University of New South Wales Law Research Series

ASIA'S DATA PRIVACY DILEMMAS 2014–19: NATIONAL DIVERGENCES, CROSS-BORDER GRIDLOCK

GRAHAM GREENLEAF

(2019) No 4, Revista Uruguaya de Protección de Datos Personales (Revista PDP), August 2019, 49-73
[2019] *UNSWLRS* 103

UNSW Law
UNSW Sydney NSW 2052 Australia

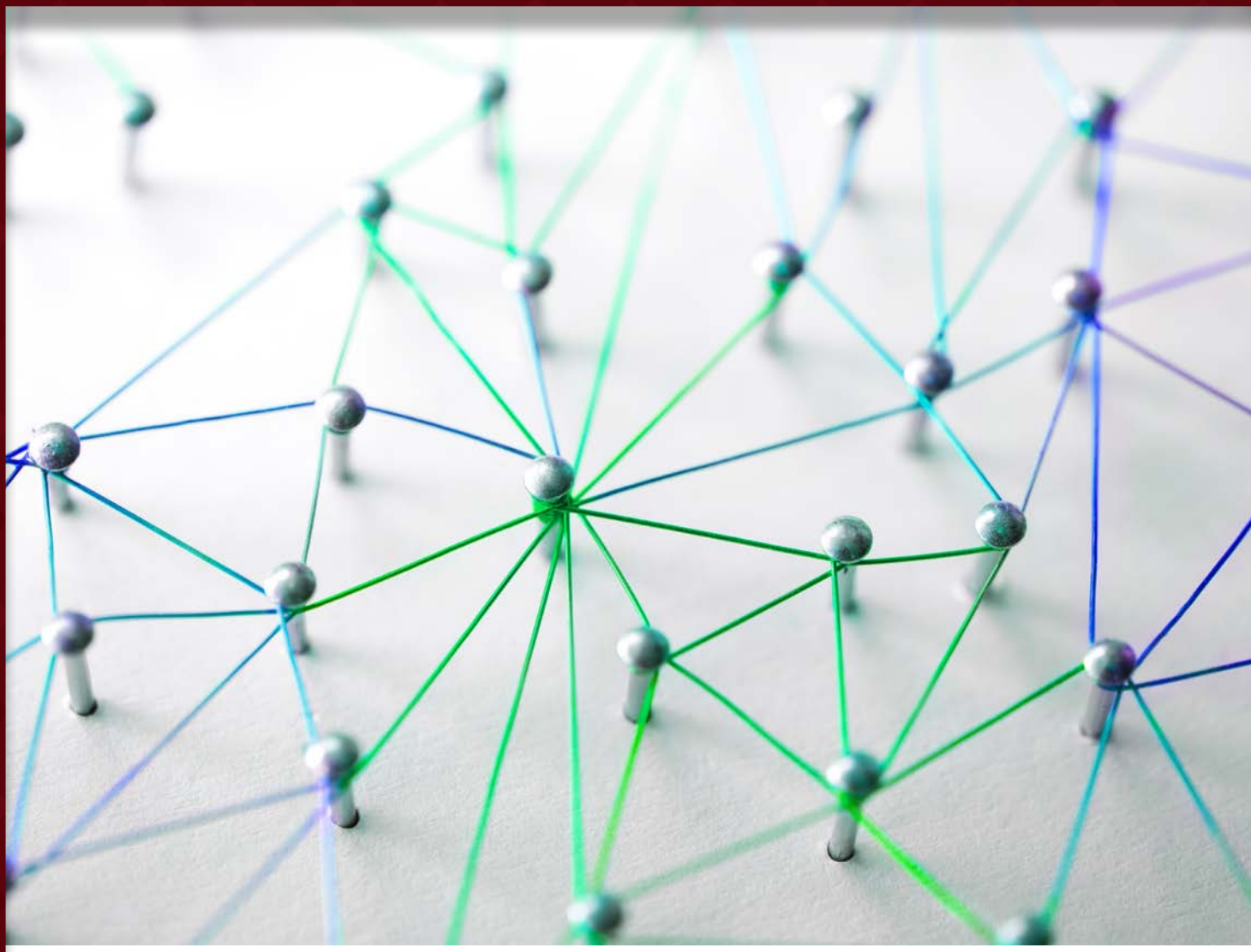
E: unswlrs@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

REVISTA PDP

Revista Uruguaya de Protección de Datos Personales

NÚMERO 4 - agosto, 2019

UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES



DOCTRINA

- *CARLA BARBOZA*
- *EDUARDO BERTONI / SOFÍA DOMÍNGUEZ BARANDICA*
- *GRAHAM GREENLEAF*
- *DANA HALLINAN*
- *JUAN ANTONIO TRAVIESO*
- *FERNANDO VARGAS*

CONVENIO 108 Y TEXTO EXPLICATIVO

DICTÁMENES

NOTA DE INTERÉS

ACTUALIZACION DE LA NORMATIVA EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

ENTREVISTA

CONSEJO EJECUTIVO URCDP

ASIA'S DATA PRIVACY DILEMMAS, 2014-19:

National divergences, cross-border gridlock

GRAHAM
GREENLEAF

Es Profesor de Derecho y Sistemas de Información en la UNSW Australia en Sydney, donde realiza investigación sobre las relaciones entre la tecnología y el derecho. Ha trabajado en protección de datos desde mediados de los años ´70. Su libro de 2014, "Asian Data Privacy Laws" analiza las leyes de privacidad en los 28 países asiáticos. Es Editor para Asia-Pacífico de "Privacy Laws & Business International Report", y publica encuestas bianuales de las leyes de privacidad en el mundo. Ha completado numerosas consultorías para la Comisión Europea en privacidad de datos en países de Asia-Pacífico. En 2018 fue invitado a participar en Bruselas, en el lanzamiento del Reglamento General de Protección de Datos (RGPD) de la UE. Es miembro del Consejo Consultivo del Convenio 108+ y del Grupo Experto de Lineamientos de la OCDE.

SUMARIO

RESUMEN

ABSTRACT

INTRODUCTION: A HALF-DECADE OF CHANGE

- TAKE-UP OF DATA PRIVACY LAWS – REGIONAL COMPARISON

NATIONAL DATA PRIVACY LAWS IN ASIA 2014-19

- NEW DATA PRIVACY LAWS – ONLY ONE 'POST-GDPR'
  - *THAILAND – CAN A JUNTA DELIVER ADEQUACY?*
  - *CHINA – AN ALTERNATIVE MODEL?*
- REVISED LAWS
  - *JAPAN – THE ILLUSION OR REALITY OF ADEQUACY?*
  - *KOREA – A DIFFERENT PATH TO ADEQUACY*
- BILLS IN PROGRESS – THE GDPR MEETS DATA LOCALISATION
  - *INDONESIA – DRAFTS WITH STRONG GDPR INFLUENCES*
  - *INDIA – AFTER PUTTASWAMY, WHERE IS THE BILL?*
- PROGRESS IN OTHER ASIAN JURISDICTIONS
  - *NORTH-EAST ASIA – LITTLE CHANGE IN TAIWAN AND MACAU*
  - *HONG KONG SAR – DEFICITS IN POWERS, BUT TRANSPARENCY CONTINUES*
  - *SOUTH-EAST ASIA (ASEAN) – THE PHILIPPINES (ENERGETIC) AND MALAYSIA (INACTIVE)*
  - *VIETNAM – LIGHTER DATA LOCALISATION*
  - *SINGAPORE – ENFORCEMENT AND RESISTANCE*
  - *SOUTH ASIA (SAARC) – LITTLE TO SEE*
  - *BHUTAN – DATA PRIVACY AS GROSS NATIONAL HAPPINESS*

INTERNATIONAL STANDARDS, DATA EXPORTS AND LOCALISATION

- *ASIA'S LACK OF REGIONAL STANDARDS*
- *THE G20'S 'OSAKA TRACK', THE WTO AND BRICS DISSENT*
- *THE CPTPP LIMITS LOCALISATION AND EXPORT RESTRICTIONS*
- *APEC-CBPRS' CONTINUING FAILURE*
- *WILL THE EU'S 'ADEQUATE' LIST EXPAND IN ASIA?*
- *OTHER 'APPROPRIATE SAFEGUARDS' FOR TRANSFERS FROM THE EU (AND ELSEWHERE)*

CONCLUSIONS: NO GRAND SOLUTIONS LIKELY

- *NATIONAL LAWS AND PRACTICES – UNEVEN EMULATION AND 'GDPR CREEP'*
- *INTERNATIONAL COMMITMENTS – GRIDLOCK AD INFINITUM?*
- *DATA PRIVACY DILEMMAS IN ASIA*

RESUMEN

En 2014, trece de los 28 países de Asia sancionaron leyes de protección de datos. Todos ellos implementaron los diez principios mínimos (Primera generación) para una ley de protección de datos que se ha consolidado en los instrumentos de la OCDE y el Consejo de Europa de 1980/81. También implementaron poco más de la mitad de los adicionales diez principios (Segunda generación) que distinguieron la Directiva de protección de datos de la UE de 1995. En relación de flujos transfronterizos, una variedad de instrumentos pelean por la primacía.

Cinco años después, mucho ha cambiado en Asia, a pesar de que el número de países con leyes de protección de datos se ha elevado solo a 15 (agregando China y Bhutan). Leyes actualizadas incluyen aquellas de Tailandia, la primera ley con una fuerte influencia del RGPD, y en Japón y Corea, afectados por su apuesta a una adecuación a la UE. India e Indonesia tienen leyes con fuerte influencia del RGPD, pero -como China- también poseen fuertes compromisos con la localización de los datos. Este artículo releva todos estos desarrollos nacionales en término de cuáles son los nuevos modelos para leyes de protección de datos que están emergiendo en Asia.

El resultado global de los desarrollos nacionales de este lustro es que la media de las leyes asiáticas ha virado de la inclusión de 5/10 principios de "segunda generación" o principios "europeos", a 6/10. Mas aún, hay al menos 40 instancias de principios de "tercera generación" tipificados por innovaciones del RGPD de la UE que han sido adoptados por las leyes asiáticas, el más popular de los cuáles es el conjunto de requerimientos para la notificación de vulneraciones de seguridad. La sanción de leyes influenciadas por el RGPD en India e Indonesia fortalecerá estas tendencias. No obstante, la ausencia de estándar regionales significativos en Asia (en comparación con África o América Latina) implica que la adopción de principios particulares no es uniforme, y la "convergencia" no es para ésta un concepto muy valioso.

A pesar de que numerosos instrumentos internacionales y sus efectos son influyentes en Asia (el acuerdo de libre comercio CPTPP, APEC-CBRs, Convenio 108+, y la adecuación del RGPD), ninguno de estos se ha convertido en dominante, o no parece que vaya a serlo. Como resultado, los países individualmente podrán optar por involucrarse con ellos en función de sus intereses nacionales y otras obligaciones. Este nuevo elemento de las leyes de localización de datos es influyente en varios países, está distorsionando alianzas tradicionales, y está causando el surgimiento de nuevos modelos para leyes de protección de datos, particularmente aquellos que incluyen la localización de datos.

ABSTRACT

In 2014, thirteen of the 28 countries in Asia[1] had enacted data privacy laws. They all implemented the ten minimum ('1st generation') principles for a data protection law which had consolidated in the 1980/81 OECD and Council of Europe instruments. They also implemented a little over half of the additional ten '2nd generation' principles which distinguished the 1995 EU data protection Directive. In relation to cross-border transfers, a variety of instruments contended for primacy.

Five years later, much has changed in Asia, although the number of countries with data privacy laws has only risen to 15 (adding China and Bhutan). Amended laws include those in Thailand, the first law with strong GDPR influences, and in Japan and Korea, affected by their bids for EU adequacy. India and Indonesia have Bills with strong GDPR influences, but – like China – also strong commitments to data localization. This article assesses all these national developments in terms of whether new models for Asian data privacy laws are emerging.

The overall result of this half-decade of national developments is that the average of Asian laws has moved from the inclusion of 5/10 '2nd generation' or 'European' principles, to 6/10. Furthermore, there are at least 40 instances of '3rd generation' principles typified by the innovations of the EU's GDPR being adopted in Asian laws, the most popular being data breach notification requirements. Enactment of GDPR-influenced laws in India and Indonesia will strengthen these trends. However, the absence of any significant regional standards in Asia (in comparison with Africa or Latin America) means that the adoption of particular principles is not uniform, and 'convergence' is not a very valuable concept in Asia.

Although numerous international instruments and their effects are influential in Asia (the CPTPP free trade agreement, APEC-CBPRs, Convention 108+, and GDPR adequacy), none of these have become dominant, or are likely to. As a result, individual countries will choose to engage with them as suits their national interests and other obligations.

1 *From Japan to Afghanistan going E-W and China to Timor Leste going N-S.*

The new element of data localization laws is influential in quite a few countries, is disrupting traditional alliances, and is causing new models for data privacy laws to emerge, particularly those including data localization.

