WILL ASIA-PACIFIC TRADE AGREEMENTS COLLIDE WITH EU ADEQUACY AND ASIAN LAWS?

GRAHAM GREENLEAF

(2020) (167) Privacy Laws & Business International Report, 18-21
[2021] *UNSWLRS* 2

UNSW Law
UNSW Sydney NSW 2052 Australia

Will Asia-Pacific trade agreements collide with EU adequacy and Asian laws?

Graham Greenleaf, Professor of Law & Information Systems, UNSW Sydney

For (2020) 167 *Privacy Laws & Business International Report* 18-21

In Asia and the Pacific, two levels of 'free trade agreements' (FTAs) [1] are operating to limit the scope of data export restrictions, and to prevent enactment of data localisation requirements, They have implications for relationships between Europe and the Asia-Pacific region. [2] On the one hand, the multilateral CPTPP (Comprehensive and Progressive Agreement for Trans-Pacific Partnership) contains such restrictions, and has become more relevant because the UK has made clear its desire to accede to it. Other multilateral agreements and proposals in the Asia-Pacific contain different versions. Restrictions on data localisation are even stronger in the trilateral US - Mexico - Canada FTA (USMCA), and may influence other agreements involving the US. At the same time, bilateral FTAs involving various Asia-Pacific countries, including Singapore, Japan, Australia and Sri Lanka, and proposed for the United Kingdom, also include provisions on data exports and data localisation. This article focuses on these Asia-Pacific agreements, the extent to which they are consistent, and their possible relationship with EU adequacy decisions.

There are complex issues raised for the EU itself by its adequacy requirements for data exports, and the resulting tensions between the EU's constitutional obligations under the EU Charter, and its obligations under GATS article XIV(c)(ii),[3] but these are not the focus of this article.

Three regional models emerging from multilaterals

By 2020 three regional FTAs (one not yet finalised), with privacy-related provisions of differing strengths, provide different models for how bilateral agreements might deal with these issues.

CPTPP – An 'APEC FTA'?

The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) has eleven signatories, but came into force on 30 December 2018 with six Parties who had ratified it and deposited their accessions (Mexico, Canada, Japan, New Zealand, Australia and Singapore). Vietnam subsequently did so, giving seven current Parties. Four of the eleven signatories (Brunei, Chile, Malaysia, and Peru) have signed but not yet ratified, although they may still do so at any time (CPTPP art. 3(2)). Any other country, or customs territory may also ratify, with the consent of all the parties, and subject to any conditions agreed (CPTPP, art. 5). Nine other APEC economies have announced interest in joining CPTPP (Colombia, Indonesia,

[1] Technically, most of the agreements discussed here are not FTAs, but are 'economic partnership agreements' (EPAs) EPAs, and have a broader scope than FTAs, often covering such matters as population movement, government procurement, and forms of international cooperation. For simplicity, I will use the familiar 'FTA' terminology.

[2] The Asia-Pacific region, in this article, includes South Asian countries, and thus the whole of Asia, as well as the 'Pacific Rim'.

[3] For a detailed analysis, see Svetlana Yakovleva "Personal Data Transfers in International Trade and EU Law: A Tale of Two 'Necessities'" (2020) *Journal of World Investment & Trade* 1–39

South Korea, Taiwan, Thailand, Philippines, the US, and in May 2020, China).[4] Since 2018, the UK has stated strong interest in joining post-Brexit. The US has indicated some interest in re-joining a revised agreement,[5] which if it occurred would increase the likelihood of enforcement of its data export and data localisation provisions. Only two ASEAN countries (Singapore and Vietnam) are parties as yet.

The CPTPP's implications for privacy legislation can be summarised as:[6]

- The CPTPP has *wide scope* in relation to measures affecting trade by electronic means.
- *Government exceptions* – It does not apply to information held or processed by or on behalf of a government, or measures related to it. The provisions only apply to 'trade by electronic means' and not to non-trade processing of information.
- It imposes *a Four-Step-Test' for any exceptions to its prohibition on data export limitations*. States have the onus to prove that their legislation (i) is 'to achieve a legitimate public policy objective'; (ii) 'is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination'; (iii) is not applied so as to be 'a disguised restriction on trade'; and (iv) 'does not impose restrictions on transfers of information greater than are required to achieve the objective'.
- There are *similar data localisation prohibitions*: a prima facie ban on requiring use of computer facilities within a party's territory to conduct business within that territory, subject to the same tough four-step test to overcome the ban.

