LOOMING FREE TRADE AGREEMENTS POSE THREATS TO PRIVACY

GRAHAM GREENLEAF

(2018) 152 *Privacy Laws & Business International Report* 23
[2018] *UNSWLRS* 38

UNSW Law
UNSW Sydney NSW 2052 Australia

Looming Free Trade Agreements pose threats to privacy

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

(2018) 152 *Privacy Laws & Business International Report*, 23-27

Free trade agreements (FTAs) never include requirements to strengthen data privacy laws, other than by vague and unenforceable gestures, although some continue to harbour illusions that they will.[1] Instead, FTAs may be toxic to domestic privacy laws which impose restrictions on cross-border data transfers, but the toxicity varies. Many FTAs are quite benign to privacy, such as the Agreement establishing the ASEAN-Australia-New Zealand Free Trade Area (AANZFTA), which merely requires parties to consider international standards.[2] The European Union has made it clear that 'EU data protection rules cannot be the subject of negotiations in a free trade agreement',[3] although existing EU rules can be reflected in FTAs.

In 2018, the threats to privacy legislation posed by FTAs have suddenly become more real. In February the US reiterated complaints against Chinese legislation restricting personal data exports, under the WTO's General Agreement on Trade in Services, (GATS, 1995). In March, a FTA was signed by 11 Asia-Pacific countries (including neither the US nor China) which has much stronger anti-privacy provisions than GATS: the revised TPP (now the CPTPP). Two other Asia-Pacific FTAs are under re-negotiation (NAFTA) or negotiation (RCEP). This article compares the approach being taken in each of these three FTAs (insofar as is known), and the GATS, and the potential effects of these agreements on data privacy laws.

US v China's *Cybersecurity Law* at the WTO

The GATS (General Agreement on Trade in Services, 1995) Article XIV(c)(ii) prohibits measures relating to privacy protection which are 'applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or [which are] a disguised restriction on trade in services.' After 22 years, no attempts had been made to have a WTO panel use this clause to strike down any data privacy provisions, although some considered it has potential to do so.[4]

However, following the November 2016 enactment of China's Cybersecurity Law,[5] the US submitted a communication[6] to the WTO's Council for Trade in Services (CTS), claiming that

* Valuable comments and information have been received from Peter Yu, Michael Geist, Clarisse Girot and Leon Trakman, but all content remains solely the responsibility of the author.

[1] A. Chander 'What the Trump Administration's NAFTA Priorities Get Right (and Wrong) About Digital Trade', ForeignAffairs.com 15 September 2017, proposing that NAFTA include requirements at least as strong as the APEC Privacy Framework <https://www.cfr.org/report/what-trump-administrations-nafta-priorities-get-right-and-wrong-about-digital-trade>.

[4] DFAT Australia, AANZFTA page, http://dfat.gov.au/trade/agreements/aanzfta/Pages/asean-australia-new-zealand-free-trade-agreement.aspx; see Greenleaf 'Free Trade Agreements and data privacy' section 2.2.2.

[3] European Commission 'Communication from the Commission to the European Parliament and the Council: Exchanging and Protecting Personal Data in a Globalised World' Brussels, 10.1.2017 COM(2017) 7 final

[4] See section 2.1 'GATS exception and unpredicatable WTO jurisprudence' in G. Greenleaf 'Free Trade Agreements and data privacy: Future perils of Faustian bargains' in Dan Svantesson and Dariusz Kloza *Transatlantic Data Privacy Relationships as a Challenge for Democracy* (European Integration and Democracy series) (Intersentia, 2017) <https://papers.ssrn.com/abstract_id=2732386>.

[5] G. Greenleaf and S. Livingston 'China's New Cybersecurity Law – Also a Data Privacy Law?' (2016) 144 *Privacy Laws & Business International Report* 1-7.

the law, and related measures,[7] 'would disrupt, deter, and in many cases, prohibit, cross-border transfers of information that are routine in the ordinary course of business'. The US stresses that these restrictions apply to 'personal information' and in doing so involve obtaining individual consents to transfers which would be 'an extraordinarily burdensome requirement that could disrupt business operations without contributing to privacy protections'. The US claims that 'Many less burdensome options exist to achieve privacy objectives, including compliance with international cross-border privacy frameworks, such as the APEC Cross-Border Privacy Rules System endorsed by China; contractual agreements between network operators and third party recipients; and third-party accreditation.' The US also objects to security assessments that may result in 'an outright prohibition on cross-border data transfers', and 'local data storage requirements' (data localization).