INTRODUCTION: A HALF-DECADE OF CHANGE

Five years ago in 2014, 13 of the 28 countries in Asia[2] had enacted data privacy laws. My overall conclusion about the standards adopted by those laws[3] was that, with minor exceptions, they all implemented the ten minimum ('1st generation') principles for a data protection law found in the 1980/81 OECD privacy Guidelines and Council of Europe data protection Convention 108. On average, they also implemented a little over half of the additional ten '2nd generation' principles which distinguished the 1995 EU data protection Directive (and in most cases the 2001 amending protocol to Convention 108). Asia's laws had thus advanced from the 1980s' minimum standards 'half way' toward the higher standards of the Directive.[4] This was less than the average standard of data privacy laws outside Europe, as assessed in 2012, which was enactment of 6.9 of the 10 '2nd generation' principles, largely because European influences on many Latin American and African countries were stronger than in Asia.[5]

In relation to enforcement, using the standards of 'responsive regulation' theory,[6] my conclusion was that South Korea and the Macau SAR had 'the widest range of enforcement mechanisms', and made effective use of them.[7] Hong Kong, while lacking legislative enforcement mechanisms until 2012, compensated by very vigorous enforcement activity. The laws in some countries like Singapore, Malaysia and the Philippines were too recent for assessment. There was little credible evidence of enforcement in Japan, Taiwan and India. Related to this, the previous 'Asian civil law model' of Ministry-based enforcement was now limited to these three countries of 'regulatory failure', plus Vietnam, and was in decline. The alternative model of a specialist data protection authority (DPA), though not necessarily an independent one, had been adopted by the newest Asian laws (Singapore, Malaysia and the Philippines), and the other earlier laws.

In mid-2019, there are now 15 Asian countries with data privacy laws meeting minimum standards, with China and Bhutan being the new entrants, plus Thailand having enacted a completely new law to replace an old and useless one. Japan has also enacted a major revision of its law, Korea various lesser revisions (and one ongoing), and there are smaller changes in other countries. Very significant wholesale replacement laws are in the process of enactment in India and Indonesia. It is therefore an opportune time to review the conclusions reached in my 2014 book, in light of a further half-decade. The details of these changes to national laws and practices are the subject of the first half of this article. References to specific sections of legislation may be found in the articles cited herein, but are generally not included in this survey.

Such a review must also take into account the multilateral instruments (treaties, declarations, guidelines etc) that affect the content and interaction of Asian data privacy laws, particularly on the crucial topic of data export restrictions, and its newly-recognised cousin, data localisation. In 2014 I dismissed the idea of a regional data privacy treaty in Asia as unrealistic, and likewise any idea of a new treaty originating from the UN, whereas the 'globalisation' of Convention 108 was seen as more realistic (but with no attempt to suggest what Asian countries might accede to it). 'Interoperability' between EU standards and APEC-CBPRs was described as 'an unrealistic goal'.[8] The second part of the article reviews changes in these multilateral arrangements over the past five years.

2 *From Japan to Afghanistan going E-W and China to Timor Leste going N-S.*

3 *G. Greenleaf Asian Data Privacy Laws: Trade and Human Rights Perspectives (OUP, 2014, paperback 2017), pp. 502-3 summary, and preceding chapter.*

4 *The 'principles' included in these ten include the Directive's requirements of and independent DPA, and access to judicial remedies, more accurately described as 'standards' than 'principles'.*

5 *The 'principles' included in these ten include the Directive's requirements of and independent DPA, and access to judicial remedies, more accurately described as 'standards' than 'principles'.*

6 *Greenleaf, Asian Data Privacy Laws, pp. 62-75.*

7 *Greenleaf, Asian Data Privacy Laws, pp. 526-7, and preceding chapter.*

8 *Greenleaf, Asian Data Privacy Laws, pp. 550-1.*

TAKE-UP OF DATA PRIVACY LAWS – REGIONAL COMPARISON

The following Table[9] provides a regional analysis of the 135 countries that now have data privacy laws.[10] Of the total of 231 countries, the 135 with data privacy laws constitute 58%, and since about 2014 (then 115 countries with laws) the majority of countries have had such laws. Asia, now with 15 of 28 countries (54%) is close to the global average. Of the larger regions (20 countries or more) outside Europe, Latin America (55%) is much the same as Asia, and Africa (46%) is next. Data privacy laws are indeed global: the only region with less that 40% of countries having them is the Pacific Islands, with none.

Region	Countries	DP Laws	%
Africa	58	27	46%
Caribbean	29	12	41%
Other European	29	26	90%
EU	28	28	100%
Asia	28	15	54%
Latin America	22	12	55%
Middle East	14	8	57%
Pacific Islands	13	0	0%
Central Asia	6	3	50%
N. America	2	2	100%
Australasia	2	2	100%
TOTAL	231	135	58%

9 *In the Table, the whole number of countries in a region is compared with the number of countries with data privacy laws, and the percentage result then shown. The number of 'countries per region' is based, with modifications to accommodate my division into regions, on Internet World Stats, Country List <http://www.internetworldstats.com/list1.htm#geo>. The total of 231 countries includes non-UN members, and sub-national regions with distinct top-level domains (such as Hong Kong or Jersey), and therefore is at least as extensive as the criteria I use for a 'country'. All such lists commence from slightly differing assumptions.*

10 *For 135 countries, Uganda, Nigeria and Kyrgyzstan must be added to the 132 countries with laws listed in G. Greenleaf 'Global Tables of Data Privacy Laws and Bills (6th Ed January 2019)' (2019) Supplement to 157 Privacy Laws & Business International Report (PLBIR) 16 pgs <https://ssrn.com/abstract=3380794>.*

NATIONAL DATA PRIVACY LAWS IN ASIA 2014-19

Although in the last five years Asia has not experienced the speed of change of data privacy laws of the preceding five years, there has still been substantial change, taking into account new laws, revised laws, enforcement changes, and particularly Bills in progress.

NEW DATA PRIVACY LAWS – ONLY ONE 'POST-GDPR'

The most significant legislative changes in Asia since 2014 are that Thailand and China now have much stronger data privacy laws, with Thailand significantly influenced by the EU's 'GDPR model', and China developing what may be an alternative model of its own.

Thailand – Can a junta deliver adequacy?

A military coup in 2014 imposed a junta government, which in February 2019 enacted a data privacy law to replace an old and ineffective law applying only to the public sector. This occurred three weeks before Thailand's first general elections since the coup. A military-backed party now leads a coalition government, including a Prime Minister and Cabinet members from the previous military government, and a largely appointed upper house.

Thailand's *Personal Data Protection Act* (PDPA) will come into force on 28 May 2020, a year after it was gazetted. It is based on a GDPR-influenced Bill proposed by the junta government in May 2018,[11] but it has many differences from that Bill. Only some of the notable points on which the Act differs from that 2018 Bill, which take a different approach to the EU's GDPR, or are significant internationally, are discussed here.

The PDPA is a comprehensive Act, unlike the private-sector-only laws in the rest of ASEAN (Philippines excepted). It exempts few parts of the private sector (credit reporting has a separate law) or public sector (courts, legislature, security and law enforcement), but further exemptions can be made by decree.

The PDPA has some stronger principles influenced by the GDPR, including the data subject's right to data portability; the right to object; data breach notifications to both the data subject and the DPA;

11 *The 2018 Bill is examined in G. Greenleaf and A. Suriyawongkul 'Thailand's draft data protection Bill: Many strengths, too many uncertainties' (2018) 153 Privacy Laws & Business International Report, 23-2*

minimal collection requirements; data retention restrictions; and strong consent requirements. Genetic and biometric data have been added to the categories of 'sensitive personal data', consistent with the GDPR. Appointment of data protection officers (DPOs) will be required, with exceptions for a 'small sized business' (criteria to be specified by PDPC). Some notable aspects of the GDPR, such as the right to be forgotten, and protections in relation to automated processing, are not included.

The PDPA will have extra-territorial effect (similar to the GDPR) in relation to marketing to, or monitoring of, persons in Thailand. Processing outside Thailand by a controller or processor located in Thailand is also covered.

A Personal Data Protection Committee (PDPC) is established as the primary body to administer the law, but it has no legislatively guaranteed independence. There is also an Office of the PDPC, which is a government department. Expert Committees will determine complaints. Many breaches of the PDPA can result in administrative fines, for which the highest maximum amount is 3 million baht (approx. US$100K). This is now a low maximum by international standards, but may still be a deterrent to some local businesses. Data subjects have a right to seek compensation from a court for any breaches of the Act (and with few defences provided), and the court may impose additional compensation up to double the original amount (ie 'triple damages').

Data exports from Thailand can occur to countries which have an 'adequate level of protection', as determined by the PDPC. However, 'adequate' is to be determined by criteria set by the PDPC, so it cannot be assumed that it will mean the same as it does in the EU. Additional provisions allowing data exports include a form of Binding Corporate Rules (BCRs), and undefined 'appropriate safeguards', both to be based on standards set by PDPC.

The main significance of the Thai law is that it is the first explicitly 'GDPR-based' law to yet be enacted in Asia. However, there are GDPR-influenced draft Bills in India and Indonesia.

China – An alternative model?

From 2011-14 China enacted five main largely consistent laws and regulations dealing with data privacy, at various levels in its complex legislative hierarchy. A number of omissions (particularly lack of subject access) meant that they were close to, but did not quite comprise, the minimum requirements for a data privacy law.[12]

The data privacy provisions of China's *Cybersecurity Law* of 2016 were China's most comprehensive and broadly applicable set of data privacy principles up to 2017, going beyond the previous laws.[13] However, that law was still missing explicit user access rights, requirements on data quality and special provisions for sensitive data, as well as having no specialist data protection authority (DPA), and being of uncertain scope in relation to the public sector. The omission (or ambiguity) of the first of these – explicit subject access rights – meant that China's law as a whole did not yet include one of the most fundamental elements of a data privacy law. However, these doubts are now sufficiently resolved. The *E-Commerce Law* of 2018 (in force 1 January 2019), a law of China's second highest legislative body, is both of wide scope within the private sector, and explicitly provides that users may make 'inquiries' concerning their information.[14] Since then, there have been two further significant developments.

The recommended standard entitled *Information Security Techniques - Personal Information Security Specification* promulgated by China's National Standardization Committee, and effective 1 May 2018[15] 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' (possibly broader than any other Chinese laws, or European laws); 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. The suggested obligations in relation to subject access, minimum collection of data, and restrictions on automated processing, are not found in other (enforceable) laws. Although only a 'standard', businesses must think twice before failing to observe a recommended standard, and it is probably realistic to consider the requirements of the 'standard' to already be part of China's data privacy law.

12 *Greenleaf Asian Data Privacy Laws (2014), pp. 225-6, and preceding chapter.*

13 *G Greenleaf and S Livingston 'China's Cybersecurity Law – also a data privacy law?' (2016) 144 Privacy Laws & Business International Report, 1-7 <https://ssrn.com/abstract=2958658>*

14 *E-Commerce Law of the People's Republic of China (Standing Committee of the National People's Congress, 31 August 2018) Art 24 "Where e-business operators receive applications for inquiries, modification, or deletion of user information, they shall promptly make the inquiry, or modify or delete the user information, after identity verification' (Source: China Law Translate).*

15 *G. Greenleaf and S. Livingston, 'China's Personal Information Standard: The Long March to a Privacy Law' (2017) 150 Privacy Laws & Business International Report 25-28. < https://ssrn.com/abstract=3128593>*

China has not yet finished its data privacy legislation agenda. A 'Personal Information Protection Law' and a 'Data Security Law', are each listed separately on the work program for the current National People's Congress (NPC).[16] They are 'Class I Projects: Draft laws for which the conditions are relatively mature and which are planned to be submitted for deliberation during the term (69 projects)', and should 'in principle' be completed within the 13th NPC's term, which will end in March 2023.' It may turn out that the above 'standard' is a test-bed for what will eventually be China's comprehensive data privacy law.

It must always be borne in mind that China's data protection laws co-exist with the Social Credit System (SCS), which is emerging as the world's most pervasive and potentially totalitarian surveillance system, but as yet is far from complete.[17] The relationship between the SCS and data privacy laws is unclear.

Two years after the *Cybersecurity Law* came into force, China is still finalising the data export and data localisation rules based on that law. On June 13, 2019, the Cyberspace Administration of China (CAC) issued, for a month's consultation, the draft *Measures on Security Assessment of the Cross-border Transfer of Personal Information* ('draft Measure on Security Assessment').[18] This second iteration of these Measures imposes them more broadly than before: 'all network operators are obliged to undergo the security assessment process before they may transfer personal information collected in the course of their operations in China to recipients outside China',[19] not only Critical Information Infrastructure operators. There are numerous requirements for the security assessment, and then further rules concerning notice to, opt-in and opt-out by data subjects, and assumption of liability by exporters. These requirements have compared with the EU's SCCs and BCRs, but the security assessment aspect makes them very different.[20]

The general data localisation provisions of the *Cybersecurity Law* have been in force since 2017, providing that all personal data and 'important data' held by 'critical information infrastructure' operators (CIIOs) must be stored in China.[21] The Law does not itself define 'critical information infrastructure', so its meaning has to be inferred from other documents.[22] However, because implementing regulations for the data localisation aspects are not included in the 2019 version of the draft *Measures on Security Assessment*, there is still uncertainty about what China's localization policies require.

There are many respects in which China's data privacy laws could be emulated (and promoted by China) as a model for data privacy regulation which is an alternative to the 'western' (more accurately 'European') model: (i) inclusion of enforceable principles which at least meet the '1st generation' criteria of the OECD Guidelines and Convention 108 (1980/81 versions); (ii) inclusion of strong data localisation requirements and data export restrictions which are more oriented to protection of State or national interests than to protection of individual citizens; (iii) the absence of a central (let alone independent) data protection authority (DPA); (iv) data privacy laws to be subordinate to data surveillance laws (such as those governing the Social Credit System); (v) optional whether the public sector is covered. Such an 'authoritarian model' of data privacy protection may have an appeal outside China, underwritten by China's economic weight and success.