CPTPP includes two provisions which go beyond diplomatic means of enforcement:

- *State party dispute settlement* provisions can result in a panel awarding monetary assessments against a party, in lieu of the suspension of TPP benefits.
- *Investor-state dispute settlement (ISDS) provisions* could apply in limited situations, particularly where a provision could be argued to constitute direct or indirect expropriation of investments.

USMCA goes further

The United States – Mexico – Canada Agreement (USMCA), the successor to NAFTA, was agreed to on 1 October 2018, and entered into force on 1 July 2020. In relation to data export restrictions, although it uses different terms, USMCA includes substantially the same '4 step test' as in the CPTPP. However, USMCA has an outright ban on data localization, without the exceptions provided through the '4 step test' found in CPTPP. Overall, the USMCA is the next iteration, after the CPTPP, of the anti-privacy-protection provisions that the US is trying to make the norm for FTAs entered into by it or its APEC allies.[7]

RCEP goes nowhere (for now)

Another proposed Asia-Pacific EPA, with broader geographical scope that CPTPP must be kept in mind. 'There are 16 countries involved in RCEP [the Regional Comprehensive Economic Partnership]: the 10 members of ASEAN—Brunei-Darussalam, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Viet Nam plus the six countries

[4] For references for each expression of interest, see Wikipedia: Comprehensive and Progressive Agreement for Trans-Pacific Partnership.

[5] *'Trump: I would reconsider a massive Pacific trade deal if it were 'substantially better' CNBC,* 25 January 2018 <https://www.cnbc.com/2018/01/25/trump-says-he-would-reconsider-trans-pacific-partnership-trade-deal.html>.

[6] see G. Greenleaf 'Asia-Pacific Free Trade Deals Clash with GDPR and Convention 108' (2018) 156 Privacy Laws & Business International Report 22-24; see also Greenleaf 'Looming Free Trade Agreements Pose Threats to (2018) 152 Privacy Laws & Business International Report, 23-27 and earlier articles cited therein.

[7] A more detailed explanation of these USMCA provisions is in Greenleaf 'Asia-Pacific Free Trade Deals Clash with GDPR and Convention 108' op cit.

with which ASEAN has free trade agreements—Australia, China, India, Japan, Korea, and New Zealand. These six countries are known as the ASEAN free trade partners.'[8] The US, Canada and Mexico are not included, and China is a leading participant. RCEP was expected to be signed by these countries at an ASEAN summit meeting in Thailand in November 2019, but India withdrew at the last minute, so finalisation of RCEP has now stalled, while discussions with India continue.

The proposed terms of RCEP's electronic commerce chapter (Chapter 10) have now (unofficially) become public,[9] so its implications for data exports and localisation can be assessed. Key aspects are:[10]

- Chapter 10 is not subject to state-to-state dispute settlement procedures, only negotiations (draft RCEP, Ch. 10, art. 17). In contrast CPTPP is subject to such procedures.
- Cross-border transfer restrictions are superficially subject to the same '4 step test' for allowed exceptions as in the CPTPP, however the question of whether measures are those 'that [a Party] considers necessary to achieve a legitimate public policy objective' is to be decided solely by that party (draft RCEP, Ch. 10, art. 16(3) and footnote 7). Measures that a Party considers necessary for 'protection of its essential security interests' also 'cannot be disputed by other Parties'. These are significant reductions in the CPTPP restrictions.
- In similar fashion, the prohibition on requirements to use or locate computing computing facilities on a Party's territory is subject to the familiar '4 step test' for exceptions, but the question of what measures are 'necessary to achieve a legitimate public policy objective' is left solely to the decision of the implementing Party (draft RCEP, Ch. 10, art. 15 and footnote 4). There is also 'completely self-judging and non-disputable national security exemption'[11] for such data localisation. This too is weaker than the CPTPP data localisation provision.