In a follow-up communication to the CTS in February 2018,[8] the US claims that at a 6 October 2017 CTS meeting 'a number of other WTO members also expressed a high degree of concern' regarding China's proposals, and requested that China refrain from finalising and implementing them. It claims that 'China has not provided any assurance that it will resolve these concerns.' The US is preparing the ground for a formal WTO dispute with China which, if it proceeds, will directly test the extent to which GATS Article XIV(c)(ii) protects privacy legislation. This could have seismic implications for data privacy laws everywhere.

The new Trans-Pacific Partnership: the CPTPP

The Trans-Pacific Partnership (TPP) was a FTA signed in February 2016 by twelve Pacific-rim nations accounting for 40 per cent of the global economy, including the US and most other significant APEC economies other than China and South Korea.[9] The new Trump Administration announced that the US would not ratify the TPP, and this meant that it was not possible for it to come into force. Despite general assumptions that this meant the TPP was dead, the other eleven TPP parties[10] signed a revised agreement, the *Comprehensive and Progressive Agreement for Trans-Pacific Partnership* (CPTPP),[11] in March 2018 in Santiago, Chile. The 11 CPTPP signatories constitute 13.5 percent of the global economy, a market of 500 million.

The uncertain parties to the CPTPP

The CPTPP will enter into force 60 days after at least six of its signatories (which need not be six of the original eleven signatories) have ratified it,[12] in relation to those signatories, and for other signatories, 60 days after they ratify it. CPTPP is, at least in theory, a FTA open to all the world: 'any State or separate customs territory may accede to this Agreement, subject to such terms and conditions as may be agreed between the Parties and that State or separate

---

[6] Council for Trade in Services - Communication from the United States - Measures adopted and under development by China relating to its cybersecurity law, S/C/W 374, 26 September 2017.

[7] As to which, see S. Livingston and G. Greenleaf 'PRC's New Data Export Rules: 'Adequacy with Chinese Characteristics'?' (2017) 147 *Privacy Laws & Business International Report* 9-12.

[8] Council for Trade in Services - Communication from the United States - Measures adopted and under development by China relating to its cybersecurity law S/C/W/376, 23 February 2018.

[9] For background, see section 3 'The Trans-Pacific Partnership (TPP) Agreement (2016) – Present Danger' in Greenleaf 'Free Trade Agreements and data privacy'.

[10] Australia, Brunei Darussalam, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, and Viet Nam.

[11] The CPTPP and explanatory documents are on the NZ Foreign Affairs and Trade (NZFAT) site <https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-concluded-but-not-in-force/cptpp/>. The specific text of the CPTPP is at <https://www.mfat.govt.nz/assets/CPTPP/Comprehensive-and-Progressive-Agreement-for-Trans-Pacific-Partnership-CPTPP-English.pdf>, which incorporates other documents.

[12] Technically, it is when they have 'notified the Depositary in writing of the completion of their applicable legal procedures', not necessarily ratification: CPTPP art. 3.1.

customs territory' (CPTPP, art. 5). It is therefore open to the US to (re)join, or to other APEC members (as South Korea and Thailand are reported to be considering), including China, or to non-APEC members (as post-Brexit UK is reported to be considering),[13] including India. The reference to accession by a 'separate customs territory' leaves the door open to Taiwan, and to the Hong Kong and Macau SARs. The parties are able to 'consider any amendment' to the CPTPP before it comes into force (art. 6), which is potentially relevant if the US tries to negotiate some other terms, as the Trump administration has suggested.

While the CPTPP could easily come into force, the fact that a country is a signatory is no guarantee that it will ratify. Who will be CPTPP's eventual parties is open to speculation.

CPTPP's potential impacts on privacy laws

The CPTPP incorporates most provisions of the TPP unchanged, with the exception of a limited set of provisions which are suspended (CPTPP art. 2 and Annex), and so the expression 'TPP' is still used in relation to the CPTPP. All of the provisions in the original TPP affecting privacy are unchanged,[14] except very slight changes to investor-state dispute settlement (ISDS) provisions. Previous criticisms of the TPPs privacy impacts are therefore also largely unchanged. The effects of CPTPP having different parties are, as explained above, completely unpredictable, and therefore ignored.

