The TPP Agreement:
An anti-privacy treaty for most of APEC

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

(2015) 138 *Privacy Laws & Business International Report*, 21-23, December 2015

Twelve Pacific-rim nations accounting for 40% of the global economy, including most significant APEC economies other than China, have reached agreement on a historic free-trade agreement, or are queuing up to join. The Trans-Pacific Partnership Agreement (TPP)[1] was signed in Atlanta, Georgia on 5 October at the conclusion of eight years of negotiation.

The TPP is primarily an agreement 'to establish a free trade area',[2] an agreement which 'will strip thousands of trade tariffs in the region and set common labour, environmental and legal standards among signatories.'[3] But it is also the first legally-binding agreement affecting data privacy that has been entered into by APEC members, although it is not formally an APEC (Asia-Pacific Economic Cooperation) instrument. The APEC Privacy Framework (2004), like all other APEC 'agreements', is not legally binding on its parties. In contrast, the TPP is a real international agreement, with enforcement provisions.

The TPP only imposes the most limited positive requirements for privacy protection, but imposes stronger and more precise limits on the extent of privacy protection that TPP parties can legally provide. The principal aim of this article is to explain these provisions and their overall effect on privacy protection.

The parties, now and future: A treaty for almost all of APEC, perhaps beyond

All twelve initial parties to the TPP are APEC member economies: Australia; Brunei Darussalam; Canada; Chile; Japan; Malaysia; Mexico; New Zealand; Peru; Singapore; the United States; and Vietnam. Four more APEC member countries have stated they wish to join the TPP: Indonesia, the second most populous country in APEC;[4] South Korea, the third-largest economy in East Asia;[5] as well as Taiwan;[6] and the Philippines.[7] That leaves just five of the twenty-one APEC member economies not involved at present. Neither China nor the Hong

* * Valuable comments have been received from Prof Nohyoung Park, Prof Leon Trakman, Chris Connolly, Prof Lee Bygrave, Sanya Reid Smith and Blair Stewart. All content remains the responsibility of the author.

[1] New Zealand Foreign Affairs & Trade 'Text of the TPP Agreement' <http://tpp.mfat.govt.nz/text>

[2] TPP, Article 1.1.

[3] Nick O'Malley ' The Trans-Pacific Partnership: Pacific countries agree to historic trade pact' *The Sydney Morning Herald* , 6 October 2015 <http://www.smh.com.au/business/the-economy/tpp-deal-pacific-countries-agree-to-historic-trade-pact-20151005-gk1vq2#ixzz3ruWzAAic>

[4] 'Indonesia will join Trans-Pacific Partnership, Jokowi tells Obama' *The Guardian* 27 October 2015

[5] Jessica J Lee 'The Truth About South Korea's TPP Shift' *The Diplomat*, 23 October 2015 <http://thediplomat.com/2015/10/the-truth-about-south-koreas-tpp-shift/>

[6] Executive Yuan 'Taiwan determined to join TPP' 27 October 2015

[7] Reuters 'Philippines' Aquino wants to join Trans-Pacific Partnership', 14 October 2015 <http://uk.reuters.com/article/2015/10/14/uk-philippines-trade-tpp-idUKKCN0S80WJ20151014>; see also Prashanth Parameswaran 'Confirmed: Philippines Wants to Join TPP', *The Diplomat*, 25 June 2015 <http://thediplomat.com/2015/06/confirmed-philippines-wants-to-join-tpp/>

Kong SAR, both APEC members, are parties to the TPP,[8] although significant opinion-makers in China are open to joining the TPP.[9] The other 'missing' APEC member economies are Papua New Guinea, Russia and Thailand.

It is still speculative whether, and when, the TPP will come into force. The final drafting of the document will not be completed for at least a month.[10] The US Congress will then have three months to review it before it votes whether or not to support it. Every other party will also need to go through any domestic processes required for ratification, possibly including enacting legislation. Many politicians on both sides of US politics have expressed opposition to the TPP, and there is still some opposition in Japan.