16 *NPC Observer <https://npcobserver.com/2018/09/07/translation-13th-npc-standing-committee-five-year-legislative-plan/>*

17 *For an authoritative assessment, see R. Creemers 'China's Social Credit System: An Evolving Practice of Control' (May 9, 2018) <https://ssrn.com/abstract=3175792 or http://dx.doi.org/10.2139/ssrn.3175792>; also Y. Chen and A. Cheung 'The Transparent Self Under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System' (2017) Vol. 12, No. 2, The Journal of Comparative Law 356-378 < https://ssrn.com/abstract=2992537>; for recent information, K. Needham 'Millions are on the move in China, and Big Data is watching' Sydney Morning Herald, 6 February 2019 <https://www.smh.com.au/world/asia/millions-are-on-the-move-in-china-and-big-data-is-watching-20190204-p50vlf.html>*

18 *Draft Measure on Security Assessment (China), unofficial English translation <https://www.insideprivacy.com/wp-content/uploads/sites/6/2019/06/Measures-for-Security-Assessment-of-the-Cross-Border-Transfer-of-Personal-Information_bilingual.pdf>*

19 *Yan Luo, Zhijing Yu and Nicholas Shepherd 'China Seeks Public Comments on Draft Measures related to the Cross-border Transfer of Personal Information' Inside Privacy, 13 June 2019*

20 *Yan Luo, Zhijing Yu and Nicholas Shepherd, ibid.*

21 *See for background S. Livingston and G. Greenleaf 'PRC's New Data Export Rules: 'Adequacy with Chinese Characteristics'?' (2017) 147 Privacy Laws & Business International Report 9-12; <https://ssrn.com/abstract=3026914>.*

22 *Livingston and Greenleaf 'PRC's New Data Export Rules' ibid.*

REVISED LAWS

Japan's law has been revised, but is not of a high standard (except for Europeans), whereas Korea is taking a different path.

Japan – The illusion or reality of adequacy?

Japan's data privacy laws, of which the centrepiece was the Act on the Protection of Personal Information (PPIA) of 2003, were characterised by me in 2014 as 'weak and obscure', with ambiguous and low-grade principles, and no credible evidence of enforcement. 'The illusion of protection' was the chapter title.[23]

In 2015 Japan enacted reforms to bring Japan's PPIA closer to international standards, including creation of a data protection authority, the Personal Information Protection Commission (PPC), which has enforcement powers, jurisdiction over the private sector (only), and requirements to act independently. The Bill enacted was significantly stronger than was indicated by early drafts. Nevertheless, its principles had many weaknesses, including a narrow concept of 'personal information'; low standards for both change of use (allowing 'duly related' uses) and disclosure to third parties (an 'opt out' procedure); no deletion requirements; obscure provisions on access and correction; no extra protection for sensitive information; and an exemption for businesses 'considered unlikely to violate the individual's rights'.[24] The enforcement provisions are minimal, with no clear provisions for the making of complaints; PPC powers to issue administrative fines limited to about US$10,000; criminal procedures that, on past experience, will never be used; and no rights to individuals to obtain compensation from the PPC or the courts.

A significant part of the 2015 PPIA reforms were 'big data' provisions concerning use of allegedly 'anonymised' data. A new concept of 'anonymous process information' (API) was introduced, but because it follows a prescribed method of anonymisation, rather than objective criteria of non-identifiability, it was obvious that it would not be consistent with EU approaches to this topic. Although API is not 'personal information', many protective provisions similar to those applied to personal information apply to API.

The European Commission decided in January 2019 that Japan's data protection system met the GDPR art. 45 requirements for a positive adequacy decision.[25] There were a number of unusual aspects of the approaches that Japan and the EU took to finalising this decision, some of which are:[26]

- Japan's post-2015 law fell short of EU requirements in four respects which Japan's PPC (DPA) addressed by making Supplementary Rules to remedy those deficiencies.[27] However, these Rules only apply to personal data originating from the EU (thus probably primarily affecting EU citizens), and do not apply to personal data sourced from Japan, or from other foreign countries. The question of whether the concept of 'essentially equivalent' protections, as required by the GDPR and the CJEU, can be satisfied by laws which, in effect, give a lower level of protection to Japanese citizens, is not addressed in the Decision,[28] but the Commission says it is 'Japan's choice' to take this approach.[29]
- GDPR art. 45 explicitly requires 'effective and enforceable data subject rights' and 'effective judicial and administrative redress'. The EDPB states that these are 'of paramount' importance' and that infringements 'should be punished in practice' and compensation awarded.[30]

23 *Greenleaf, Asian Data Privacy Laws (2014) pp. 263-5 and the preceding Ch. 8 'Japan – The Illusion of Protection.'*

24 *For details see G. Greenleaf, Japan: Toward International Standards – Except for 'Big Data' (June 19, 2015). (2015) 135 Privacy Laws & Business International Report, 12-14 < https://ssrn.com/abstract=2649556>*

25 *[European Union] Commission Implementing Decision of 23.1.2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information < https://ec.europa.eu/info/sites/info/files/draft_adequacy_decision.pdf >*

26 *For detailed critical analysis, see G. Greenleaf 'Japan's Proposed EU Adequacy Assessment: Substantive Issues and Procedural Hurdles' (2018) 154 Privacy Laws & Business International Report, 1, 3-8; extended online version at <https://ssrn.com/abstract=3219728>; G. Greenleaf 'Questioning 'Adequacy' (Pt I) – Japan' (2017) 150 Privacy Laws & Business International Report, 1, 6-11 <https://papers.ssrn.com/abstract_id=3096370>; G. Greenleaf 'Japan and Korea: Different Paths to EU Adequacy' (2019) 156 Privacy Laws & Business International Report, 9-11. <https://ssrn.com/abstract=3323980>.*

27 *(European) COMMISSION IMPLEMENTING DECISION of 23.1.2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information ('Japan Final Decision'), Brussels, 23.1.2019 , C(2019) 304 final; Final Decision paras. (15)-(16).*

28 *If insistence on changes which are not restricted to EU-sourced data is considered to be likely to breach the EU's obligations under GATS art. 14, the Decision could but does not state this.*

29 *Commission statement (B. Gencarelli) to the EU Partliament LIBE Committee, 26 September 2018.*

30 *See Greenleaf 'Japan's Proposed EU Adequacy Assessment' 2018, p. 7.*

Despite it being clear that enforcement and redress must be demonstrated in practice, and not only exist on paper, the Decision ignores this. It lists many examples of where the PPC or the courts can, in theory under legislative provisions, take enforcement actions, but it does not give any examples of specific penalties issued or compensation granted, either administrative or judicial.[31]

- A strong aspect of the Decision is that it makes it clear that the 'Japanese back door', which allowed personal data exports from Japan to overseas companies merely because they are certified under the APEC CBPRs scheme, has been shut in relation to any data originating from the EU, by one of the Supplementary Rules.[32] Such onward transfers now require the consent of the individual data subject in the EU, which is an improvement but still open to criticisms.[33] Under the GDPR, consent is not a basis for transfer to third countries, but is only a very constrained derogation, which the EDPB considers must remain the exception not the rule.[34]
- The Decision is very thorough in explaining where and why Japan's laws meet GDPR standards, but there remain apparent 'gaps' between the GDPR and explicit provisions of Japan's laws. These include: requirements for data protection by design and by default; data portability; mandatory DPIAs; mandatory DPOs; and de-linking ('right to be forgotten'). There is also very weak protections for automated decision-making,[35] and data breach notification requirements which are voluntary,[36] both of very limited scope. While it is clear that 'essentially equivalent' protection does not require the inclusion of every GDPR innovation, the Decision does not provide valuable criteria for assessing what is and is not required.

Unless any of matters is called into question by the CJEU in its interpretation of the GDPR, the Commission's decision disposes of them. Both the European Parliament[37] and the European Data Protection Board (EDPB),[38] in their opinions on the Commission's draft Decision, neither endorse nor reject it. On my interpretation, they each implied but did not expressly state that the Commission had failed to demonstrate the adequacy of Japan's protections. However, they accepted the inevitability of a positive adequacy Decision. The EDPB invited the Commission to review 'this adequacy finding' at least every two years, not four years, and the Commission will do so. The result is that this first adequacy Decision under the GDPR, while very valuable to the EU in demonstrating that positive decisions in relation to its largest trading partners are possible, does not appear to be a strong or clear precedent for future adequacy decisions.

Korea – A different path to adequacy

Korea's has a number of data privacy laws, of which the most significant are the Network Act, covering information content service providers (ICSPs), the Credit Information Act and the Personal Information Protection Act (PIPA) which covers all sectors not covered by other Acts, and has an independent DPA (the PIPC), but one without sufficient powers. Overall, these laws remain the strongest laws in Asia, and by 2014 already included (although not uniformly) many elements of the 1995 Directive and anticipated some elements of the GDPR.[39] Although some aspects of Korea's laws are still in the process of amendment for the purposes of its adequacy application to the EU (discussed below), there have also been numerous changes to strengthen enforcement provisions in Korea's data privacy laws since 2014. Only two of the most important are mentioned here.[40]

Problems caused by difficulties of obtaining proof of damage for consumers in civil damages actions

31 *Japan Final Decision ,Paras. (97)-(112).*

32 *Japan Final Decision, paras (75)-(80); see Greenleaf 2018, pp. 5-7 for reasons why this was necessary.*

33 *Greenleaf, 2018, p.6.*

34 *Greenleaf, 2018, p.6.*

35 *Japan Final Decision, paras. (93)-(94).*

36 *Japan Final Decision, paras. (57)-(59).*

37 *European Parliament, Opinion on the draft Decision concerning Japan, 13 December 2018, para. [27].*

38 *European Data Protection Board (EDPB), Opinion on the draft Decision concerning Japan, 13 December 2018, para. [30]*

39 *See Greenleaf, Asian Data Privacy Laws, Ch. 5 'South Korea – The Most Innovative Law'.*

40 *For details of many of the changes summarised in the following, see Kwang-Bae Park and Hwan-Kyoung Ko, 'Amendments to the Credit Information Act Promulgated on March 11, 2015', Lee & Ko Data Protection / Privacy Newsletter, March 2015 <http://www.leeko.com/newsl/dpp/201503/dpp1503_eng01.html>; Kwang-Bae Park and Hwan-Kyoung Ko, "Amendment to the Personal Information Protection Act Passed in the National Assembly on July 6, 2015 - Adoption of punitive damages, statutory damages provisions", Lee & Ko Data Protection / Privacy Newsletter, July 2015. <http://www.leeko.com/newsl/dpp/201507/dpp1507_eng1.html>; Kwang-Bae Park and Hwan-Kyoung Ko, "MOGAHA Announces Updated 'Standards of Personal Information Security Measures'" Lee & Ko Data Protection / Privacy Newsletter, February 2015.*

following massive data spills were addressed by amendments to all the relevant laws in 2014-15. They provided that defendants may be required by a court to pay statutory damages of up to KRW 3 million (around US$3,000) to each affected user for a negligent or wilful violation of a data protection requirement that causes data loss, theft, or leakage, without the user having to prove actual damage resulting from such violation, and for punitive damages of up to three times the actual damages of the data subject ('treble damages') if the data subject can prove: (i) an intentional or grossly-negligent violation of the law by the handler; (ii) that the data subject's personal information was lost, stolen, leaked, forged, falsified or damaged due to such violation; and (iii) the actual amount of damages resulting from such a violation.[41] The PIPA amendment also added a statutory damages provision that allows a data subject to claim up to KRW 3 million (around US$3,000) in damages when the data subject can prove (i) wilful misconduct or negligence of the handler, and (ii) the fact that data subject's personal information was lost, stolen, leaked, forged, falsified or damaged because of the wilful misconduct or negligence. These provisions for statutory and punitive damages remain in advance of those required by the GDPR.

The Network Act was also amended in 2014 to provide that ICSPs may be required by the Korean Communications Commission (KCC) to pay administrative fines of up to 3% (previously 1%) of the ICSP's annual turnover for failure to obtain user consent prior to the collection and use of personal information. The Credit Information Act was similarly amended in 2015, and similar amendments to PIPA are in the legislative process. The first application of these major penalties was in relation to the 'Interpark data leak'[42] which resulted in KCC imposing a fine ('administrative surcharge') of 4.5 billion won (around US$4.5 million) on one of the largest Korean online shopping malls. Cyber criminals, allegedly associated with North Korea, fraudulently obtained personal information of 10.3 million customers, and attempted to blackmail the company for KRW 3 billion (around US$3 million). The fine was imposed for negligent failure to protect customer data, and was 60 times higher than previous fines. Korea's progressive enactment of administrative fines of up to 3% of turnover from 2014 onward was in advance of the EU, and the Interpark fine of US$4.5 million was larger than any fine in the EU prior to CNIL's fine against Google of 50 million euros in January 2019, now dwarfed by the UK ICOs proposed July 2019 fines against British Airways (£183 million) and Marriott (£99 million). This fine is also the largest in Asia, approximately five times larger than the largest Singaporean fine.