In summary,[15] the implications of the CPTPP for privacy legislation in State parties are:

(i) *Broad scope* – Chapter 14 ('Electronic Commerce') applies to 'measures adopted or maintained by a Party that *affect* trade by electronic means' (art. 14.2.2, emphasis added), so its scope may be much broader than measures that govern or 'apply to' trade, and broader than the normal meaning of 'electronic commerce'. The wide scope in relation to electronic services is confirmed by Art. 14.2.4: 'measures affecting the supply of a service delivered or performed electronically are subject to the obligations contained in the relevant provisions of Chapter 9 (Investment), Chapter 10 (Cross-Border Trade in Services) and Chapter 11 (Financial Services)'.

(ii) *Some exceptions for government* – Although government-owned or controlled enterprises may be subject to the TPP (art. 1.3), Chapter 14 does not apply to government procurement; or information held or processed by or on behalf of a government, or measures related to it (art. 14.2.3). The provisions only apply to 'trade by electronic means' and not all processing of information by electronic means. For example, localisation of processing of health data for governments should not be affected irrespective of the limits (below) on data localisation.

(iii) *Minimal requirements to protect privacy* – There is some vague and non-enforceable encouragement to parties to adopt a legal framework that protects personal information of users of e-commerce (art. 14.8), with Brunei and Vietnam being (in effect) allowed to opt out. Limits on unsolicited commercial electronic messaging (such as opt-out or opt-in) are required, with some means of recourse (art. 14.14).

---

[13] For a review of such speculation, see 'South Korea considers joining revamped Pacific trade deal CPTPP' *The Straits Times*, 13 March 2018 < http://www.straitstimes.com/asia/east-asia/south-korea-considers-joining-revamped-pacific-trade-deal-cptpp>.

[14] See NZFAT 'TPP vs CPTPP' <https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-concluded-but-not-in-force/cptpp/tpp-and-cptpp-the-differences-explained/>.

[15] These effects are explained in much greater detail in Greenleaf 'Free Trade Agreements and data privacy', sections 3.2 – 3.9.

(iv) *A 'four step test' for data export limitations* – The TPP first requires that cross-border transfers of personal information (data exports) must be allowed when this is for the conduct of the business of a service supplier from one of the TPP parties (art. 14.11.2). Any exceptions from this obligation must be justified under the 'four step test' which requires a restrictive measure to satisfy four requirements: (i) it is 'to achieve a legitimate public policy objective'; (ii) it 'is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination'; (iii) it is not applied so as to be 'a disguised restriction on trade'; and (iv) it 'does not impose restrictions on transfers of information greater than are required to achieve the objective' (art. 14.11.3). In earlier FTAs, States have not had the onus of proving all four such requirements.[16] This version may impose a 'regulatory chill' on governments considering stronger data export limitations, particularly when coupled with ISDS provisions. In analogous situations, WTO challenges to regulations have almost always succeeded, with governments being unable to satisfy all four steps.[17]

(v) *Similar data localisation prohibitions* – The TPP deals with data localisation in much the same way as data export restrictions: a prima facie ban on requiring 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 (art. 14.13 'Location of Computing Facilities'). 'Computing facilities',[18] only include those 'for commercial use', but whether that means exclusively or only primarily for such use is unclear.

(vi) *State party dispute settlement* – State parties can use the dispute settlement provisions of Chapter 28 to resolve disputes concerning interpretation or application of the TPP, whenever they consider that another party's 'actual or proposed measure' does not comply with its TPP obligations. This can result in a panel awarding monetary assessments against a party, in lieu of the suspension of TPP benefits. Given that many of the current CPTPP signatories have data export limitations in their laws, and quite a few have some data localisation requirements, there may be some reluctance to take action because of risks of 'the pot calling the kettle black'. However, this could change completely if the US re-joined CPTPP and decided to aggressively protect US data industries against cross-border restrictions.

(vii) *Investor-state dispute settlement (ISDS) provisions* – Potentially of greater importance are the procedures in relation to investment disputes under Chapter 9 ('Investment'), and the possibility of investor-state dispute settlement (ISDS) provisions being used. ISDS potentially applies whenever an investor from state party A makes an investment in the territory of state party B (art. 9.1 definition: 'investor of a Party'). The most significant investment protection relevant to data privacy is the prohibition of direct or indirect expropriation of investments,[19]

---

[16] B. Kilic and T. Israel, 'The Highlights of the Trans-Pacific Partnership E-commerce Chapter' Public Citizen/CIPPIC, 5 November 2015 <http://www.citizen.org/documents/tpp-ecommerce-chapter-analysis.pdf>.