There are other provisions in the RCEP draft deserving more discussion, particularly definitions and questions of scope (draft RCEP, arts. 2 and 3). The exclusion of government use of data is broad.

New bilateral agreements and proposals

These three multinational agreements provided Asia-Pacific countries (and others like the UK) provide three models for handling data export and data localisation questions. USMCA is the most restrictive, because there are no exceptions to its localisation ban. CPTPP is much the same on data exports, but allows exceptions to the ban on data localisation. The RCEP draft allows far more latitude, on both topics, to State parties, and fewer enforcement risks.

---

[8] New Zealand Foreign Affairs and Trade 'RCEP Overview' <https://www.mfat.govt.nz/en/trade/free-trade-agreements/agreements-under-negotiation/regional-comprehensive-economic-partnership-rcep/rcep-overview/#countries>

[9] 'RCEP e-commerce chapter text', *Bilaterals.org* website < https://bilaterals.org/?rcep-e-commerce-chapter-text-41085>;

[10] For details see Jane Kelsey 'Important differences between the final RCEP electronic commerce chapter and the TPPA and lessons for e-commerce in the WTO' *Bilaterals.org* website, February 2020 <https://www.bilaterals.org/?important-differences-between-the>.

[11] Terminology used by Kelsey, opcit.

US-Japan Digital Trade Agreement

The US-Japan DTA,[12] signed in October 2019 and in force since 1 January 2020, is in substance the same as USMCA, in that it includes the '4 step test' in relation to data exports (art. 11), but does not make any provision for exceptions in relation to data localisation, except for 'covered financial service providers' ('Location of Computer Facilities', art. 12). The agreement incorporates GATS, but excludes clause XIV(c), perhaps suggesting that in relation to data exports this agreement is more strict than GATS (art. 3(1)).

The Japan-UK CEP proposed Agreement

The UK's first major post-Brexit trade agreement, the *UK-Japan Comprehensive Economic Partnership Agreement* (CEPA) was agreed in principle by the UK's International Trade Secretary Liz Truss and Japan's Foreign Minister Motegi Toshimitsu on 11 September 2020. Newly retired Prime Minister Abe would see this as an example of the 'data free flow with trust' which he convinced the G20 to endorse.[13]

The text of the draft agreement is not yet available, but the text is expected to be finalised in October. The UK government[14] says that CEPA includes 'Cutting-edge digital & data provisions that go far beyond the EU-Japan deal. These will enable free flow of data whilst maintaining high standards of protection for personal data. … as well as introducing a ban on data localisation, which will prevent British businesses from having the extra cost of setting up servers in Japan.'

In its National Data Strategy, released at the same time, the UK describes its fifth 'mission' as 'championing the international flow of data', which will include 'looking to secure positive adequacy decisions from the EU to allow personal data to continue to flow freely from the EU/EEA to the UK, [and] implementing an independent UK Government capability to conduct data adequacy assessments for transfers of personal data from the UK.[15] It will also involve 'developing a new UK capability that delivers new and innovative mechanisms for international data transfers' and 'work with partners in the G20 to create interoperability between national data regimes'.

Nothing concrete is known beyond these brief statements, but they raise important questions:

- Commentators suggest that the 'provisions on data and digital are expected to be modelled on the CPTPP approach'[16] (discussed above). This is very plausible in relation to data export conditions (and the USMCA provisions are in effect the same). However, it is not certain that the CPTPP's '4-step test' for data export restrictions is consistent with the GDPR's requirements for adequacy, particularly in light of the *Schrems II* decision of the CJEU.
- Furthermore, the UK's description of 'provisions that go far beyond the EU-Japan deal' raises the question of whether CEPA will include the requirements (currently applying to UK-sourced data) that Japan must give special data protection treatment to EU-

---

[12] US-Japan Digital Trade Agreement 2019 <https://ustr.gov/countries-regions/japan-korea-apec/japan/us-japan-trade-agreement-negotiations/us-japan-digital-trade-agreement-text>

[13] G. Greenleaf 'G20 Makes Declaration of Data Free Flow With Trust': Support and Dissent' (2019) 160 Privacy Laws & Business International Report, 18-19

[14] UK Government Press Release 'UK and Japan agree historic free trade agreement' 11 September 2020 <https://www.gov.uk/government/news/uk-and-japan-agree-historic-free-trade-agreement>.

