once purpose is completed, it must be requested;
- The Commission does not appear to have legislatively guaranteed independence or tenure (this may be due to lack of familiarity with Indonesian law); this may be a key weakness;
- Various exceptions to data export restrictions may be both too weak; others may be too strong;
- There are many GDPR principles which do not appear to be included, such as:
  - Separate obligations imposed on processors;
  - Requirements for Data Protection Officers (DPOs);
  - Requirements for Data Protection Impact Assessments (DPIAs);
  - Data portability;
  - Suspension of processing (inclusion is unclear);
  - Right to have human review of automated decisions.

- There is already a version of the 'right to be forgotten' in a 2016 amendment, but its implementation depends on regulations yet to be made (and is otherwise left to the Courts). It would be preferable if this right and its implementation requirements were stated in this Bill.

Despite these limitations (some of which may be resolved by translation clarifications), an initial overall assessment is that this Bill, if enacted in this form, would be one of the stronger laws in Asia, with standards much higher than the minimum standards for a data privacy law, higher than or equivalent to the 1995 Directive in many respects, but not yet as high as the GDPR.

Vietnam

Law 24 on Cybersecurity (English translation) (via Allens><Linklaters)
https://www.allens.com.au/pubs/pdf/priv/cupriv22jun18.pdf

Cybersecurity law (June 2018) establishes data localization requirements

L Biu, H. Nguyen and K. Nguyen 'Client Update: Vietnam issues a stringent new cybersecurity law', Allens><Linklaters, 22 June 2018
https://www.allens.com.au/mobile/page.aspx?page=/pubs/priv/cupriv22jun18.htm

This article sets out many unanswered questions concerning the law.

W. Piemwichai and Tu Ngoc Trinh 'Vietnam's New Cybersecurity Law Will Have Major Impact on Online Service Providers', Tilleke & Gibbons, June 18 2018 (via Lexology)
https://www.lexology.com/library/detail.aspx?g=9426a7b1-3122-4cb8-b484-2300b5061731

Singapore

G. Greenleaf 'Notes on recent Singapore privacy developments' (unpublished, May 2018)
These notes on 2017-8 developments refer to a book chapter on Singapore's law (Greenleaf, 2018)[11] and a report to the Asian Business Law Institute (Chia, 2018)[12]:

- Guidelines concerning 'anonymisation'/de-identification of personal data which appear to leave more scope for use of personal data than European standards (Greenleaf, 2018, para. 8.13). 'Anonymised' data can also be exported without restriction (Chia, 2018, para. 55). PDPC suggestions that they will implement a 'regulatory sandbox' are probably aimed at allowing 'big data' experiments based on these Guidelines, or further weakening of them.
- The PDPC does not have independence from government (Greenleaf, 2018, paras. 8.64-65).
- Administrative fines up to S$1 million, with complaints regularly resulting, in practice, in S$10K-S$30K fines and occasionally S$50K (see Greenleaf, 2018, para. 8.70 for examples). Other than Korea, no other Asian law results in fines of this magnitude, this often, low though it is by European standards. In theory, the potential S$1 million fine meets European standards, at least prior to the GDPR.

---

[11] G. Greenleaf 'The Asian context of Singapore's Law', Chapter 8 of S. Chesterman (Ed) *Data Protection Law in Singapore (2nd Ed) (Academy Press, 2018)*

[12] Ken Chia Jurisdiction Report – Singapore in (Asian Business Law Institute (ABLI) *Regulation of Cross-Border Transfers of Personal Data in Asia*, February 2018 <http://abli.asia/PUBLICATIONS/Data-Privacy-Project>

- Regular reporting of decisions <https://www.pdpc.gov.sg/Commissions-Decisions/Data-Protection-Enforcement-Cases>, with respondents always named, giving transparency likely to affect respondent behaviour and encourage complainants. In Singapore, a small and compliance-conscious jurisdiction, 'name and shame' is likely to be an effective sanction. (Greenleaf, 2018, paras. 8.77-79).