Korea is seeking an adequacy assessment from the EU, with progress being described by the European Commission as being 'at an advanced stage'.[43] Bills to comprehensively amend Korea's four main data privacy laws were introduced into Korea's National Assembly in November 2018 to advance this goal, but are not yet enacted. The key Bill is the *Partial Amendment to the Personal Information Protection Act*.[44] The Bills have three main purposes[45], each of which is discussed further here.[46]

- Korea's previously proposed scope of an adequacy decision was limited to those parts of the private sector under the 'Network Act' and the jurisdiction of the Korean Communications Commission (KCC). This was primarily because the Personal Information Protection Commission (PIPC), while independent in its decision-making, did not have any independent powers to enforce its decisions but had to rely upon enforcement by the Ministry of the Interior and Safety (MOIS). The Korean government and the European Commission agreed that this approach was too narrow to provide meaningful benefits to EU-Korean trade, from either the Korean or EU perspectives. Korea therefore proposed to make the PIPC a 'central administrative agency' under the Prime Minister, with independent authority over all situations of processing of personal information, and to transfer to it all powers and functions of the Ministry under PIPA, and of KCC under the Network Act. PIPC is also to be empowered to investigate violations and to impose administrative fines up to 3% of turnover, the power currently held by KCC

41 *PIPA (Korea), art. 39(3); Network Act (Korea), art. 32(2).*

42 *Whon-il Park 'Interpark data leak' (KoreanLII, 2017) <http://koreanlii.or.kr/w/index.php/Interpark_data_leak>.*

43 *European Commission Media Release 'Commissioner Jourová's intervention at the event "The General Data Protection Regulation one year on: Taking stock in the EU and beyond" Brussels, 13 June 2019 <http://europa.eu/rapid/press-release_SPEECH-19-2999_en.htm>*

44 *All sections quoted are from an unofficial draft translation provided by the KCC.*

45 *Kwang Bae Park et al 'Korea's Proposed Overhaul of Data Protection Laws' (156) Privacy Laws & Business International Report*

46 *All of these points are discussed in more detail, with section references to Bills, in G. Greenleaf 'Japan and Korea: different paths to EU adequacy' (2019) 156 Privacy Laws & Business International Report 9-11 <https://ssrn.com/abstract=3323980>.*

but not by PIPC. The European Commission will have to assess whether these no doubt welcome proposals will meet the GDPR's technical standards for the necessary powers and independence of a DPA. These reforms represent a considerable shift in bureaucratic power, and it still remains to be see the extent to which they will be enacted.

- Similar to Japan, Korea is now proposing to deal with aspects of 'big data' processing directly in PIPA, rather than under the 2016 'Big Data Guidelines', which had no clear legal status. The PIPA Bill distinguishes personal information, pseudonymized information and anonymized information in ways which are appear to be consistent with the GDPR. However, to accommodate 'big data' processing, the Bill provides that a controller 'may process pseudonymized information without the consent of the data subject for the purpose of statistics, scientific researches, public-interest archiving, etc.'. 'Process' includes disclosure to third parties, so this is an area of considerable privacy dangers, particularly in the breadth of meaning of 'statistics' and 'scientific research', which will raise significant issues in adequacy discussions with the EU.
- Various other provisions in the reform Bills will, if enacted, move Korea's laws closer to the GDPR. One has a 'data portability' right, and includes limits on automated decision-making. To address a perceived weaknesses in Korea's current laws concerning data exports, compared with GDPR standards, 'special provisions regarding (i) safeguards to be implemented for the cross-border transfer of personal information, (ii) restrictions on the onward transfer of personal information, [and] (iii) the designation of a local representative'.[47] Some overseas providers of information services within Korea will be required to nominate a 'domestic agent' (local representative) to carry out duties of a chief privacy officer and fulfill reporting obligations, and the overseas provider will be liable for their failures to do so. Transfer of personal data overseas will generally require the consent of the data subject, based on notifications, including of the data to be transferred, the country of the recipient, the recipient's identity, the purpose of transfer and the duration of retention of data, and the transferor must take any other protective measures required by Presidential Decree. The same restrictions purport to apply to any further onward transfers by that recipient, but whether such an exercise of extra-territorial jurisdiction will be effective is questionable.

When and to what extent these proposed reforms are enacted will have a significant effect on the nature of the EU's adequacy assessment of Korea. Although adequacy negotiations are not public, Korea's approach appears to be very different from that taken by Japan, because there is no equivalent to Japan's Supplementary Rules which apply stronger GDPR-like provisions only to EU-origin personal data but not to Japan-origin data. The Korean approach has been to strengthen its law through legislation applying to all personal data, irrespective of its source, although it is likely that Presidential Decrees will be needed to clarify some issues between Korea and the EU, once adequacy negotiations advance further. It will be very valuable to the privacy of the Korean people, and also to the future of the EU concept of adequacy, if Korea continues its inclusive approach by making such Decrees apply to all personal data, irrespective of its source, and rejects Japan's insular approach.

BILLS IN PROGRESS – THE GDPR MEETS DATA LOCALISATION

The largest and third largest countries in Asia by population, India and Indonesia, each of which is advancing economically at a rapid rate, are likely to enact data privacy laws within the next year or two. These laws which will be comparable to that of Thailand, being laws enacted by democracies, covering both public and private sectors, with a DPA (possibly one which is independent), and with many principles influenced by the EU's GDPR, but also with data localisation provisions. If and when enacted, these laws will change the landscape of data privacy in Asia.

Indonesia – Drafts with strong GDPR influences

Indonesia already has a data privacy law which meets minimum standards, partly from a pre-2014 law and regulation which constituted 'a short enforceable privacy code',[48] and significantly expanded into a minimum standards data privacy

47 *Park et al, cited above.*

48 *G. Greenleaf Asian Data Privacy Laws (2014), pp. 374-388, concerning Article 26 of Law No 11 of 2008 concerning Electronic Information and Transactions (Law 11/2008) and Government Regulation No 82 of 2012 on the Implementation of the Electronic Transactions and Information Law (GR 82/2012)*

law by a regulation in 2016.[49] However, these laws remain largely unenforced, mainly because there is no data protection authority to oversee them. Various branches of the Indonesian government have been drafting a comprehensive new law since 2015 or earlier. The Minister of Communication and Informatics (MOCI) (Kementerian Komunikasi dan Informatika (Kominfo) in Bahasa) has lead responsibility for the drafting of a comprehensive Data Protection Bill, in consultation with other government bodies. An internal government version (April 2018) is the basis of the following summary,[50] but the final version will inevitably differ from any drafts.

The main point to be made is that the draft Bill has many strengths, when compared with the GDPR as a global high standard. GDPR-compatibility is one of the Indonesian government's objectives. The Bill provides comprehensive coverage of both private and public sectors, and of all persons in Indonesia. There is some extra-territorial coverage (but not based on GDPR criteria), relating to acts outside Indonesia which have consequences in Indonesia, or harm Indonesia's national interests. There are few exemptions from the whole Act, with most exceptions only from specific principles, and no general exemption for publicly available information.

The principles included are extensive, covering all basic principles plus the following: a vague right to request limitation of processing; opt-in (consent) required for both pseudonymous processing and direct marketing; and data breach notification to individuals required. 'Specific' (or sensitive) personal data includes the conventional categories (excluding religious beliefs), plus genetics and biometrics.

A Commission (DPA) is established to administer the law, responsible directly to the President. It may investigate and adjudicate on infringements; to conduct mediation between parties, with agreed results of mediation being enforceable. This 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.

The DPA may impose administrative penalty sanctions of at least US$75,000 (1BN rupiah), and up to 25 times as much (25 BN rupiah). Compensation claims may be made to a court, or to the Commission, for any infringements. Criminal offences apply to many breaches of the Act, the most severe with potential sentences of 10 years gaol.

Personal data transfers outside Indonesia may be justified in various ways: the consent of the data subject; or the law of the recipient country providing 'an equal or higher level of protection' than Indonesia's; or based on contract or international agreements; or an exemption from the Commission. The Commission may determine a White List based on strength of foreign laws.

On the other hand, there are many apparent limitations of the Bill, when compared with the GDPR (although some may result from inadequate translation). There is no automatic destruction of personal data once the purpose of collection is completed, it must be requested. The Commission does not appear to have legislatively guaranteed independence or tenure (but perhaps this may arise otherwise under Indonesian law). Many new GDPR principles do not appear to be included, such as: separate obligations imposed on processors; requirements for Data Protection Officers (DPOs); Data Protection Impact Assessments (DPIAs); data portability; and a right to have human review of automated decisions. Indonesia already has a version of the 'right to be forgotten' from a 2016 amendment, but its implementation depends on regulations yet to be made (and is otherwise left to the Courts). It is not stated in this Bill.

Despite these limitations (some of which may be resolved by translation clarifications), my initial overall assessment is that a Bill like this, if enacted, would be one of the stronger laws in Asia, with standards much higher than the minimum standards for a data privacy law, placing Indonesia among the Asian counties with the strongest GDPR influences.

Current data export restrictions in Indonesia are complex and obscure.[51] However, there are several

49 *Regulation No 20 of 2016 concerning Personal Data Protection in Electronic Systems (MCI 20/2016), an implementing measure mandated by GR 82/2012, added considerable detail to both previous laws, and provides a two-year transition period for full compliance (ie to 1 December 2018). ; see A. A. Rahman 'Indonesia to Introduce Personal Data Protection Rules in Electronic Systems' (2016) <https://andinadityarahman.com/indonesia-to-introduce-personal-data-protection-rules-in-electronic-systems/>; More detailed version: 'Indonesia Enacts Personal Data Regulation' (2017) 145 Privacy Laws & Business International Report 1.*

50 *The government subsequently released another, less developed, version for public discussion – see Baker & McKenzie 'Indonesia: Government Pushes Draft Data Protection Law' Global Compliance News May 18 2018 <https://globalcompliancenews.com/indonesia-draft-data-protection-law-20180518/> .*

51 *J. P. Kusumah and D. Kobrata Jurisdictional Report – Indonesia in C. Girot (Ed.) Regulation of Cross-Border Transfers of Personal Data in Asia (ABLI, 2018), paras. 19-20, 30-39, and 61 <https://abli.asia/PUBLICATIONS/Regulation_of_Cross-border_Transfers_of_Personal_Data_in_Asia>.*

Indonesian regulations already requiring 'data localisation', in the following areas:

- *Electronic system providers (ESPs) offering public services* – Data centres/recovery centres must be located in Indonesia, but provided a copy of the data is kept in Indonesia, it does not appear that there is a prohibition on a copy being transferred abroad. The question of what is a 'public service' is complex.[52] These provisions have 'already been used to request a major foreign company to establish its data centre in Indonesia' and 'it appears that the data localisation requirement can apply to foreign entities if the processing or storing of personal data by the foreign entity is considered to have legal implication within Indonesian jurisdiction and/or to have legal implications outside Indonesian jurisdiction but harms the national interest'.[53]
- *ESPs in the financial sector* – All ESPs in the financial sector are required to store in Indonesia all transaction data (in effect, any action with legal consequences made by using a computer, computer network and/or other electronic media).[54]
- *Data centres of banks and insurers* – Separately from questions of electronic transactions, banks must locate their data centres and disaster recovery centres in Indonesia, for all data. Similar requirements apply to insurance, but only for specified types of data. Applications can be made for exceptions.[55]

Although Indonesia has data localisation laws, as do China, Vietnam and India (next discussed), each of these countries' approaches to data localisation is different, as will be discussed in the conclusions.

India – After Puttaswamy, where is the Bill?

At present, India's data protection law is based on an incoherent and largely ignored set of Rules under s43A of the *Information Technology Act*, as amended in 2011. It is probably Asia's weakest data privacy law, from the perspective of citizens' rights. Two applications by India to the EU for a positive adequacy assessment, before and after the 2011 amendments, were unsuccessful, as they should have been. India attempted to demand 'data secure status' as part of EU trade negotiations but was also rebuffed. Various reform Bills failed to proceed.[56]

Since 24 August 2017, the new starting point for understanding of data privacy in India is the unanimous decision of a nine judge 'constitution bench' of India's Supreme Court in *Puttaswamy v Union of India*[57] 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. *Puttaswamy* 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.'[58]

Subsequent smaller constitution benches are now deciding the constitutionality of various pieces of legislation, and practices, in light of the fundamental right of privacy. In *Navtej Johar v Union of India* a unanimous five judge Constitution Bench held[59] that India's criminalization of homosexual conduct (s. 377 of the Criminal Code) was unconstitutional post-*Puttaswamy*). The Indian government decided not to oppose the petition, saying it would leave the decision to the Court. The decision may have wide implications within India.[60] Outside India, the decision has

52 *Kusumah and Kobrata, 2018, paras. 41-51.*

53 *Kusumah and Kobrata, 2018, paras. 47-48.*

54 *Kusumah and Kobrata, 2018, para. 52.*

55 *Kusumah and Kobrata, 2018, paras. 53-57.*

56 *G. Greenleaf Asian Data Privacy Laws (OUP, 2014), pp. 432-3, and preceding chapter.*

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

58 *ibid*

59 *Navtej Singh Johar & Ors. v. Union of India thr. Secretary Ministry of Law and Justice W. P. (Crl.) No. 76 of 2016 (Supreme Court of India) (decided 6 September 2018)*

60 *Alok Prasanna Kumar 'Section 377 judgment could form beginning of a body of path-breaking jurisprudence in India' Scroll 6 September 2018 <https://scroll.in/article/893468/section-377-judgment-could-form-beginning-of-a-body-of-path-breaking-jurisprudence-in-india>; Gautam Bhatia 'The Indian Supreme Court Reserves Judgment on the De-criminalisation of Homosexuality' Oxford Human Rights Hub, 15 August 2018 <http://ohrh.law.ox.ac.uk/the-indian-supreme-court-reserves-judgment-on-the-de-criminalisation-of-homosexuality/>*

already been followed by Botswana's High Court to declare unconstitutional a similar provision.[61]

A five judge constitution bench heard the challenge to the constitutionality of India's 'Aadhaar' (biometric ID) system, and the *Aadhaar Act 2016*. Puttaswamy was again the lead petitioner.[62] The court held by a 4/1 majority that the Aadhaar scheme was capable of being constitutionally valid, but that many aspects of the current *Aadhaar Act 2016* were unconstitutional. Legislation intended to 'remedy' these constitutional deficiencies, and in particular to enable Aadhaar use by the private sector, was enacted in July 2019.[63]

It is very likely that, in order to protect the constitutionality of other legislation and practices, the Indian government will have to legislate comprehensively to protect privacy in relation to both the public and private sectors in India, and to do so consistently with the requirements of *Puttaswamy #1*. The Indian government therefore commissioned the Report[64] of the Committee of Experts under the Chairmanship of Justice B. N. Srikrishna ('Srikrishna Report'), delivered in July 2018, accompanied by a draft *Personal Data Protection Bill 2018* ('Srikrishna Bill').[65] Despite submissions on the draft Bill closing on 10 September 2018, following which the government had undertaken to produce a Bill for introduction to Parliament, no such Bill had emerged by mid-2019. However, the world's largest election had preoccupied India for many months until June 2019. The new IT Minister has announced that one of his key priorities will be to pass the Srikrishna Bill in this Parliamentary session.

