The TPP & Other Free Trade Agreements: Faustian bargains for privacy?

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

WORKING DRAFT – Comments please: <mailto:graham@austlii.edu.au>

14 February 2016 – 10,500 words

Contents

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

Introduction – Bargaining with privacy rights

Free Trade Agreements (FTAs) are not likely to be sources of privacy rights, but may act as limitations on the operation of privacy laws. Countries negotiating new bilateral or multilateral trade agreements, particularly but not exclusively the USA, are likely to attempt to include a requirement that the parties do not include any significant data export restrictions, or 'data localisation' provisions in their laws.

In this paper, the effect of FTAs on data protection / data privacy prior to 2015's Trans-Pacific Partnership (TPP) agreement is first considered, then the TPP's effect is analysed in some detail, followed by consideration of future FTAs still at the negotiation stage. The TPP is the first multilateral trade agreement with detailed provisions relating to privacy protection.

The USA's forum-shifting on data exports

The USA is masterful at forum-shifting to attain its diplomatic goals:[1] at one time it will focus on bilateral relationships, then shift to regional agreements, next global multilateral fora – and back and forth as the need requires. Other countries do similarly, but none with the stamina of the USA. Since the first national data privacy laws in the 1970s, the USA (through both trade diplomats and US Chambers of Commerce and the like) has steadfastly opposed all impediments to the transfer of personal data from other countries to US companies, and to the US government. This often involves opposition to countries enacting strong data privacy laws at all, but that has proven to be a losing battle, with 109 jurisdictions having now adopted such laws, most of them including data export restrictions of some type.[2] With multilateral agreements the US has had significant success in keeping both the 2013 revisions to the OECD privacy Guidelines, and the APEC Privacy Framework, weak and unenforceable and with no data export restrictions of concern. For nearly two decades it seemed as though it had tamed the toughest regional data export restrictions, those in the EU data protection Directive, by obtaining a 'Safe Harbor' for its companies from the EU. That stratagem failed with the *Schrems* decision finding that it was illegal for the European Commission to bargain with privacy rights instead of following the Directive's requirements. The proposed replacement, the 'EU-US Privacy Shield' agreement negotiated by the EU Commission, still has many hurdles to jump before it is adopted. Attempts to convince the EU that there was some type of 'interoperability' with the APEC Cross-border Privacy Rules system (APEC-CBPRs), that should be accorded a willing suspension of disbelief by the EU, have also been politely dismissed.[3]

This article concerns yet another US stratagem to prevent personal data export restrictions, and another complex set of fora in which this game is played out: free trade agreements (bilateral, regional and global), and the shadowy world of FTA negotiations. It is very similar territory to the world of TRIPS and trade in which the USA succeeded with IP.

Data privacy agreements: Not bananas

International treaties are bargains between countries. There have been a number of international agreements concerning privacy rights, but they have been of a very different nature from Free Trade Agreements. Council of Europe Convention 108 (1981), the EU data protection Directive (1995), and the near-complete EU data protection Regulation (2015) all

[1] For a sustained discussion of its successes in the field of intellectual property, see Peter Drahos with John Braithwaite *Information Feudalism: Who Owns the Knowledge Economy?* Earthscan 2002, particularly chapters 6 and 7.

[2] 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 <http://ssrn.com/abstract=2603529>

[3] For a summary, see Graham Greenleaf *Asian Data Privacy Laws* (OUP, 2014) Chapter 18, Section 2.

involved guarantees of free flow of personal data (an aspect of freedom of speech) in return for guarantees of minimum standards of privacy protection by other parties, so as to ensure that free flow of personal data would not endanger the privacy of their citizens. Although they are not binding international agreements, the OECD Guidelines (1980) and the APEC Privacy Framework involve similar balancing of privacy-related interests. The other international agreements involving rights of privacy are the International Covenant on Civil and Political Rights (1967) and the European Convention on Human Rights (1953), each of which involve the parties making commitments to protect numerous human rights, subject to certain conditions, in return for other countries doing likewise. These involve some trade-offs in relation to privacy protection, because (for example) the right of free expression necessarily place limits on the right of privacy. Similarly, freedom of religion, or of other beliefs, would be meaningless unless there was some protection of privacy. So these agreements can be described as bargains that only concern human rights, and necessarily must consider more than one human right.