Proposed 'reforms'

- The PDPC is proposing to weaken the significance of consent even further (Greenleaf, 2018, para. 8.28, at end) (see PDPC's Response to the Public Consultation on Approaches to Managing Personal Data in the Digital Economy[13]).
- A 'regulatory sandbox' is under consideration by the PDPC (discussed above).
- A mandatory data breach notification scheme is supported by PDPC, based on 'a consistent risk-based approach, and a higher threshold for notification to affected individuals as well as to PDPC', and is likely to result in legislation (see 'PDPC's Response' above).

Data exports, APEC-CBPRs etc

- PDPC has developed its own recommended (not mandatory) Standard Contract Clauses (SCCs) for transfers (Chia, paras. 83-85). EU – Singapore (and in effect, ASEAN) cooperation might be possible here.
- Mutual recognition (within ASEAN and beyond) of both CBPRs certifications (once Singapore is fully involved), and Trustmarks, are possible policy directions (Chia, paras. 86-93). The likelihood of these being based on the very low OECD/APEC standards – rather than even slightly higher Singaporean standards – if deemed by PDPC to be 'comparable' – is a considerable problem for the EU in obtaining transfer mechanisms in the Asia-Pacific which are consistent with EU GDPR adequacy standards.
- Singapore's DPA and its controlling Department (IMDA) called for Singapore-based organisations to participate in Singapore's Data Protection Trustmark (DPTM) certification, requiring that evaluation by one of three independent assessment bodies to determine whether they are able to meet their obligations under the PDPA. It is described as a 'local certification scheme' with no mutual recognition of other schemes at this stage.[14] DPTM certification therefore does not authorise data exports to APEC-CBPRs certified companies in the US.
- According to Chia 'Singapore is also exploring other avenues of bilateral or multilateral co-operation with foreign counterparts in the area of data protection, such as free trade negotiations, and mutual recognition of data protection regimes between Singapore and its key trade and economic partners.'
- A separate regime for international data transfers operates in the banking sector, prevailing in the event of inconsistency with the PDPA (Chia, 2018, paras. 21-31)
- Singapore is becoming a participant in the APEC Cross-Border Privacy Rules system (APEC CBPRs), having announced its intention to participate in July 2017, and had its application approved by APEC CBPRs Joint Oversight Panel in February 2018. The Minister states that Singapore will align its own proposed Trustmark standards with the APEC-CBPRs standards (Chia, 2018, para. 1-3). APEC-CBPRs will not operate in Singapore until it appoints an 'Accountability Agent' (AA).

---

13 <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Legislation-and-Guidelines/PDPC-Response-to-Feedback-for-Public-Consultation-on-Approaches-to-Managing-Personal-Data-in-the-Dig.pdf?la=en>.

14 IMDA 'Data Protection Trustmark Certification' 29 August 2018 <https://www.imda.gov.sg/dptm>; see also Anne L. Petterd, Andy Leck, Ken Chia and Ren Jun Lim 'Singapore launches pilot Data Protection Trustmark certification scheme' Baker & McKenzie/Lexology 30 August 2018.

South Asia

India

G. Greenleaf 'Notes on post-Puttaswamy Indian developments (unpublished) August 2018

A nine judge 'constitution bench' of India's Supreme Court unanimously decided in *Puttaswamy v Union of India*[15] on 24 August 2017 that India's Constitution recognises an inalienable and inherent right of privacy as a fundamental constitutional right. It is an implied right, because privacy is not explicitly mentioned in the Constitution, but it is implied by Article 21's protections of life and liberty, and is also protected by other constitutional provisions providing procedural guarantees. Privacy protection is also required by India's ratification of the UN's *International Covenant on Civil and Political Rights* (ICCPR), article 17 of which protects privacy. The decision will affect private sector practices ('horizontal effect') as well as actions by the Indian state ('vertical effect'). The Court identified three main aspects of privacy: privacy of the body; privacy of information; and privacy of choice. Subsequent smaller constitution benches will now decide the constitutionality of various pieces of legislation, and practices, in light of the fundamental right of privacy. These include the constitutionality of India's ID system (the Aadhaar), the criminalisation of homosexual conduct, and prohibitions on consumption of certain foods, and probably many more issues. It is very likely that, in order to protect the constitutionality of other legislation and practices, the Indian government will now have to legislate comprehensively to protect privacy in relation to both the public and private sectors in India.[16]