It is difficult to adequately convey comparisons between two such complex pieces of legislation as the Srikrishna draft Bill and the GDPR, each of approximately 100 clauses.[66] Only the most important points of comparison are summarised here.

The Data Protection Authority of India (DPAI) to be established, although described as 'independent' is subject to broad instructions from the government. The DPAI will have a very wide range of enforcement powers, influenced by 'responsive regulation' theory.[67] These include imposition of administrative penalties of 2% to 4% of the data fiduciaries' 'total worldwide turnover of the preceding financial year.'

The Bill provides broad coverage of the private and public sectors, with definitions of 'personal data' and 'sensitive data' similar to the GDPR. Data minimisation, a strong interpretation of consent, and demonstrable grounds for lawful processing, are very similar to the EU. Other obligations of data controllers ('data fiduciaries') cover many significant new elements of the GDPR, including demonstrable accountability, privacy by design and data breach notification. The rights of data subject ('data principals') include data portability and the 'right to be forgotten'. However, some of the more bureaucratic obligations will only apply to 'significant data fiduciaries', designated by the DPAI (and a few others): registration; data protection impact assessments (DPIAs); data protection officers (DPOs); record-keeping to demonstrate compliance; and annual audits. 'Small entities' with less than US$30,000 turnover per year, are also excused from some other obligations. The few significant GDPR elements not included in the Srikrishna Bill include the following: privacy by default; protections against automated processing; an explicit right to object to or block processing; and an explicit direct marketing opt out.

The Srikrishna Bill's data localisation and data export requirements create complex combinations of obligations because it distinguishes between three results:

- *Local copy requirement (localisation #1):* All personal data must be located on a server in India (s. 40(1)), with government

61 *Motshidiemang v Attorney General (Lesbians, Gays and Bisexuals of Botswana (LEGABIBO), Amicus Curiae) (2019) High Court of Botswana, 11 June 2019.*

62 *Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar judgment), Supreme Court of India, 26 September 2018 <https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf>, 1448 pages.*

63 *Aadhaar and Other Laws (Amendt.) Act, 2019; see 'Parliament passes Aadhaar amendment bill' Deccan Herald, 9 July 2019 <https://www.deccanherald.com/national/national-politics/parliament-passes-aadhaar-amendment-bill-745933.html>*

64 *Committee of Experts under the Chairmanship of Justice B.N. Srikrishna A Free and Fair Digital Economy Protecting Privacy, Empowering Indians, 2018 < http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf >*

65 *Personal Data Protection Bill 2018 <http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf>*

66 *For a longer comparison, see G. Greenleaf 'GDPR-Lite and Requiring Strengthening – Submission on the Draft Personal Data Protection Bill to the Ministry of Electronics and Information Technology (India)' (20 September, 2018). UNSW Law Research Paper No. 18-83 <https://ssrn.com/abstract=3252286 >.*

67 *The Srikrishna Report p. 151 cites G.Greenleaf Asian Data Privacy Laws (OUP, 2014) as their basis for stating that 'a responsive regulatory framework equipped with a range of tools has been found by us to be of critical importance' referring to Chapter 3, part 4 'Standards for enforcement mechanisms and 'responsive regulation'.*

exemptions allowed except for sensitive data. Localisation is already being required for some financial transactions.

- *Export prohibitions (localisation #2):* Categories of 'critical personal data' (CPD) specified by government cannot be exported, except to a destination held 'adequate' (SCCs or BCRs would not be sufficient), or for emergencies
- *Export permission requirements (localisation #3):* All non-CPD can be exported, but only if an export exception is satisfied, including adequacy of destination (as determined by the DPIA), or CSCs or BCRs where the exporter retains liability; or DPIA-designated emergency situations. If the conditions are not met, the data is unable to be exported, and in effect in category (ii).

India's data localisation is as complex as China's, but without the overriding requirement of 'security assessments' of data fiduciaries being carried out by State agencies. There is little doubt that some version of such a general data localisation policy will be enacted in India, as it is also consistent with India's draft Electronic Commerce Policy (February 2019).[68]

The Bill also has extraterritorial effects similar to the EU, applying to overseas companies targeting or profiling persons in India, and to Indian companies carrying out processing overseas. There is also a Government power to exempt specified processing of personal data of foreign nationals not present in India (an 'outsourcing exemption', like in the Philippines), which we might expect would be applied to the USA, but India would guarantee not to apply it to data originating from the EU.

Looking at the Srikrishna draft Bill overall, my conclusions are:[69]

1. The draft Bill sets out a serious and modern law, influenced heavily by the GDPR and including most of its elements. However, its tripartite distinction, in terms of the extent of obligations, between 'significant', normal, and 'small' data fiduciaries is the first to attempt to 'moderate' the GDPR in the this way. It could be an appealing model for other developing economies to take. However, it is potentially open to abuse, if the DPIA does not declare some data fiduciaries to be 'significant' when it is clear that they should. The effect of this on EU adequacy considerations remains to be seen.
2. The Report and Bill both reflect a very different regulatory philosophy from the EU GDPR's radical dispersal of decision-making responsibility (and liability for wrong decisions) to data controllers. The Indian model is more prescriptive, but a justifiable regulatory option, provided it does not give excessive discretion to the government or the Data Protection Authority.
3. The very broad exemptions from most of the Act for processing in the interests of State security or relating to law enforcement, although purportedly constrained by legality, necessity and proportionality (are dangerously vague). The DPAI also has discretion to expand the grounds of lawful processing.
4. The Bill's data localisation requirements adopt an unjustifiable generic approach to data localisation, through blanket local copy requirements (with exceptions to be specified by government), and export prohibitions also specified by government.

If the Srikrishna Bill is enacted in something close to its current form, Asia will have another new model for data privacy laws: strong GDPR influences; different obligations on different classes of data fiduciaries; and complex data localisation requirements.

PROGRESS IN OTHER ASIAN JURISDICTIONS

Bhutan's law is new. There have been only minor legislative changes in the other eight Asian jurisdictions with laws, but there have been some significant internal changes in operations.

North-east Asia – Little change in Taiwan and Macau

Taiwan continues not to have any specialised data protection authority, so the effectiveness or enforcement of its *Personal Information Protection Act* (PIPA) is difficult to gauge. Amendments in 2016 to Taiwan's Act added enhanced protection for special categories of sensitive data, but made compliance easier by relaxing the consent requirement for ordinary (non-sensitive personal data, and reduced the risk of criminal liability for violations of the PIPA. It has stated that it 'hopes

68 *For a summary see Sneha Johari 'India's Draft Ecommerce Policy is really a Digital Economy Policy, impacts the whole ecosystem' Medianama, 26 February 2019 <https://www.medianama.com/2019/02/223-india-draft-e-commerce-policy/>.*

69 *G. Greenleaf 'GDPR-Lite and Requiring Strengthening' cited above.*

to participate' in APEC CBPRs.[70] In the absence of a DPA, Taiwan's National Development Council (NDC) has opened a data protection coordination office, and has submitted a self-evaluation report on Taiwan's data protection to the EU, in order to commence adequacy discussions.[71]

Macau's Office for Personal Data Protection (GPDP) still has not been formally established by its own legislation, but continues to operate as a 'project' under the Chief Executive's Office, twelve years after the PDPA was enacted. It continues to have one of Asia's most transparent enforcement practices (like Singapore, but no longer Hong Kong), publishing around 20 complaint resolutions notes per annum[72] (in English translations, even though English is not an official language in Macau), as well as the occasional authorisation of data exports.[73]

Hong Kong SAR – Deficits in powers, but transparency continues

In 2014 Hong Kong's data privacy regime could be considered one of the most effective in Asia, possibly 'Asia's leader in data privacy', despite a relatively weak Act, because of a vigorous enforcement regime.[74] Since then, under a new Commissioner (PCPD), the vigour of enforcement seemed initially to have diminished, but since 2017 has again become transparent from the PCPD website.[75] This includes the resumption of casenotes (complaint summary), of up to 15 per annum; Administrative Appeal Board case summaries; and summaries of the few court decisions on the Ordinance, plus some examples of minor prosecutions of breaches included under 'News'. The PCPD has also resumed publishing investigation report under s. 48(2), previously a favoured means of enforcement which enabled 'name and shame' as an enforcement technique. There have now been five such reports against public and private sector bodies since 2015, which although modest compared with 31 such reports from 2010-14, indicates that PCPD enforcement continues.

In June 2019 PCPD issued a s48(2) report in relation to the data breach by Cathay Pacific affecting 9.4 million people,[76] and which has potential implications for EU extra-territorial jurisdiction. However, the PCPD could only order that the airline take measure to prevent and remediate the manifest security breaches that had occurred, because it has no powers to issue administrative fines. This demonstrates that the Hong Kong legislation is inadequate to deal with the scale of breaches that now occur, particularly in light of the UK ICO's proposed fine of £183 million against British Airways for a data breach of similar scale. While the local visibility and transparency of the PCPD continues, its enforcement powers are now unjustifiably outdated and insufficient. Hong Kong no longer leads in Asian data protection.

South-east Asia (ASEAN) – The Philippines (energetic) and Malaysia (inactive)

The Philippines Data Privacy Act (DP Act), enacted in 2012, included more than the minimum '1st generation' principles, such as deletion rights, protection of sensitive information, data portability (in advance of the GDPR, and data breach notification, but no data export restrictions. Its enforcement regime appeared to have a broad and serious 'toolkit'. Much was uncertain because of vague and ambiguous drafting.[77] This otherwise potentially strong Act was also marred by an exemption from the Act of any personal data collected legally in foreign jurisdictions but 'being processed in the Philippines' – in other words, an exemption for any outsourced processing – which is likely to make any EU finding of adequacy impossible to obtain.[78]

Although theoretically coming into force in 2012, the Act remained dormant until 2016, because until a National Privacy Commission (NPC) was appointed, and made Implementing Rules and Regulations (IRR), very few of its provisions were enforceable, and none were enforced. Outgoing President Aquino appointed the three NPC Commissioners shortly before

70 *Taiwan Executive Yuan Taiwan's achievements during 2016 APEC Economic Leaders' Week', 8 December 2016 <http://english.ey.gov.tw/News_Hot_Topic.aspx?n=9CAC6D643D2B87F8&sms=C7706D6F9D246174>.*

71 *'EU lauds Taiwan's efforts to push for talks on data transfer deal' Taiwan News, 11 March 2019 < https://www.taiwannews.com.tw/en/news/3655633> .*

72 *OPDP (Macau) 'Complaint Case Notes' <http://www.gpdp.gov.mo/index.php?m=content&c=index&a=lists&catid=209> .*

73 *OPDP (Macau) 'Authorisations' <http://www.gpdp.gov.mo/index.php?m=content&c=index&a=lists&catid=206> .*

74 *Greenleaf, Asian Data Privacy Laws (2014), pp. 120-1 and preceding chapter.*

75 *See 'Compliance and enforcement' on PDPC (HK) website <https://www.pcpd.org.hk/>.*

76 *PCPD Media Statement (HK) 'Cathay Data Breach Incident-Personal Data Security & Retention Principles Contravened-Lax Data Governance' 6 June 2019 <https://www.pcpd.org.hk/english/news_events/media_statements/press_20190606.html>.*

77 *Greenleaf, Asian Data Privacy Laws (2014), pp. 352-3.*

78 *Greenleaf, Asian Data Privacy Laws (2014), p. 348.*

leaving office.[79] The NPC rapidly issued finalized IRRs so that the Act became effective.[80] The NPC has taken a very activist approach to publicising the Act and to some aspects of enforcement. It recommended the criminal prosecution under the Act of the head of the Philippines' Electoral Commission, for negligently allowing a massive data breach, as well as restorative measures by the agency.[81] The NPC has not yet published results of other investigations in any routine way (unlike Singapore or Macau), but in 2018 released all its Advisory Opinions, many of which are based on quite specific enquiries to the NPC.[82] With about 70 opinions in 2017, this is a very substantial body of authoritative interpretation of the DP Act, unless and until contradicted by court decisions. It is a novel form of transparency.