Scope limited to measures affecting trade

Chapter 14 ('Electronic Commerce') applies to 'measures adopted or maintained by a Party that affect trade by electronic means', so the scope may be much broader than measures that govern or 'apply to' trade.

However, it does not apply to '(a) government procurement; or (b) information held or processed by or on behalf of a Party, or measures related to such information, including measures related to its collection' (Article 14.2.2). Although government owned or controlled enterprises may be subject to the TPP,[11] this provision creates exclusions. It will for most purposes exclude the collection or processing of information by or on behalf of governments, reinforcing that the provisions only apply to 'trade by electronic means' and not all processing of information by electronic means. This means, for example, that legislation requiring local storage and processing of government information is exempt from the TPP. In such cases, there is no need to consider the data localisation restrictions in Article 14.13.

The scope of any privacy protection required is further limited to only some private sector activities by Article 14.8, next discussed.

Weak data protection requirements

Article 14.8 ('Personal Information Protection') is the only TPP provision requiring some positive protection of personal information, other than the direct marketing provision.

For the purpose of 'enhancing consumer confidence in electronic commerce',[12] (but without any mention of protecting human rights) Article 14.8.2 requires that 'each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce'. This legal framework need only apply to 'users of electronic commerce'. It need not apply to all private sector activities (even if commercial), nor to categories of private sector personal data such as employee information. Public sector

[8] Macau SAR, the other Chinese territory which has a data privacy law, is not an APEC member economy.

[9] Reuters 'China communist party paper says country should join U.S.-led trade pact', 24 October 2015 <http://www.reuters.com/article/2015/10/25/us-china-trade-tpp-idUSKCN0SJ01X20151025#2GF0PVwz1pTAh15m.99>

[10] ibid

[11] TPP Article 1.3, definition of 'enterprise': 'enterprise means any entity constituted or organized under applicable law, whether or not for profit, and whether privately or governmentally owned or controlled, including any corporation, trust, partnership, sole proprietorship, joint venture, association, or similar organization.'

[12] TPP Article 14.8.1: 'The Parties recognise the economic and social benefits of protecting the personal information of users of electronic commerce and the contribution that this makes to enhancing consumer confidence in electronic commerce'.

personal data need not be included unless it comes within 'electronic commerce', and even then might fall outside Article 14.2.2 discussed above.

As to what type of 'legal framework' will suffice, a note to Article 14.8.2 specifies that '[f]or greater certainty, a Party may comply with the obligation in this paragraph by adopting or maintaining measures such as a comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy'. This last clause seems to be written with the US Federal Trade Commission in mind. Given that a 'legal framework' is required, mere self-regulation would not appear to be sufficient, which is an advance on the APEC Privacy Framework.[13] However, since a 'measure' is defined to include 'any … practice' (Article 1.3), as well as laws, even this is not completely free from doubt.

Article 14.8.2 also requires that 'in the development of its legal framework for the protection of personal information, each Party should take into account principles and guidelines of relevant international bodies'. However, no specific international instruments are mentioned, and there is no list of principles included in the TPP. Nor are any specific enforcement measures mentioned. These absences make the 'legal framework' required by the Article completely nebulous.

Article 14.8.5 provides that 'Recognising that the Parties may take different legal approaches to protecting personal information, each Party should encourage the development of mechanisms to promote compatibility between these different regimes. These mechanisms may include the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement, or broader international frameworks.' The APEC Cross-border Privacy Rules Scheme (CBPRs) purports to be such a mechanism, but the 'autonomous' recognition of EU 'adequacy' status, or recognition under other 'white-list' approaches could also constitute such 'recognition of regulatory outcomes'.

Article 14.8.3 requires that '[e]ach Party shall endeavour to adopt non-discriminatory practices in protecting users of electronic commerce from personal information protection violations occurring within its jurisdiction'. 'Non-discriminatory practices' is not defined, but would presumably include a requirement that data privacy laws should not limit their protection only to the citizens or residents of the country concerned, as was once the case with privacy laws in countries such as Australia, and is still proposed in India. In any event, the inclusion of 'shall endeavour' removes any force from this provision, as does 'shall encourage' in Article 14.8.5.