Puttaswamy also held that governments could only interfere with the fundamental right of privacy if they observed three conditions: 'first, there is a legitimate state interest in restricting the right; second, that the restriction is necessary and proportionate to achieve the interest; third that the restriction is by law.'[17] One immediate implication of this is that the government's 'Aadhaar' biometric ID system, since it is clearly an interference with privacy, must observe these conditions of legitimacy and proportionality, both in its administration and in the legislation implementing it. The Aadhaar system is under current challenge before a constitution bench of the Supreme Court, which has heard the matter but reserved its decision. It is possible that a strong general data protection law, as well as specific improvements to the Aadhaar legislation, will be required by the Supreme Court as conditions for the constitutionally valid operation of the Aadhaar system.

In the year since *Puttaswamy*, considerable developments have taken place in India, notably:

- The Report[18] of the Committee of Experts under the Chairmanship of Justice B. N. Srikrishna ('Srikrishna Report') in July 2018.
- The draft *Personal Data Protection Bill 2018* ('draft Bill')[19] accompanying the SriKrishna Report.

---

[15] *Justice K.S. Puttaswamy (Retd.) v. Union of India* 2017 (10) SCALE 1.

[16] See G. Greenleaf 'Constitution Bench' to decide India's data privacy future' (2017) 148 *Privacy Laws & Business International Report*, 28-31, for details of the committee established to draw up such a law, and background to the Court's decision.

[17] ibid

[18] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians* < http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf >

[19] Personal Data Protection Bill 2018 <http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf>

- The Indian Government has called for submissions on the draft Bill by 10 September 2018, following which the government will produce a Bill for introduction to Parliament.
- In the *Navtej Johar v Union of India* case (decided 6 September 2018) a five judge Constitution Bench of the Indian Supreme held unanimously that India's criminalization of homosexual conduct (s. 377 of the Criminal Code) was unconstitutional (as a result of *Puttaswamy*). The Indian government decided not to oppose the petition, saying it would leave the decision to the Court.
    - For analysis of the judgments, see Alok Prasanna Kumar 'Section 377 judgment could form beginning of a body of path-breaking jurisprudence in India' *Scroll* 6 September 2018.[20]
    - For background, see Gautam Bhatia 'The Indian Supreme Court Reserves Judgment on the De-criminalisation of Homosexuality' *Oxford Human Rights Hub*, 15 August 2018.[21]
- The five judge constitution bench in the Supreme Court case challenging the constitutionality of the Aadhaar ID system, and the *Aadhaar Act 2016* (Puttaswamy again the lead petitioner) reserved its decision in May 2018, after a 40 day hearing (2nd longest in Indian history). 'Justice Chandrachud is the only link between the five-judge bench and the nine-judge bench which had ruled on right to privacy.'[22] The Court's decision had to be delivered by 2 October, on which date the current Chief Justice, who is part of the bench on this case, will retire. It was delivered on 26 September (below)
    - The SriKrishna Report recommends amendments to the *Aadhaar Act* (separately from the question of constitutionality).
- Data localisation provisions in a directive by the Reserve Bank of India (RBI), anticipating to some extent the data localization recommendations in the SriKrishna report.

Judgment in J. K.S. Puttaswamy v. Union of India (Aadhaar judgment) 26 September 2018
https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf

[The court held 4/1 that the Aadhaar scheme was capable of being constitutionally valid, but that many aspects of the current Aadhaar Act 2016 were unconstitutional. The 3 judgments run to 1448 pages.]

G. Greenleaf 'India's 'Fourth Way': GDPR-Lite with Chinese characteristics?' (2018) 155 *Privacy Laws & Business International Report* (October 2018, in publication)
Includes a comparison of the Srikrishna Report's draft Bill with the GDPR.

G. Greenleaf, 'GDPR-Lite and requiring strengthening – Submission on the draft *Personal Data Protection Bill* to the Ministry of Electronics and Information Technology (India)' September 20, 2018.
https://ssrn.com/abstract=3252286

Includes recommendations for improvements to the Srikrishna Report's draft Bill.