Malaysia's *Personal Data Protection Act 2010* (PDPA) is limited to the private sector, with a non-independent Commissioner, and has few principles beyond the minimum.[83] After five years, Malaysia's Department of Personal Data Protection has shown few visible signs of enforcing the PDPA, despite that Act being in force for six years. One reason is that, in effect, the Malaysian PDPA can only be enforced through prosecutions, and those must be with the consent of the Public Prosecutor. There is nothing on the PDPC website to indicate that the Commissioner has yet taken any steps to enforce the Act, such as reports of investigated complaints.[84] Three cases have been reported where 'processing personal data without certification of registration' (essentially, failure to pay registration fees) has resulted in small fines.[85] A new Regulation allows the Commissioner to offer to compound specified offences – in effect to allow a fine to be paid instead of prosecution. In 2017 a previous Commissioner proposed a 'White List' of countries with supposedly 'adequate' laws for data export purposes, but which included the USA and China without any justification. This has not been formally adopted as yet, and may have been abandoned. Following the electorate's decisive dismissal of Malaysia's scandal-plagued government in May 2018, the new Minister claims that the PDPA is being reviewed, including in light of the GDPR which he implied required 'comprehensive changes to business practices'.[86] It is reported that this will involve a data breach notification regime,[87] but no other details are available, and there is no time-frame.

Vietnam – Lighter data localisation

Vietnam's data privacy laws, which are scattered across various regulations and sectors, were 2014 'a reasonable approximation of the basic principles set out in the 1980 OECD Guidelines or the ... APEC Privacy Framework'. However, they lacked any of the elements found in the EU 1995 Directive, or the GDPR, except perhaps some ability to prevent continuing processing.[88] The most recent post-2014 addition, the Law on Cyber-Information Security (CISL), a highest-level law enacted by the National Assembly, significantly expands Vietnam's existing data privacy laws, in that it sets out what is probably the most comprehensive set of data privacy principles yet found in a Vietnamese law. Its scope is limited to commercial processing and only in cyberspace,[89] although it defines 'cyberspace' so as to suggests that the scope also includes VPNs and possibly certain intranets. Like China, Vietnam has no overall Data Protection Authority, but relies on Ministry-based enforcement, details of which are not readily available.

A 2013 law required some businesses to have a server located in Vietnam, if state authorities so requested, a limited sectoral data localisation requirement. Vietnam currently has no explicit legislation on data export restrictions, but consent or government approval is required for overseas

79 *G. Greenleaf, Philippines Appoints Privacy Commission in Time for Mass Electoral Data Hack (2016) 141 Privacy Laws & Business International Report, 22-23 <https://ssrn.com/abstract=2824419>*

80 *G. Greenleaf, Philippines Puts Key Privacy Rules in Place but NPC Faces Pressure (2016) 143 Privacy Laws & Business International Report, 19-21 <https://ssrn.com/abstract=2895600>*

81 *See the Philippines section in G. Greenleaf '2014-2017 Update to Graham Greenleaf's Asian Data Privacy Laws - Trade and Human Rights Perspectives' (July 12, 2017). UNSW Law Research Paper No. 17-47 <https://ssrn.com/abstract=3000766>.*

82 *NPC Advisory Opinions (Philippines) <https://privacy.gov.ph/advisory-opinions/>*

83 *Greenleaf, 2014, pp. 322-355.*

84 *PDPC (Malaysia) <http://www.pdp.gov.my/index.php/en/mengenai-kami/maklumat-organisasi/pejabat-pesuruhjaya>*

85 *Kherk Ying Chew 'Malaysia: Enforcement of the Personal Data Protection Act 2010' Baker & McKenzie, 1 November, 2017 <https://globalcompliancenews.com/malaysia-enforcement-personal-data-protection-20171101/>*

86 *Bernama 'Personal Data Protection Act under review – Gobind' MalaysiaKini 18 March 2019 <https://www.malaysiakini.com/news/468441>*

87 *Yuet Ming Tham 'Important Changes to the Malaysia Data Privacy Regime' Sidley 9 April 2019 <https://www.sidley.com/en/insights/newsupdates/2019/04/important-changes-to-the-malaysia-data-privacy-regime>*

88 *Greenleaf, 2014, pp. 368-372.*

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

transfers.[90] Vietnam enacted a controversial *Law on Cyber Security* in June 2018 introducing data localisation requirements, but also imposing severe penalties on the publication of anything considered to be anti-State activities. It 'imposes tremendous obligations on both onshore and, especially, offshore companies providing online services to customers in Vietnam'.[91] However, the data localization requirements are less strict than in previous drafts: 'The adopted version of the law seems to relax these restrictions by requiring the online service providers to store the Vietnamese users' information within Vietnam for a certain period of time. However, during the statutory retention time, the law does not appear to expressly prohibit the online service providers from duplicating the data and transferring/storing such duplicated data outside of Vietnam.'[92] 'Another requirement found in previous drafts', the same authors note, 'that offshore service providers must locate servers in Vietnam, has been removed from the final version. However, by requiring offshore service providers to "store" Vietnamese users' information in Vietnam, the offshore service providers, as a practical matter, will likely need to locate servers in Vietnam, either by directly owning/operating the servers or leasing servers owned/operated by other service providers in Vietnam, to store such information'.

Singapore – Enforcement and resistance

In 2014, before Singapore's *Personal Data Protection Act* (PDPA) had come into full operation, it presented as an Act with 'an exceptionally limited scope, perhaps the narrowest of any Asian law', but one which 'does appear to have a serious and multi-faceted enforcement pyramid', so that businesses would be wise to take its limited requirements seriously.[93] The last five years have borne out these assessments, as documented elsewhere by me[94] and in relation to enforcement in a 2018 report by Chia to the Asian Business Law Institute.[95] Only the distinctive aspects of Singapore's law in operation, and proposed reforms to it, are discussed here.

The Personal Data Protection Commission (PDPC) has proven to be a serious regulator, even though legislative changes have clarified that it does not have independence from government.[96] It reports details of its decisions regularly,[97] 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. PDPC may issue administrative fines up to S$1 million. In practice, fines in the S$10K-S$30K range are common, and S$50K not unusual. Other than Korea, no other Asian law results in fines of this magnitude, this often, low though they now are by European standards. In January 2019 the PDPC fined Singapore Health Services (SingHealth) S$250,000, and Integrated Health Information Systems (IHIS), S$750,000 (US $550,000), its largest fines to date, for what the PDPC called the 'worst breach of personal data in Singapore's history,' resulting in the disclosure of personal data for 1.5 million patients and the outpatient prescription records of approximately 160,000 patients.[98]

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. In February 2019, the Minister announced that Singapore is considering, as part of an ongoing review of the Personal Data Protection Act (PDPA), introducing data portability.[99] These are the only proposals to strengthen the relatively weak principles in Singapore's law in the direction of the GDPR. Other proposed reforms are likely to weaken

90 *Waewpen Piemwichai Jurisdictional Report – Vietnam in C. Girot (Ed.) Regulation of Cross-Border Transfers of Personal Data in Asia, (ABLI, February 2018) , paras. 18-45 <http://abli.asia/PUBLICATIONS/Data-Privacy-Project>.*

91 *W. Piemwichai and Tu Ngoc Trinh 'Vietnam's New Cybersecurity Law Will Have Major Impact on Online Service Providers', Tilleke & Gibbons, June 18 2018 <https://www.tilleke.com/index.php?q=resources/vietnam%E2%80%99s-new-cybersecurity-law-will-have-major-impact-online-service-providers>*

92 *Piemwichai and Trinh, ibid.*

93 *Greenleaf, Asian Data Privacy Laws, pp. 314-5.*

94 *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).*

95 *Ken Chia 'Jurisdiction Report – Singapore' in C. Girot (Ed.) Regulation of Cross-Border Transfers of Personal Data in Asia, February 2018 <http://abli.asia/PUBLICATIONS/Data-Privacy-Project>*

96 *For details see Greenleaf 'The Asian context of Singapore's Law' 2018, paras. 8.64-65.*

97 *PIPC decisions <https://www.pdpc.gov.sg/Commissions-Decisions/Data-Protection-Enforcement-Cases>,*

98 *In the matter of an investigation under section 50(1) of the Personal Data Protection Act 2012 and Singapore Health Services Pte. Ltd and Integrated Health Information Systems Pte. Ltd [2019] SGPDPC 3*

99 *K. Kwang 'Singapore plans data portability requirement as part of PDPA update' Channel News Asia, 25 February 2019 <https://www.channelnewsasia.com/news/singapore/singapore-personal-data-protection-act-portability-rights-move-11287772>*

Singapore's law, from a consumer perspective: Guidelines concerning 'anonymisation' or de-identification of personal data appear to leave more scope for use of personal data than European standards; PDPC suggestions of a 'regulatory sandbox' are probably aimed at allowing 'big data' experiments based on these Guidelines, or further weakening of them; and PDPC is proposing to weaken the significance of consent even further.

Singapore is attempting to develop a multi-faceted approach to the problems of cross-border data traffic.[100] PDPC has developed its own recommended (not mandatory) Standard Contract Clauses (SCCs) for transfers. Singapore stated its intention to participate in the APEC APEC-CBPRs in July 2017, but has not yet appointed an 'Accountability Agent' (AA), so cannot do so yet. Possible policy directions include mutual recognition (within ASEAN and beyond) of both CBPRs certifications (once Singapore is fully involved), and Trustmarks. PDPC and its controlling Department (IMDA) called for Singapore-based organisations to participate in Singapore's Data Protection Trustmark (DPTM) certification, which requires an 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,[101] The Minister states that Singapore will align its own proposed Trustmark standards with APEC-CBPRs standards. 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.

The result of all these developments is that Singapore, along with Japan (despite its 'adequate' status) lead the group of Asian countries that wish to have little to do with strengthening their laws in the directions suggested by the example of the EU, or the arguments put forward by proponents of human rights. On the other hand, they do not support the 'data sovereignty' approaches of counties favouring data localisation (sometimes influenced by China). For these countries, a limited amount of data protection is a requirement for trust in online business, including cross-border transfers, but that is all. I will call them 'the resisters'.

South Asia (SAARC) – Bills pending

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. Nepal has a public sector law,[102] and Bhutan a comprehensive but otherwise limited new 2018 law (discussed below). There are some minor but no major developments in the other jurisdictions,[103] except a draft private sector *Personal Data Protection Bill 2018* in Pakistan and a Ministry proposal for a comprehensive, GDPR-influenced, Personal Data Protection Bill in Sri Lanka. If enacted, these two Bills would be major developments.

Bhutan – Data privacy as gross national happiness

The land-locked kingdom of Bhutan is known internationally for favouring a measure of 'Gross National Happiness' rather than GDP. It can now add to its GNH the *Information, Communications and Media Act of Bhutan 2018*,[104] passed by the National Assembly in 2017, and in force from mid-2018. Although the data protection principles in the Act are stated briefly, they do more than give Bhutan a minimal data privacy law, because they include seven of the ten 'second generation' principles (see the Table in the Conclusion). Although only applying to provision of the 'ICT and Media Sectors', and providers and users of their service. 'ICT services' are given a very broad meaning, and will normally include public facilities (and thus the public sector), so the law will cover almost any use of electronic information. The act establishes a Bhutan Infocomm and Media Authority which is not fully independent, but has powers to investigate and resolve complaints. There are provisions for compensation, and for offences.

100 *See generally Chia 'Jurisdiction Report – Singapore' paras 1, 21-23 and 83-93,*

101 *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.*

102 *Greenleaf, Asian Data Privacy Laws, pp. 436-446.*

103 *G. Greenleaf 'Privacy in South Asian (SAARC) States: Reasons for Optimism' (2017) 149 Privacy Laws & Business International Report 18-20 <https://ssrn.com/abstract=3113158>.*

104 *Information, Communications and Media Act of Bhutan, 2018 <https://www.dit.gov.bt/information-communications-and-media-act-bhutan-2018>.*

INTERNATIONAL STANDARDS, DATA EXPORTS AND LOCALISATION

Agreed standards for data privacy laws, whether within a geographical region such as Asia, or at an international level, can have two main effects on international data flows. Adherence to them by legislation can result in increased convergence of standards, making countries more willing to allow personal data concerning their citizens to be exported to countries with similar standards. If common standards for such personal data exports can be agreed upon between countries, then businesses within and without those countries have a reduced compliance burden.

The context of the problem has continued to change, and undue focus on the difficulties of transfers from the EU (and their solutions) is unhelpful. This is because almost all data privacy laws have data export restrictions (of many different kinds), and every new or revised law multiplies the complexity of every other country's problems of obtaining data imports.

This part of the paper examines the extent to which the international mechanism discussed in 2014 have (and have not) developed over the past five years. It will help explain why it is unlikely for the near future that Asia will develop a significant degree of convergence or data export consistency. The Singapore-based Asian Business Law Institute (ABLI)[105] has a multi-year project to explore possible mechanism to reduce problems of personal data transfers between countries within Asia, and also outside Asia. The project has already generated exceptionally valuable research on the position in each country,[106] but it is unsurprising that solutions have not yet emerged.