Direct marketing limitations

Parties are required to take measures (which need not be laws) regarding unsolicited commercial electronic messages, to facilitate recipients preventing their ongoing receipt (opt-out), or requiring consent to receipt (opt-in), or otherwise providing for their minimisation. They must provide 'recourse' (which is not required for general privacy protection) against non-compliant suppliers, and shall endeavour to cooperate with other Parties (Article 14.14: Unsolicited Commercial Electronic Messages). Brunei, which does not currently have a data protection law, is given time to comply.

Restrictions on data export limitations

'Cross-Border Transfer of Information by Electronic Means' is addressed in Article 14.11. It first recognises 'that each Party may have its own regulatory requirements concerning the

[13] G Greenleaf *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (OUP, 2014), p. 36.

transfer of information by electronic means' (Article 14.11.1). It then requires that cross-border transfers of personal information be allowed when this activity is for the conduct of the business of a service supplier from one of the TPP parties.[14]

Any exceptions from this obligation to allow personal data exports must be justified under Article 14.11.3, which allows such a restrictive measure only if it satisfies four requirements: (i) it is 'to achieve a legitimate public policy objective'; and (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.'[15]

Alleged failure to meet any one of these requirements in this 'four-step-test' could result in a country's data export restrictions facing dispute settlement proceedings. This four-step-test is typical of conditions to allow exceptions in trade agreements, and is not an extreme restriction on data exports or localisation (at least not compared with what might have been included). For example, the aim of obtaining a positive 'adequacy' assessment by the European Union could be argued to be a 'legitimate policy objective'. However, it is of concern that these requirements might create a 'regulatory chill',[16] particularly when coupled with ISDS provisions (as discussed below).

Prohibitions on data localisation

Snowden revelations and the European Court of Justice[17] have confirmed that personal data cannot be protected against US agencies once it is located on US servers. One response is for a country to require that some categories of data be only stored and processed on local servers ('data localisation').

The TPP deals with data localisation in much the same way as data export restrictions: a *prima facie* ban, subject to tough tests to overcome the ban. Its anti-data-localisation provisions are in Article 14.13 ('Location of Computing Facilities'), which follows a similar approach to the data export provisions. First, formal acknowledgment is given to each Party's right to have its own 'regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications' (Article 14.13.1). 'Computing facilities', for this Article, only include those 'for commercial use'. [18]

Then, a TPP Party is prohibited from requiring a service supplier from one of the TPP parties (a 'covered person') 'to use or locate computing facilities in that Party's territory as a

---

[14] TPP Article 14.11.2: "Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person'. See also Article 14.1, definition of 'covered person'.

[15] TPP Article 14.11.3: 'Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on transfers of information greater than are required to achieve the objective.''

[16] Luke Nottage and Leon Trakman 'As Asia embraces the Trans-Pacific Partnership, ISDS opposition fluctuates' *The Conversation* (Australia) 20 November 2015 <https://theconversation.com/as-asia-embraces-the-trans-pacific-partnership-isds-opposition-fluctuates-50979>

[17] *Maximillian Schrems v Data Protection Commissioner* (6 October 2015) Court of Justice of the European Union, Judgment in Case C-362/14

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

condition for conducting business in that territory' (Article 14.13.2). In other words, data localisation is *prima facie* banned. Then, the same 'four-step-test' of justification for any exceptions is applied as was the case for data export limitations.[19]

Russia's data localisation requirements would have little chance of passing these tests, if it became a TPP party. Data localisation requirements in the laws of Vietnam and (if it joins TPP) Indonesia will have to meet the four-step-test or breach TPP.

Both the data export and data localisation provisions are subject to exceptions in the lists of Non-Conforming Measures (NCMs) accepted for each State party. There are no specific NCMs for articles 14.11 or 14.13, but they could be affected by exceptions phrased in general terms for some States.