[17] Public Citizen, 'Only One of 44 Attempts to Use the GATT Article XX/GATS Article XIV "General Exception" Has Ever Succeeded: Replicating the WTO Exception Construct Will Not Provide for an Effective TPP General Exception', August 2015, <http://www.citizen.org/documents/general-exception.pdf>. See discussion in Greenleaf 'Free Trade Agreements and data privacy', section 3.5.

[18] TPP Art. 14.1 definition: '*computing facilities* means computer servers and storage devices for processing or storing information for commercial use.'

[19] TPP Art. 9.7.1: 'No Party shall expropriate or nationalise a covered investment either directly or indirectly through measures equivalent to expropriation or nationalisation (expropriation) …'.

> except for a public purpose and for payment of fair and prompt compensation (art. 9.7.1). Failure to compensate will lead to the threat of ISDS procedures. While a breach by a party of the data export limitation or data localisation provisions will not automatically trigger entitlement to ISDS provisions by affected companies (art. 9.6.3). It could, if such breaches can be said to constitute an indirect expropriation of the investment in a company (for example, one established to be dependent on information surveillance). If so, then the possibilities of ISDS actions should frighten any country that has a data privacy law but has a smaller litigation budget than an Internet giant based in another party. Perhaps Google or Facebook are for the moment based in the wrong country, but will that change? Countries may need to draw breath both before enacting new laws, and before embarking on any strong enforcement of existing laws, for fear of an ISDS reaction. So, although ISDS provisions do not affect privacy *per se*, their interaction with data export or data localisation provisions could do so, and quite severely.

These CPTPP requirements still embody the type of binding international privacy treaty that those opposed to data privacy would like to achieve: (a) no substantive or meaningful requirements to protect privacy; (b) coupled with prohibitions on data export limitations or data localisation requirements that can only be overcome by a complex 'four-step test' of justification; and (c) backed up by the risk of enforcement proceedings between states or under ISDS provisions, both involving uncertain outcomes from dubious tribunals and potentially very large damages claims.

Of the current CPTPP signatories, it is not clear which, if any, are likely winners from this. But if the US decides to rejoin, the other parties have handed to it and to US companies their heads on a platter. This FTA is potentially very toxic for data privacy laws.

The anti-privacy virus spreads from Singapore to Sri Lanka

Even before the CPTPP was signed, the Singapore-Sri Lanka FTA of January 2018[20] included an e-commerce chapter based on the TPP, including data localization and data transfer provisions (text not yet officially available, may be released on 1 April). Michael Geist, who has seen the text, comments that 'it is concrete evidence that the TPP e-commerce chapter is like a virus that will spread to non-TPP countries [and] it is particularly problematic in the case of Sri Lanka, since that country does not even have general privacy protections'.[21]

NAFTA renegotiated?

The North American Free Trade Agreement (NAFTA), currently being renegotiated between the US, Canada and Mexico, came into force in 1994 before the Internet was in common commercial use. Canada and Mexico have comprehensive data privacy laws including some personal data export restrictions, the US does not. In 2017 the US informed the other NAFTA parties that it proposed to renegotiate the agreement, including to include a new 'digital trade chapter'.[22] Its proposed contents are as yet unknown. It is possible that the Trump Administration may instead withdraw the US from NAFTA, given its distaste for multilateral FTAs.

---

[20] L. Chia 'Singapore and Sri Lanka sign free trade agreement', *Channel News Asia* 23 January 2018 <https://www.channelnewsasia.com/news/singapore/singapore-and-sri-lanka-sign-free-trade-agreement-9886990>

[21] M. Geist, personal correspondence with the author, 20 March 2018.

[22] This is sometimes described as the NAFTA parties agreeing to update the agreement: S. A. Aronson *Information Please: A Comprehensive Approach to Digital Trade Provisions in NAFTA 2.0* Centre for International Governance Innovation (CIGI), November 201 <https://www.cigionline.org/sites/default/files/documents/Paper%20no.154web.pdf>.

The US objectives in the renegotiations, include that the US seeks to 'establish rules to ensure that NAFTA countries do not impose measures that restrict crossborder data flows and do not require the use or installation of local computing facilities'.[23] In other words, the US seeks restrictions in the same categories as in the TPP and the CPTPP: data export limitations and data localisation.

Canada's representation in the negotiations is by a 'NAFTA Council' which has been criticised as 'missing key perspectives and representation from the privacy and access profession, and from civil society.[24] Canada's position has also been criticised as supporting data localisation only for government data, and being too willing to accept bans on data localisation in relation to data held by the private sector.[25] Even this limited Canadian position is likely to conflict with US demands aimed against laws in British Columbia and Nova Scotia 'requiring personal information collected by governments, such as health records, to be stored on [Canadian] domestic servers to prevent it being accessed for reasons other than those for which it was collected'.[26] Canada's position supports government exemptions, but will it prevail?