[15] UK Department for Digital Culture, Media and Sport *National Data Strategy*, 9 September 2020 <https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy>

[16] Stephen Booth 'What the UK-Japan trade deal signifies' *Policy Exchange*, 11 September 2020 <https://policyexchange.org.uk/what-the-uk-japan-trade-deal-signifies/>

sourced data in order to be considered to provide 'adequate' protection.[17] If the UK has dropped all special requirements for Japan, and in effect CEPA implements a 'mutual adequacy agreement', will this prevent the EU finding that UK law provides adequate protection to personal data from the EU?

- Will CEPA include a data localisation provision similar to the '4 step test' exceptions in CPTPP, or will it go further, like USMCA and the US-Japan DTA, and simply ban all data localisation requirements? Such a ban would affect not only Japan and the UK as between themselves, but would have flow-on effects affecting all other countries with which they each trade. It would also in effect mean that four of the seven existing CPTPP parties (plus the UK) are committed to an outright ban rather than to allowing the CPTPP exceptions to localisation.

Trade talks between the UK and other CPTPP parties, Australia, Canada, and New Zealand are all expected to start within the next two months,[18] and it will be significant whether they include provisions on data exports and localisation influenced by those in the UK-Japan CEPA and US-Japan DTA.

UK seeks CPTPP membership

UK International Trade Secretary Liz Truss said the Japan–UK CEPA 'is an important step towards joining the Trans-Pacific Partnership and placing Britain at the centre of a network of modern free trade agreements with like-minded friends and allies'.[19] For the UK to join the TPP would require the consent of the seven current parties, or possibly more parties unless the UK is placed at the head of the current queue of nine other countries (see above).

If the UK does accede to CPTPP, it will stop being an 'APEC agreement' and will signal that it is now becoming an agreement with potentially global reach, albeit one that affects data privacy negatively, not through positive requirements for data protection. Convention 108/108+ in contrast, is based on positive obligations, and has global ambitions.

Singapore's bilateral agreements

The Singapore – Australia 'Digital Economy Agreement' (SADEA) of 6th August 2020, in effect, only applies to data held by the private sector, and not to 'information held or processed on behalf of' one of the government Parties (art. 2(2)), except for Open Government Data (art. 25). SADEA's provisions concerning cross-border transfers (data exports) (art. 23) are in substance the same as the requirements of the CPTPP (the '4 step test'). For Australia, this does not apply to 'credit information, or related personal information, of a natural person' (art. 2(4)). So credit records of Australians, though held by the private sector, can be required to be held or processed within Australia. SADEA's provisions concerning 'location of computer facilities' (data localisation) (art. 24) are also the same in substance as CPTPP's '4 step test'. However, these data localisation exceptions do not apply to financial institutions, and cross-border financial service suppliers', provided that financial regulators can have 'immediate, direct, complete and ongoing access to information processed or stored' off-shore (art. 25).

---

[17] See G. Greenleaf, 'Japan: EU Adequacy Discounted' (2018) 155 Privacy Laws & Business International Report 8-10;

[18] Graham Lanktree '5 things to know about the UK-Japan trade deal' Politico, 11 September 2020 <https://www.politico.eu/article/five-things-from-the-uks-trade-deal-with-japan/>

[19] UK Government Press Release op cit.

A three-way Digital Economy Partnership Agreement (DEPA)[20] between Singapore Chile and New Zealand was also concluded in January 2020. Its data export and localisation provisions are in effect the same as those in SADEA.