Asia's lack of regional standards

There is still no Asia-wide enforceable regional data privacy agreement, nor any such agreement at the sub-regional level. The only sub-regional agreement is the 2016 *ASEAN Framework on Personal Data Protection*[107] which is a non-binding 'record of Participants' intentions' with no practical effects and no obligations concerning implementation. It refers to the APEC Privacy Framework, and includes principles similar to those APEC principles, but with the addition of a principle concerning cessation of retention of personal data.

The closest Asia comes to regional standards are the supra-regional standards resulting from some Asian jurisdictions (but not India and the rest of South Asia) being part of APEC and its Cross-border Privacy Rules system (CBPRs, see below), and the APEC-related free trade agreement, the Comprehensive and Progress Trans-Pacific Partnership (CPTPP, see below).

Africa and Latin America are both more advanced than Asia in the development of regional data privacy standards. In Africa the ECOWAS Supplementary Act of 2013 on data privacy,[108] with a relatively high level of protections approaching those of the 1995 EU data protection Directive, is now in force between 15 west African states, ten of which have enacted data privacy laws. The African Union 'Malabo Convention' of 2014, dealing with both cybercrime and data protection, and with standards similar to ECOWAS, is not yet in force. It has five of the required 15 ratifications, and a further 11 signatories from the 54 AU member states. The network of Latin American data protection authorities (abbreviated as RIPD or RedIP) finalized in 2017 the *Standards for Personal Data Protection for Ibero-American States,*[109] at the request of the XXVth *Ibero-American Summit of Heads of State and Government* in 2016. This 'RIPD Standard' has a strong consistency with the EU's GDPR and with Convention 108+. It is a standard, not a binding commitment to legislate, but there is at present activity within the Organisation of American States (OAS), which includes all 35 independent states in the Americas, toward developing such a binding agreement.

The G20's 'Osaka Track', the WTO and BRICS dissent

Since he introduced the term at the January 2019 Davos World Economic Forum, Japanese Prime Minister Abe has hoped to make the concept of 'Data Free Flow with Trust' (DFFT) one of the centerpieces of Japan's hosting of the 2019 G20 Leader's Summit in Osaka. The June summit produced two declarations which may have a long-

105 *Asian Business Law Institute (ABLI) 'Convergence of the rules and standards for cross-border data transfers in Asia' Project < https://abli.asia/PROJECTS/Data-Privacy-Project> .*

106 *C. Girot (Ed.) Regulation of Cross-Border Transfers of Personal Data in Asia (ABLI, 2018), <https://abli.asia/PUBLICATIONS/Regulation_of_Cross-border_Transfers_of_Personal_Data_in_Asia>.*

107 *Telecommunications and IT Ministers of the ASEAN member states 'ASEAN Framework on Personal Data Protection' <http://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf> November 2016.*

108 *Supplementary Act on Personal Data Protection within ECOWAS <http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf >.*

109 *RIPD Standard 2017 <http://www.redipd.es/documentacion/common/Estandares_eng_Con_logo_RIPD.pdf>.*

term effect on global data privacy rules, but their significance is far from certain due to their vague terms, and to the number of significant countries that are as yet staying outside of the processes that have been established.

The *G20 Osaka Leaders' Declaration,*[110] endorsed by all G20 leaders, includes a section 'Innovation: Digitalization, Data Free Flow with Trust' (arts.10-12, 3 of 43), is very bland, but refers to the challenges of data privacy in the context of IP rights and cybersecurity:

> *Cross-border flow of data, information, ideas and knowledge generates higher productivity, greater innovation, and improved sustainable development, while raising challenges related to privacy, data protection, intellectual property rights, and security. By continuing to address these challenges, we can further facilitate data free flow and strengthen consumer and business trust. In this respect, it is necessary that legal frameworks, both domestic and international, should be respected.*

The *Osaka Declaration on Digital Economy*[111] was made by 24 countries, including the US, China, Russian, the EU, Latin American and east Asian countries.[112] However four potentially significant countries did not participate: India, Egypt, Indonesia and South Africa. The Osaka Declaration was downgraded to a secondary event in order to avoid singling out the four countries that had yet not signed on.[113] The signatories declared the launch of the 'Osaka Track', described as 'a process which demonstrates our commitment to promote international policy discussions, *inter alia*, international rule-making on trade-related aspects of electronic commerce at the WTO'. They confirmed their 'commitment to seek to achieve a high standard agreement with the participation of as many WTO Members as possible', noting that 78 WTO Members are 'on board' with the Joint Statement on Electronic Commerce issued in Davos on 25 January 2019. They resolved to aim for substantial progress in the negotiations by the 12th WTO Ministerial Conference in June 2020. Abe has announced Japan will organize a meeting of 'Osaka Track' participants, possible as early as July 2019.[114]

India is refusing to support this Davos e-commerce initiative, its Commerce and Industry Minister, Piyush Goyal, arguing in Osaka that 'developing countries need time and policy space to build deepest understanding of the subject and formulate their won legal and regulatory framework before meaningfully engaging in e-commerce negotiations'.[115] Goyal reiterated India's policy favouring data localisation, reflecting the Modi government's policy that data is a national asset, not primarily an individual right, as set out in its draft e-commerce policy (as discussed above in relation to India).

'Data Free Flow with Trust' may be a new label, but it is not a new concept when applied to data privacy, even if it is new in relation to IP or cybersecurity. The idea that free flow of personal data could only be guaranteed by trust between countries has been around since at least 1980. It appeared in the original OECD privacy Guidelines and Council of Europe data protection Convention as trust induced by adherence to minimum standards of data protection. Agreement on what constitutes the 'minimum standards' has been the problem. It is not clear why shifting discussions back to a WTO forum will have any effect in relation to data privacy, although it might in relation to IP and cybersecurity.

The new element is the number of countries introducing data localization policies and laws (in varying forms), which can affect all three areas of concern because they are not necessarily limited to personal data. India and Indonesia's general data privacy laws are still in draft, but they already have some data localization laws. So do China, Vietnam and Russia, but they signed the Osaka Track statement, indicating that participation does not signal any particular view about data localization. The Joint Statement[116] by the leaders of the BRICS countries (both those that did not sign on to the Osaka Track), stressed the centrality of the WTO to a rules-based multilateral trading system, in contrast to the current view of the USA, but

110 *G20 Osaka Leaders' Declaration, June 2019 <https://g20.org/pdf/documents/en/FINAL_G20_Osaka_Leaders_Declaration.pdf>*

111 *Osaka Declaration on Digital Economy <https://www.meti.go.jp/press/2019/06/20190628001/20190628001_01.pdf >.*

112 *Argentina, Australia, Brazil, Canada, China, the European Union, France, Germany, Italy, Japan, Mexico, Republic of Korea, Russian Federation, Saudi Arabia, Turkey, United Kingdom, United States, Spain, Chile, Netherlands, Senegal, Singapore, Thailand, and Viet Nam.*

113 *Satoshi Sugiyama 'Abe heralds launch of 'Osaka Track' framework for free cross-border data flow at G20' The Japan Times, 28 June 2019, <https://www.japantimes.co.jp/news/2019/06/28/national/abe-heralds-launch-osaka-track-framework-free-cross-border-data-flow-g20/> .*

114 *'G20 leaders' joint declaration again omits 'protectionism' The Japan News, 30 June 2019 <http://the-japan-news.com/news/article/0005843262.*

115 *Aditi Agrawal 'Piyush Goyal at G20: Data is a sovereign asset, free trade can't justify its free flow' Medianama, 11 June 2019.*

116 *Joint Statement on BRICS Leaders' Informal Meeting on the margins of G20 Summit, 28 June 2019 <http://pib.nic.in/PressReleseDetail.aspx?PRID=1576270>; Signed by the leaders of Brazil, Russia, India, China and South Africa.*

otherwise there was no explicit 'BRICS solidarity' evident. Indian trade Minister Piyush Goyal said that data was a 'new form of wealth', important for development, and there was a need to take into account the requirements of developing countries within WTO discussions rather than outside them.[117] There are no longer any simple division on these issues, but rather a global fragmentation of views.

The CPTPP limits localisation and export restrictions

In 2017-18 the previous Trans Pacific Partnership (TPP) was scrapped after President Trump refused US ratification, but it was then replaced by the 11 other parties proceeding with the *Comprehensive and Progressive Trans-Pacific Partnership* (CPTPP), which was largely the same in its provisions which impose significant limitations on the ability of parties to enact data export restrictions or data localisation requirements, beyond those found in the WTO's General Agreement on Trade in Services (GATS), art. XIV. Japan, Malaysia, Singapore and Vietnam are the Asian jurisdictions which are signatories to the CPTPP. Korea, Indonesia, the Philippines and Thailand are not signatories to the CPTPP, although they are entitled to accede to it because they are APEC members. So is China, but very unlikely to sign.

CPTPP came into force between its six initial ratifying parties, including Japan and Singapore, on 30 December 2018.[118] Vietnam was to commence on 14 January 2019. The US-Mexico-Canada FTA has similar provisions but is not yet in force. The data localisation and data export provisions in these free trade agreements (FTAs) may be inconsistent with provisions in the laws of some of these countries (including provisions necessary for EU adequacy), and also with their other international obligations such as in Convention 108.[119] As parties to CPTPP, it is arguable that Japan, New Zealand and Canada may already have made commitments inconsistent with being considered adequate by the EU; and Mexico may have done similarly in relation to its commitments under Convention 108.

Will these potential inconsistencies lead to litigation or diplomatic enforcement activities? In a different context, in February 2018, the threats to privacy legislation posed by FTAs became more real, when the US reiterated complaints against Chinese legislation restricting personal data exports, under the WTO's General Agreement on Trade in Services, (GATS, 1995). The US has not yet attempted to join the CPTPP (after abandoning the TPP), but it might do so, in which case the likelihood of enforcement actions would increase.[120]

Another Asia-Pacific FTA is now under negotiation, under strict secrecy, the *Regional Comprehensive Economic Partnership* (RCEP).[121] It is not yet known what privacy-related clauses this agreement might contain. Australia, China, Japan, Korea, New Zealand, India, Singapore, Thailand, Malaysia, Indonesia, Vietnam and other ASEAN countries are involved in the negotiations, so it is potentially very important because neither China nor India are involved in CPTPP.

APEC-CBPRs' continuing failure

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.[122] This endorsement does not carry any legal obligations with it – it is not a treaty. However, the Framework is the foundational standard on which the APEC CBPRs is based, standards well below those of the GDPR (or the Directive).

In 2017-18 Singapore, Australia and Taiwan ('Chinese Taipei' in APEC-speak) were approved to participate in the Asia-Pacific Economic Cooperation's Cross-Border Privacy Rules System (CBPRs). APEC's Electronic Commerce Steering Group Joint Oversight Panel (ECSG-JOP) held that their laws met APEC requirements. Mexico (2014), Canada (2014), and Korea (2016) obtained approval earlier. If and when any of these six countries appoint 'Accountability Agents' (AAs), then companies in their jurisdictions can apply to be certified as CBPRs-compliant. Until then,

117 *'G20 summit: India does not sign Osaka declaration on cross-border data flow' < https://scroll.in/latest/928811/g20-summit-india-does-not-sign-osaka-declaration-on-cross-border-data-flow>*

118 *Australia, Canada, Japan, Mexico, New Zealand and Singapore (with Vietnam to commence on 14 January 2019) – See DFAT Australia CPTPP site <https://dfat.gov.au/trade/agreements/in-force/cptpp/Pages/comprehensive-and-progressive-agreement-for-trans-pacific-partnership.aspx>.*

119 *G. Greenleaf 'Asia-Pacific free trade deals clash with GDPR and Convention 108' (2018) 156 Privacy Laws & Business International Report, 32-34.*

120 *ibid*

121 *Australia Department of Foreign Affairs and Trade Regional Comprehensive Economic Partnership – About the RCEP Negotiations <https://dfat.gov.au/trade/agreements/negotiations/rcep/Pages/regional-comprehensive-economic-partnership.aspx>.*

122 *Greenleaf, Asian Data Privacy Laws, 2014, pp. 33-37.*

'participation' in APEC CBPRs has no practical effect. None of these countries has yet appointed an AA. Canada called for applicants to be AAs in 2017.[123] It seems that some countries say they wish to participate in APEC CBPRs, and take preparatory steps, but then do not do so.

As at mid-2019, only the US (26 companies certified since 2013[124]) and Japan (3 companies certified since 2016[125]) have appointed AAs,[126] so after six years of operation, APEC CBPRs only involves a tiny number of US and Japanese companies. CBPRs is therefore of negligible practical significance as yet. The European Commission states in its Decision concerning Japan's adequacy assessment that certification of a company as APEC CBPRs compliant cannot be the basis for any onward transfer of EU-origin personal data from a country that is held to be GDPR-adequate.[127] This will further diminish the business case for CBPRs. On the other hand, APEC CBPRs has been recognised in the proposed USMCA tripartite free trade agreement (not yet finalised).