If the US succeeds in establishing strong anti-privacy rules in NAFTA, this may become its benchmark for future bilateral or multilateral FTAs (assuming it enters into them in future).

RCEP – A rival pact?

There are 16 countries involved in the Regional Comprehensive Economic Partnership (RCEP) negotiations: the ten members of ASEAN[27] plus the six countries with which ASEAN has free trade agreements—Australia, China, India, Japan, Korea, and New Zealand. These 'ASEAN Free Trade Partners' are economically much more significant than the ASEAN countries. The 16 RCEP countries have a total population of more than 3 billion, a total GDP of around $US23 trillion (2015 IMF figures), and they account for about 27% of global trade (2014 UNCTAD figures). Potentially, RCEP is twice as large in trade terms as the CPTPP's current signatories.

RCEP negotiations began in 2012 and have involved 21 rounds of negotiations since then.[28] As Yu points out, the RCEP negotiations include many countries intentionally excluded from the TPP negotiations: both China and India, but also Indonesia and a number of smaller ASEAN countries. These are all countries that might have had difficulty meeting some of the higher standards of various TPP chapters. One potential role for RCEP is as a TPP rival, with less

---

[23] United States Trade Representative *Summary of Objectives for the NAFTA Renegotiation* November 2017 <https://ustr.gov/about-us/policy-offices/press-office/press-releases/2017/november/ustr-releases-updated-nafta>.

[24] Privacy & Access Council of Canada 'NAFTA Renegotiation will affect information privacy, access to information, and data protection compliance in Canada', undated, <https://pacc-ccap.ca/nafta-renegotiation-will-affect-information-privacy-access-to-information-and-data-protection-compliance-in-canada/>; citing M. Geist 'Canada's NAFTA Council: Political and Industry Boxes Checked But Missing Key Perspectives', *Michael Geist Blog*, 3 August 2017, <http://www.michaelgeist.ca/2017/08/canadas-nafta-council-political-industry-boxes-checked-missing-key-perspectives/>

[25] M. Geist 'Canadian Position on Data Localization Rules in Trade Deals Revealed: Protection for Government Data Only', *Michael Geist Blog*, 18 December 2017 <http://www.michaelgeist.ca/2017/12/canadian-position-data-localization-rules-trade-deals-revealed-protection-government-data/>

[26] Janyce McGregor 'NAFTA talks: U.S. proposal for cross-border data storage at odds with B.C., N.S. law' CBC News, 25 July 2017 < http://www.cbc.ca/news/politics/nafta-data-storage-privacy-1.4220272>

[27] ASEAN members: Brunei-Darussalam, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Viet Nam.

[28] For a detailed history and analysis of significance of RCE, see P. K. Yu 'The RCEP and Trans-Pacific Intellectual Property Norms', 50(3) *Vanderbilt Journal of Transnational Law* 673; for subsequent details see Wikipedia: Regional Comprehensive Economic Partnership.

demanding standards, and different leadership.[29] After completion of negotiations by the 'RCEP 16', it is intended that other countries may apply to join.

The most recent RCEP Ministerial statement[30] discloses little concerning the potential content of RCEP, and other than for leaked intellectual property and investment draft chapters, few details are known widely. The investment chapter has been described as 'designed to give private parties the right to extract costly damages from governments that implement policies that harm profits'.[31] An e-commerce draft chapter, the most likely to affect privacy laws, was first discussed in 2015 negotiations in Thailand, with nine meetings since then. It is not know for certain whether an e-commerce chapter will be included. On the one hand, privacy-hostile governments such as Australia have been actively seeking evidence of deleterious effects of data export restrictions and data localisation,[32] and free trade zealots in business groups are advocating complete abandonment of any restrictions on data exports.[33] On the other hand, while consumer NGOs were expecting such restrictions to appear in an e-commerce chapter and were starting to organise resistance on behalf of consumers and citizens,[34] by late 2017 one NGO expert concluded 'it seems that the e-commerce chapter is going to be less ambitious and contentious than that of the TPP' and will avoid data localisation.[35] Despite this optimism, it is clear enough that there is a strong push to include the same types of anti-privacy provisions in RCEP as are now included in the CPTPP, but on the other hand, why should countries with strong data export and/or data localisation laws, such as China and Indonesia, welcome provisions aimed at making those laws illegal?