Dispute settlement

State parties to the TPP can use Chapter 28's dispute settlement provisions involving specially constituted panels, to resolve disputes concerning interpretation or application of the TPP. 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. Most of these provisions pose few problems for privacy protection. A breach by a party of the data export limitation and data localisation provisions will not automatically trigger entitlement to ISDS provisions by affected companies in, say, the USA (Article 9.6.4).

The most significant investment protection relevant to data privacy is the prohibition of direct or indirect expropriation of investments,[20] except for a public purpose and for payment of fair and prompt compensation (Article 9.7.1). Failure to compensate will lead to the threat of ISDS procedures. However, what if the main benefit to a company in the US, in setting up e-commerce facilities in another country, was the transfer of personal data to the US where data privacy laws posed far less interference in what could be done with the data than under the laws of that country? Could breaches of the data export limitation or data localisation provisions then constitute an indirect expropriation of the investment? The ISDS possibilities should frighten every country that has a data privacy law but has a smaller litigation budget than Google or Facebook.

This may not cause countries that already have data export restrictions to rush to water them down, but any party that is considering enacting new or stronger data privacy laws (including any data localisation) will have to give some very serious thought to the possibilities of actions, particularly ISDS actions. They may also need to draw breath before embarking on any strong enforcement of existing laws, for fear of an ISDS reaction.

Conclusions: A Faustian bargain

These TPP requirements seem to embody the type of binding international privacy treaty that the US (in particular) wishes 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,

[19] TPP Article 14.13.3: 'Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective. '

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

both involving uncertain outcomes from dubious tribunals[21] and potentially very large damages claims. This approach is consistent with the 2013 revisions to the OECD privacy Guidelines,[22] but with much sharper teeth.

For the US, it is a great deal: no need to worry about how strong local privacy laws in other countries may be (that battle is largely lost anyway, with 109 countries already with data privacy laws[23]), because it will now be more difficult to prevent most personal data from being exported to the US, where such laws do not significantly impede commercial use, and where state surveillance also has wide reign. Perhaps there are TPP signatories other than the US aiming to be net personal data importers, or who explicitly don't care about to which overseas countries their own citizens' personal data is exported, but they are difficult to identify.

For all the other states whose personal data will be 'hoovered up', it is more likely to be a Faustian bargain: put at risk the protection of the privacy of your citizens (except at home) in return for the golden chalice of trade liberalisation. TPP may mean no enforceable requirements of privacy protection, but enforceable free flow of personal data, and a one-way flow at that. For privacy, it is a poor bargain. The main problem with the TPP is that human rights such as privacy protection should not be bargaining chips in trade agreements, where they require that states decide what their protection is worth compared with greater access to trade in bananas[24]

The strength of this argument depends on the extent to which the two four-step-tests (satisfaction of which will now be required to justify data export restrictions or data localisation requirements), coupled with the prospect of ISDS actions, will have the consequences of regulatory chill and regulatory roll-back that I predict and fear. There can be reasonable arguments that they will not. But should this risk be taken?

The TPP is the first multilateral trade agreement with detailed provisions relating to privacy protection. If the TPP is defeated in the US Congress, this will be a net gain for privacy protection, whatever one thinks about the other potential economic advantages of the TPP. The TPP's privacy-related provisions reflect US interests to a considerable extent. It remains to be seen whether future multilateral trade agreements will contain similar provisions.

---

[21] Hill, above.

[22] Greenleaf *Asian Data Privacy Laws*, Ch 19, section 3.1 'Revised OECD privacy Guidelines 2013'.

[23] G Greenleaf, G 'Global data privacy laws 2015: 109 countries, with European laws now in a minority' (2015) 133 *Privacy Laws & Business International Report,* 14-17.

[24] 'This is not bananas we are talking about' said Spiros Simitis, 'Europe's de facto privacy doyen', when discussing EU/US tensions over the 1995 EU privacy Directive, cited by Lee Bygrave 'International agreements to protect personal data', J Rule and G Greenleaf (Eds) *Global Privacy Protection: The First Generation*, Edward Elgar, 2008, p. 15.