The earlier Sri Lanka - Singapore Free Trade Agreement (SLSFTA), in force since May 2018, [21] takes a slightly less restrictive approach than the '4 step test' in vogue since CPTPP, because it omits the 4th step (least restrictive measure requirement in relation to both data exports and data localisation (see Clauses 9.9 and 9.10). SLSFTA is therefore another, slightly older (2018) variation on what is now becoming familiar.

Other Asia-Pac data export developments

Trade agreements are not the only data privacy developments affecting relationships between Asia-Pacific countries. New data privacy laws and Bills must be considered. APEC's CBPRs has attempted to provide an industry-based alternative approach for nearly a decade.

Do data localisation bans conflict with pending Asian laws?

The strict '4 step test' conditions for exceptions to data localisation bans found in the CPTPP and increasingly included in Asia-Pacific bilateral agreements raise the question of how many Asia-Pacific data privacy laws are going in the opposite direction and including data localisation requirements? Existing laws in China (since the *Cybersecurity Act* 2016), Indonesia and Vietnam do have localisation requirements, often in very imprecise terms. Bills still undergoing enactment in India,[22] Sri Lanka[23] and Pakistan[24] all have data localisation provisions, usually for something like 'critical personal data'. Thailand is the only Asian country to enact a post-GDPR data privacy law, and a cybersecurity law, which make no mention of data localisation.[25] Asia is therefore not going to become a solid wall of opposition to data localisation, no matter what Japan, Singapore, Australia and the US might prefer. CPTPP (unlike USMCA) does not include a complete ban, but its strict '4 step test' may still be too strict. 'Data free flow with trust' is not for everyone. International data privacy principles will need to accommodate justifiable versions of data localisation, rather than outright opposition.

APEC CBPRS remains a sideshow

Singapore is only the third country, with the US and Japan, to meaningfully participate in the APEC Cross-border Privacy Rules Scheme (CBPRs), because it has appointed five 'Assessment Bodies' ('Accountability Agents' in APEC jargon), to assess whether companies are CBPRs-compliant.[26] However, only one Singaporean company has as yet been certified as CBPRs-

---

[20] Digital Economy Partnership Agreement (DEPA) <https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-concluded-but-not-in-force/digital-economy-partnership-agreement/depa-text-and-resources/>

[21] See Chapter 9, 'Electronic Commerce' of the SLSFTA <https://www.enterprisesg.gov.sg/non-financial-assistance/for-singapore-companies/free-trade-agreements/ftas/singapore-ftas/slsfta>

[22] G. Greenleaf 'India's data privacy Bill: Progressive principles, uncertain enforceability' (2020) 163 Privacy Laws & Business International Report, 6-9.

[23] G. Greenleaf 'Advances in South Asian Data Privacy Laws: Sri Lanka, Pakistan and Nepal' (2019) 164 Privacy Laws & Business International Report, 22-25,

[24] G. Greenleaf 'Pakistan's DP Bill: DPA will have powers but lack independence' (2020) 165 Privacy Laws & Business International Report, 20-23.

[25] G. Greenleaf and A. Suriyawongkul 'Thailand– Asia's strong new data protection law' (2019) 161 Privacy Laws & Business International Report, 1, 3-6.

[26] IMDA (Singapore) 'APEC Cross Border Privacy Rules (CBPR) System' <https://www.imda.gov.sg/programme-listing/cross-border-privacy-rules-certification> updated 18 June 2020.

compliant.[27] It is likely that other Singaporean companies cannot see any business case to justify registration and other implementation costs. This makes sense, because Singapore has a data privacy law (*Personal Data Protection Act* 2012 – PDPA) which already imposes CBPRs-standard rules on all Singaporean companies, so overseas companies considering data exports to Singapore should be more reassured by that than by CBPRs certification. Some may also be hesitant to make representations ('APEC compliant') which could have common law consequences.