All that it is possible to yet conclude is that RCEP will probably constitute the next important site of contestation over the role of FTAs in constraining national independence in relation to data flows of personal information.

Can FTAs endanger EU adequacy?

An unanswered question is whether, by becoming a party to a FTA which places limits on its ability to enact data export restrictions affecting 'onward transfers' of personal data originating from the EU, a non-EU country might endanger its ability to obtain a positive 'adequacy' finding under the EU's GDPR. Limits which are consistent with GATS article XIV(c)(ii) should not present a problem, because EU countries are also bound by the GATS. We must assume that the GATS is consistent with the GDPR (and vice-versa) until proven incorrect. However, stronger FTAs may not be consistent with the GDPR.

Canada's adequacy status must be re-assessed under the GDPR within four years, so NAFTA may affect it, and Mexico will be affected if it seeks an adequacy assessment (it is currently applying to accede to CoE Convention 108). New Zealand and Canada are parties to the CPTPP who also must face adequacy re-assessments. The effect of the CPTPP may first be

---

[29] Yu 'The RCEP and Trans-Pacific Intellectual Property Norms', 685-692.

[30] The Fourth Regional Comprehensive Economic Partnership (RCEP) Intersessional Ministerial Meeting, , Joint Media Statement, 3 March 2018, Singapore <http://asean.org/storage/2018/03/JMS-4th-RCEP-ISSL-MM-FINAL-0303181.pdf>.

[31] J. Love '2015 Oct 16 version: RCEP draft text for investment chapter' 22 April 2016 *Knowledge Ecology International* website <https://www.keionline.org/23065>.

[32] Australian Government *RCEP Negotiations: Discussion Paper on Electronic Commerce*, May 2017.

[33] For example D. Elms, Asian Trade Centre *E-Commerce and Digital Trade Proposals for RCEP*, Auckland Round, June 2016: 'Proposed RCEP language. No Party may prevent a service provider of another Party from transferring information outside the Party's territory, including personal information.'

[34] J. Panday 'RCEP Discussions on Ecommerce: Gathering Steam in Hyderabad' Electronic Frontier Foundation, 24 July 2017 <https://www.eff.org/deeplinks/2017/07/rcep-discussions-ecommerce-gathering-steam-hyderabad>.

[35] J. Panday 'E-commerce RCEP Chapter: Have Big Tech's Demands Fizzled? 'Electronic Frontier Foundation, 4 August 2017 < https://www.eff.org/deeplinks/2017/08/e-commerce-rcep-chapter-have-big-techs-demands-fizzled>.

fseen when the EU makes a decision concerning Japan's current application for a positive 'adequacy' assessment, since Japan is a CPTPP signatory. Korea is not yet a CPTPP signatory, though it is a negotiating party in RCEP, and has also applied to the EU for an adequacy finding. For both Japan and Korea, onward transfer limitations are an issue in their EU adequacy applications.[36]

Conclusions: Out of the bottle

After decades during which free trade agreements have been a potential threat to privacy, the potential has come much closer to reality with US actions against China in the WTO CTS, and with the February 2018 signing of the CPTPP by a very economically significant group of eleven countries. The anti-privacy virus is out of the bottle, with its effects already felt in a bilateral FTA and likely to be replicated in NAFTA. Whether the potentially more powerful RCEP agreement will follow or perhaps abandon this direction is unpredictable, as is the future extent of the US's influence.

Stop Press: Trump's TPP U-turn increases privacy dangers

Since this article was written, President Trump has ordered US officials to examine the US joining the revised TPP (CPTPP) but only 'if the deal were substantially better than the deal offered to Pres. Obama' (as per Presidential tweet).[37] The current terms of the CPTPP have suspended some terms originally inserted for US benefit, and adding even better terms may be resisted strongly, so there is no reason to assume that the Trump aim will be achieved. US 're-entry' would also have to be ratified by Congress, possibly one with different numbers after the November 2018 mid-term elections. The 'unknowns' are therefore very high, but as this article has argued, a CPTPP open to enforcement actions by the US and US companies would be one which has become considerably more dangerous to privacy.

---

[36] G. Greenleaf 'Questioning 'Adequacy' (Pt I) – Japan' (2017) 150 *Privacy Laws & Business International Report*, 1, 6-11; 'Questioning 'Adequacy' (Pt II) – South Korea' (2018) 151 *Privacy Laws & Business International Report* 14-16.

[37] S. Donnan 'Brazen about-face by Trump in TPP policy rethink' *The Financial Times*, 14 April 2018.