APEC economy	Approved to join APEC-CBPRs	Accountability Agent appointed	No. of Companies certified
USA	**2012**	**2013**	**26**
Japan	**2014**	**2015**	**3**
Canada	2014	-	0
Mexico	2014	-	0
Korea	2016	-	0
Singapore	2017	-	0
Taiwan	2018	-	0
Australia	2018	-	0
Other 11 in APEC	-	-	0

123 *See Gazette <http://www.gazette.gc.ca/rp-pr/p1/2017/2017-01-21/pdf/g1-15103.pdf > at p. 242.*

124 *TrustAct APEC CBPR Certified Companies < https://www.trustarc.com/consumer-resources/trusted-directory/#apec-list> as at 15 July 2019.*

125 *See JIPDEC's APEC CBPRs Certified Companies list <https://english.jipdec.or.jp/protection_org/cbpr/list.html> (as at 15 July 2019).*

126 *APEC CBPRs Accountability Agents listing < http://cbprs.org/accountability-agents/> .*

127 *[European Union] Commission Implementing Decision of 23.1.2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information < https://ec.europa.eu/info/sites/info/files/draft_adequacy_decision.pdf >*

Little Asian progress for Convention 108+

The 'modernisation' of data protection Convention 108 was completed, by the parties to the existing Convention agreeing to a Protocol amending it, on 18 May 2018. The new version (called '108+' to distinguish it) will not come into force for some years.[128] The standards required by 108+ of the laws of acceding countries are higher than those of Convention 108, arguably mid-way between 108 and the GDPR.[129] Since it became open for signature on 10 October 2018, any new countries wishing to accede will have to accede to both the Protocol (ie to 108+) as well as to Convention 108. The UN Special Rapporteur on the Right to Privacy (SRP) has recommended that all UN member states should accede to Convention 108+ and implement its provisions in their domestic law, and where possible to implement additional GDPR principles, while leaving the door open to a broader international agreement at a later date.[130] The EU also endorses accession to Convention 108 by countries seeking a positive adequacy assessment (GDPR, recital 105). Parties to 108+ commit to allowing free flow of personal data to other parties, in return for the same benefit,[131] obligations enforceable only by diplomatic means.

Convention 108 has had reasonable success since its 'globalisation' started with the completion of Uruguay's accession in 2013. It now has 55 Parties, with three from Latin America (Uruguay, Mexico and Argentina), and five from Africa (Tunisia, Cape Verde, Senegal, Mauritius and Morocco). Burkina Faso remains eligible to accede to 108.

However, Convention 108 has had a lack of success in Asia with no accessions as yet, although Japan, Korea, the Philippines and Indonesia are accredited as Observers. The task of attracting accessions to Convention 108+ may be more difficult because of the higher standards that acceding countries must meet. Of the 15 countries in Asia with data privacy laws many will not be able to meet the basic Convention 108+ requirements that a Party must be a State that can claim to be democratic,

128 *For details see G. Greenleaf (2018) 'Modernised' data protection Convention 108+ and the GDPR' 154 Privacy Laws & Business International Report 22-3 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3279984>.*

129 *G. Greenleaf 'Renewing Convention 108: The CoE's 'GDPR Lite' Initiatives' (2016) 142 Privacy Laws & Business International Report,14-17 <https://ssrn.com/abstract=2892947>.*

130 *United Nations General Assembly, seventy-third session Report of the Special Rapporteur on the right to privacy, 17 October 2018, para. 117(e) <http://www.worldlii.org/int/other/UNSRPPub/2018/11.html>.*

131 *There is an exception allowing higher regional standards to also be required, such as adequacy under the EU GDPR.*

with a data privacy law that covers both its public and private sectors, and includes an independent DPA. These various criteria rule out nine of the 15: China, Vietnam, Taiwan, Hong Kong, Macau, Singapore, Malaysia, Nepal and Bhutan. Indonesia and India would be ineligible on their current limited laws, but may not be if their new Bills are enacted, subject only to the question of whether these laws would meet the higher standards of 108+. That leaves only Thailand, Japan, Korea and the Philippines as possible 108+ accessions as at mid-2019. The junta-appointed upper house in Thailand raises issues in relation to democracy. The Duterte government's Trumpish antipathy to international institutions like the International Criminal Court make a Philippines accession request unlikely in the short term, although its DPA says it is looking into the possibility.[132] Japan no longer needs 108+ to assist its EU adequacy case, and is preoccupied with its 'Osaka Track', the consistency of which with 108+ is too early to assess. The legislation currently before the Korean legislature would improve its position in relation to 108+ as well as EU adequacy, and the Korean government may be positively disposed toward accession, but has not made any announcement to this effect.

In summary, Asia seems at present unlikely to be a major source of the continuing globalization of Convention 108+, less so than Africa or Latin America. However, new laws and policies, including in any of India, Indonesia, Korea, Japan or the Philippines, could change this momentum.

Will the EU's 'adequate' list expand in Asia?

The GDPR coming fully into force on 25 May 2018 created a more concrete 'international standard': those countries which wish to obtain or retain a finding by the European Commission that they 'ensure an adequate level of protection' must satisfy the requirements of art. 45. Which Asian countries, other than Japan and Korea, could do so? The Japanese adequacy decision has shown how low (or 'reasonable') a benchmark the GDPR adequacy standard can be, not much different from the Directive except that there must now be credible protection of private sector data against public sector accesses.

Although otherwise credible in relation to its private sector (at least by the 'Japan standard'), Singapore is disqualified by the lack of independence of its DPA. Malaysia likewise. Taiwan has no DPA, and would not realistically be able to obtain a positive adequacy assessment until it does. Perhaps, on the Japanese standard, the Philippines could apply, but it would not be so important to the EU that the answer is 'yes', and (at best) any data imported into the Philippines from the EU for the purposes of further processing would have to be excluded from the scope of such a determination, because the Philippines data privacy law does not apply to such data. Thailand has expressed interest in applying for an adequacy determination, but the extent of independence of its DPA would need to be examined. It seems unlikely that Chinese politics would allow Hong Kong or Macau to apply, and in any event Hong Kong does not have any data export restrictions. Whether India or Indonesia might become credible applicants is unknown. Although the position is no doubt more complex than these brief observations suggest, and is always subject to amendments arising from negotiations (as was the case with Japan), it is nevertheless apparent that there are no easy roads to positive adequacy determinations yet to be found in Asia.

Other 'appropriate safeguards' for transfers from the EU (and elsewhere)

As the European Commission insists quite often, art. 45 adequacy decisions are not the only basis for approved transfers of personal data between the EU and other countries. Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), approved codes and approved certification mechanisms, providing 'appropriate safeguards' under art. 46 can support large-scale transfers. However, uncertainty will surround the effectiveness of SCCs (and other mechanisms) at least until the CJEU delivers its decision in the 'Schrems #2' case, only now being heard, challenging the validity of the use of SCCs for data transfers to the USA, because of the extent of US government access to such data.

Whatever the position in the EU, these same mechanisms, if adopted in Asian data privacy laws, may provide parts of the answers for cross-border transfers within and outside Asia. Singapore has a particular interest in developing such mechanisms.

132 *L. Hunt 'Does Duterte's War on the International Criminal Court Really Matter?' The Diplomat 5 April 2018.*

CONCLUSIONS: NO GRAND SOLUTIONS LIKELY

With the passage of the last half-decade, Asia remains the most economically significant region of the global least likely to adopt uniform answers to the dilemmas of data privacy law. Convergence of national laws is only likely to occur in a limited and uneven way, and no single international instrument is likely to dominate the resolution of cross-border issues.

National laws and practices – Uneven emulation and 'GDPR creep'

The lack of any regional data privacy standard or agreement across the Asian region, or any significant standards at a sub-regional level such as ASEAN, means there is no easy path to convergence of standards in national legislation. Inconsistency continues, as it did pre-2014. The average implementation of 2nd generation (EU Directive influenced) principles across the eleven Asian jurisdictions with laws in 2014 was slightly more than 5 of the 10 principles (see Introduction). In 2019, the fourteen Asian laws covering the private sector[133] include on average just over 6 of these principles. The increases are primarily due to the new Thai law and the 2015 reforms of Japan's law, but the inclusion of both China's 2016 Law (and accompanying 'standard'), and Bhutan's law, have also increased the average.

2nd Generation – 'European standards'	EU Directive	Asian laws including standard	No.
Data retention limits (destruction or anonymisation) after processing achieved	EU Dir 6(1)(e) *GDPR 5(1)(e)*	Bhutan, HK, Indonesia, Japan, Korea, Malaysia, Macau, Philippines, Taiwan, Singapore, Thailand, Vietnam	12
Recourse to the courts to enforce data privacy rights (incl. compensation, and appeals from decisions of DPAs)	EU Dir 22, 23 *GDPR 78, 79, 82*	Bhutan, China, HK, India, Indonesia, Korea, Macau, Philippines, Taiwan, Singapore, Thailand, Vietnam	12
Minimum necessary collection for the purpose (not only 'limited')	EU Dir 6(1)(c), 7 *GDPR 5(1)(c)*	Bhutan, China, HK, India, Korea, Malaysia, Macau, Taiwan, Singapore, Thailand	10
Restricted data exports based on data protection provided by recipient country ('adequate'), or alternative guarantees	EU Dir 25 *GDPR 44-49*	China, India, Japan, Korea, Malaysia, Macau, Singapore, Thailand, Taiwan	9
Specialised Data Protection Authority(-ies) (DPA) required	EU Dir 28 *GDPR 51-59, 77*	Bhutan, HK, Japan, Malaysia, Korea, Macau, Philippines, Singapore, Thailand	9
Additional protections for sensitive data in defined categories	EU Dir 8 *GDPR 9, 10*	Bhutan, China, Japan, Korea, Malaysia, Macau, Philippines, Taiwan, Thailand	9
Rights to object to processing, including to 'opt-out' of direct marketing uses of personal data	EU Dir 14(a), (b) *GDPR 21*	Bhutan, China, HK, Korea, Malaysia, Macau, Taiwan, Thailand, Vietnam	9
General requirement, and exhaustive definition, of *legitimate processing'*	EU Dir 6(1)(a) *GDPR 5(1)(a), 6*	Bhutan, China, Korea, Malaysia, Macau, Philippines, Taiwan, Thailand	8
Prior notification to or checking by DPA of some sensitive processing	EU Dir 20 *GDPR 36*	HK, Japan, Korea, Malaysia, Macau	5
Limits on automated decision-making (incl. right to know processing logic)	EU Dir 15, 12(a) *GDPR 22*	China, Macau, Philippines	3
		Av. over 14 countries = 6.1/10 principles	86

Some of the innovations of the EU's GDPR are also already found in Asian laws. These include: data breach notification to DPA for serious breaches (China, Korea, Philippines, Thailand, Vietnam, and of limited scope in Japan), or to data subjects if of high risk (Indonesia, Taiwan, Philippines,

133 *Nepal's law, which only covers the public sector, is omitted for this purpose.*

Korea, Thailand); collective actions before DPAs or courts by public interest privacy groups (China, Korea; Philippines, Taiwan, Vietnam); DPAs able to issue administrative fines (Japan, Korea, Singapore, Taiwan, Thailand); Mandatory DPOs (Korea; Thailand); right to portability (Philippines, Thailand); extra-territorial jurisdictions based on 'targeting' (Thailand); and 'right to be forgotten' (Indonesia). This list is not comprehensive, but at least 40 examples of principles similar to GDPR innovations have already been enacted across Asia.

The main conclusion that appears from the developments in national laws since 2014 is that, while the lack of any regional standard or agreement means that national developments are not likely to be uniform, there is a measurable development of stronger data privacy principles in Asian laws, both in the increased extent of enactment of '2nd generation' 'European principles', and in the extent of uptake of new '3rd generation' principles, prompted by the GDPR. 'Convergence' is not a term applicable in Asia, except to indicate that overall standards continue to become stronger – slowly, unevenly, but in a consistent direction.

Irrespective of what GDPR-like elements are included in Asian national laws, and irrespective of the likelihood of the extra-territorial jurisdictions of the GDPR applying to companies based in Asia, it is possible that the 'unofficial' or de-facto effects of the GDPR in Asia are even more important. This 'GDPR creep' consists of both 'vertical effects' (companies headquartered outside Asia requiring their subsidiaries in Asia to be 'GDPR-compliant'), and 'horizontal effects' (companies based outside Asia requiring their suppliers of services located in Asia to be 'GDPR-compliant').[134]

International commitments – Gridlock ad infinitum?

None of the multinational instruments discussed above are likely to dominate all the others in coverage or effectiveness: the 'Osaka track' provokes dissent and has no clear objectives; the CPTPP data export and localisation clauses are unlikely to be enforced unless the US 'rejoins'; APEC-CBPRs remains a propaganda piece, not a reality; Convention 108+ has few prospects of accession; and candidates for EU adequacy are equally scarce. No initiative has adherents among a majority of significant Asian countries. At present, with no single answer to these problems, the pragmatic approach for any country may be to adopt a mix of 'solutions' – with the risk that some may be contradictory – including development of various 'appropriate safeguards'.

Data privacy dilemmas in Asia

On the Asian front of the Data Wars, it is increasingly difficult to know how many sides there are, or whose side various countries are on. Hostilities between the EU and the USA continue, but China must now be counted as a third combatant, considered hostile by both the EU and USA because of its strong stand on data localisation, which hits a sympathetic chord in many other countries, such as India and Vietnam, under the name of 'data sovereignty'. The result is confusion for allies of the main contenders (if they can decide who they are) and for neutrals caught in between. This seem likely to continue indefinitely.

134 *G. Greenleaf '"GDPR Creep" for Australian Businesses But Gap in Laws Widens' (2018) 154 Privacy Laws & Business International Report 1, 4-5 <https://ssrn.com/abstract=3226835>.*