However, Singapore has done something much more significant, from the perspective of Singaporean companies wishing to legally export personal data outside Singapore: 'Singapore recognises the APEC CBPR and PRP certifications for overseas transfers of personal data under the PDPA. This means that organisations in Singapore can easily transfer personal data to the overseas certified recipient without meeting additional requirements.'[28] At present, this only assists Singaporean companies wishing to export personal data to over thirty US companies that are CBPRs-certified.[29] It adds nothing to exports to Japan, which has a law stronger than Singapore's law, and in any event has only certified three Japanese companies. It is of benefit only to the US (which has no laws sufficient to meet export requirements), and the US companies that are CBPRs-certified. Singapore is trying hard to make CBPRs meaningful, but examination still shows that its effects are still negligible. Businesses across the Asia-Pacific realise that CBPRs offers little. Within the relevant APEC sub-groups, interest is said to be shifting from CBPRs to a broader range of solutions.

ABLI's review of Asian data transfer mechanisms

A more comprehensive perspective is found in the Singapore-based Asian Business Law Institute's *Transferring Personal Data in Asia: A path to legal certainty and regional convergence* (May 2020),[30] a 78 page 'comparative review' of mechanisms used to allow personal data transfers across 14 Asia-Pacific jurisdictions from Japan to India (and including Australia). It is accompanied by a very detailed *Comparative Table on Asian Laws and Regulations on Personal Data Transfers*. A summary of key findings of the review[31] identifies the value of steps such as: Asian data privacy laws increasing the number of different mechanisms by which transfers can take place (or for regulators to clarify that they can take place); processes of convergence of less contentious aspects of these laws in the direction of higher, international, standards; and reduction on reliance on consent as the basis for transfers; and more explicit definitions of terms such as 'adequacy'. These are practical steps, and (in theory) countries that at parties to the CPTPP should also be ensuring that when they take them, they are complying with the '4 step test' as well. Perhaps giving multiple options for compliance would increase prospects of satisfying that test.

---

[27] See (Singapore) Directory of APEC Cross Border Privacy Rules (CBPR) Certified Organisations <https://www.imda.gov.sg/programme-listing/Cross-Border-Privacy-Rules-Certification/CBPR-Certified-Organisations>, listing as at 10 June 2020 only Crimsonlogic Pte Ltd.

[28] IMDA (Singapore) 'APEC Cross Border Privacy Rules (CBPR) System' op cit; On 28 May 2020 PDPC amended the PDPA Regulations to recognise certification under CBPRs or PRP as compliant with s 26 of the PDPA *(see ABLI Review, below, p. 56)*.

[29] CBPRS *CBPR Compliance Directory* <http://cbprs.org/compliance-directory/cbpr-system/>

[30] Clarisse Girot *Transferring Personal Data in Asia: A path to legal certainty and regional convergence* Asian Business Law Institute May 2020 ('ABLI Review') <https://info.sal.org.sg/abli/ebooks/privacy/>

[31] C. Girot 'Transferring data across borders in Asia: Potential for convergence' (2020) 165 Privacy Laws & Business International Report, 16-18.

Conclusions

Asia-Pacific multilateral agreements, plus a profusion of bilateral (or trilateral) FTAs involving Singapore, Australia, Canada, Mexico, Sri Lanka, the UK and the US, among others now include data export and data localisation clauses. This creates a far more complex privacy landscape in the Asia-Pacific.

These agreements bring CPTPP-inspired clauses (or the stricter USMCA version of anti-localisation) into much greater likelihood of inconsistency and conflict with, one the one hand, EU adequacy requirements of export limitations, and, on the other hand, the increasing number of Asian data privacy laws with broad mandates for data localisation. However, the RCEP agreement, if and when finalised consistent with the current draft, will contain provisions on both data exports and localisation which contain more generous exceptions than either CPTPP or USMCA, or any of the bilateral agreements to date. RCEP may involve countries not parties to either of those agreements.

Conflicts over international agreements are usually slow-moving diplomatic theatre, with dramatic events like the *Schrems II* decision being rare. However, the seeds of conflict are becoming more numerous.

Information: Prof Hiroshi Miyashita, Prof Michael Geist, other confidential commenters, and Jill Matthews have all provided valuable comments and information for this article, but responsibility for content remains with the author.