---

[20] <https://scroll.in/article/893468/section-377-judgment-could-form-beginning-of-a-body-of-path-breaking-jurisprudence-in-india>

[21] < http://ohrh.law.ox.ac.uk/the-indian-supreme-court-reserves-judgment-on-the-de-criminalisation-of-homosexuality/>

[22] Dhananjay Mahapatra 'Supreme Court reserves verdict on Aadhaar validity' Times of India, 11 May 2018 https://timesofindia.indiatimes.com/india/supreme-court-reserves-verdict-on-aadhaar-validity/articleshow/64116972.cms

Greenleaf, Graham, 'Constitution Bench' to Decide India's Data Privacy Future (2017) 148 *Privacy Laws & Business International Report*, 28-31

[This is for background to the *Puttaswamy* case] This article was written during the hearing of the most important case concerning privacy in Indian history, by a nine Judge 'Constitution Bench' of India's Supreme Court, from July 19 to August 4 2017: *Puttaswamy v Union of India*. As explained, the case was to 'determine whether or not privacy is a fundamental right under India's Constitution. A positive answer will require answers to further questions, including what types of privacy are encompassed by the right, and whether it is only a 'vertical' right, enforceable against the State, or a 'horizontal' right, enforceable by one private individual against another. It will provide grounds for challenges to the validity of many aspects of legislation at all levels of Indian government, starting immediately with the *Aadhaar Act 2016* concerning India's ID system. If it is a horizontal right, the Indian government could be required to enact privacy legislation to implement the right, and would probably need to do so in any event in order to protect the constitutionality of legislation attacked on privacy grounds.' [Note: Now that the Court has unanimously given such a positive answer, these consequences are playing out in numerous further cases.] The article outlines the main arguments provided by the petitioners, the government, and their allies.

The article also considers the cases immediately preceding the *Puttaswamy* decision. *Viswam v Union of India* concerned the constitutionality of Indian government's attempt, by s. 139AA in the Income Tax Act, to require mandatory linking of the Aadhaar ID number to a person's Permanent Account Number (PAN), a 10-digit alphanumeric number allocated by the Information Technology Department to individuals and entities. Despite the Court placing impediments before these plans while the constitutional issues remain unresolved, the Modi government's 'let's see what we can get away with' approach continues.

Other South Asian countries

[The constitutional challenge by petitioner Ratnasabapathy in the Supreme Court against the issue of Sri Lanka's new electronic national identity card (e-NIC), mentioned below, does not seem to have proceeded further since November 2017.]

Greenleaf, Graham 'Privacy in South Asian (SAARC) States: Reasons for Optimism' (2017) 149 *Privacy Laws & Business International Report* 18-20

The SAARC region (South Asian Area of Regional Cooperation), comprising the eight states of South Asia (India, Sri Lanka, Bangladesh, Pakistan, Bhutan, Nepal, Maldives and Afghanistan), is the Asian sub-region with the least development of data privacy laws. This article reviews the position in the seven South Asian countries other than India, since mid 2014.

Development of privacy protection in South Asia has been stalled by many factors, but there are now some reasons for optimism. Since a previous comprehensive review in mid-2014, there have been no new data privacy laws for any of these countries in the past three years. However, there are indicators that such laws are under development in four (Sri Lanka, Bhutan, Nepal and Maldives), plus significant developments in other countries in relation to Right to Information (RTI) laws, and some political and other developments important to note in relation to potential longer-term developments. There are no relevant regional developments resulting from the SAARC agreements.

However, the most significant regional factor is the possible implications of the Indian Supreme Court decision on the fundamental constitutional right of privacy. A nine judge 'constitution bench' of India's Supreme Court unanimously *decided in Puttaswamy v Union of India* on 24 August 2017 that India's Constitution recognises an inalienable and inherent right

of privacy as a fundamental constitutional right. *Puttaswamy* has already had an effect on litigation in Sri Lanka, and is likely to affect privacy developments in South Asia and elsewhere for decades to come.