Free trade agreements require countries to do something quite different. They must decide the extent to which stronger protection of their citizens' privacy should be traded for greater access to foreign markets in rice, cars or textiles. Should freedom of speech, freedom of religion, the right to criticise foreign governments, or to legislate for marriage equality, or against racial discrimination, be traded in FTAs for reduced tariffs on car tyres or wheat or liberalisation of insurance service markets? If not, they why should the privacy rights of a country's citizens be bargaining chips? As Spiros Simitis, 'Europe's de facto privacy doyen', said when discussing EU/US tensions over the 1995 EU privacy Directive, 'This is not bananas we are talking about.' [4]

Taking this approach, the only role that privacy rights should play in Free Trade Agreements is a negative one: as explicit exceptions confirming that other FTA provisions have nothing to do with limiting the protection of privacy (or other human rights). Perhaps it is reasonable that there should also be limitation on such privacy protections where they are shams, merely disguising limitations on trade but with no justifiable role in privacy protection. But how can these be included in FTAs without real privacy protections also being sacrificed, bargained away for bananas?

This article therefore examines the history and likely future of privacy-related provisions in FTAs, taking a sceptical view of the relationship of FTAs to human rights.[5]

FTAs and privacy prior to 2015's TPP

Until 2015 the most significant multilateral FTAs referring to privacy or data protection have been the global General Agreement on Trade in Services (GATS), and some regional multilaterals. There are however a large number of completed regional multilateral FTAs, with one incomplete list including 21 such agreements.[6] Some examples are discussed here, particularly from the Asia-Pacific region.

---

[4] As described and 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.

[5] For a detailed discussion of human rights considerations in relation to the TPP and other FTAs, see Sanya Reid Smith 'Potential Human Rights Impacts of the TPP', section 'Some TPP issues common to multiple human rights', Third World Network, 2015 <http://www.twn.my/title2/FTAs/General/TPPHumanRights.pdf>.

[6] *List of multilateral free trade agreements* - Operating agreements (Wikipedia) <https://en.wikipedia.org/wiki/List_of_multilateral_free_trade_agreements>: ASEAN Free Trade Area (AFTA) - 1992; ASEAN–China Free Trade Area (ACFTA) - 2010; ASEAN–India Free Trade Area (AIFTA) - 2010; Asia-Pacific Trade Agreement

Bilateral FTAs, of which there are a vast number,[7] sometimes refer to data protection, but often only in very general terms. They are not discussed here.

GATS exception and unpredictable WTO jurisprudence

The issue of privacy laws being used as trade barriers could potentially be raised at the World Trade Organization (WTO). Article XIV(c)(ii) of the GATS (General Agreement on Trade in Services, 1995) provides that:

> Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures: . . . (c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to: . . . (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts.

The Article's carve-out of data privacy protections therefore includes three potentially significant limits. The chapeau refers to both application of measures which constitute 'unjustifiable discrimination between countries', and to 'disguised' trade restrictions. The Article also requires that the enforcement measures are 'necessary' to secure compliance with the data privacy laws enacted.

There have been few extensive discussion of the implications of this and other GATS provisions[8] for data privacy restrictions. The New Zealand Law Commission[9] in 2008 found it 'difficult to predict' and merely agreed with Bennett and Raab that it is possible 'that at some point, and in some context, international data protection will be tested within the WTO',[10] noting Shaffer's conclusion[11] that it was unlikely that the EU's 'adequacy' requirements could be successfully challenged at the WTO.[12] Bygrave, however, considered that 'a fairly cogent argument can be made that the EU has breached the chapeau criteria by entering into the Safe Harbor agreement with the USA but without, it would seem, offering third countries (for

---

(APTA) - 1975; Central American Integration System (SICA) - 1993; Central European Free Trade Agreement (CEFTA) - 1992[1]; Commonwealth of Independent States Free Trade Area (CISFTA) - 2011; Common Market for Eastern and Southern Africa (COMESA) - 1994; G-3 Free Trade Agreement (G-3) - 1995; Greater Arab Free Trade Area (GAFTA) -1997; Dominican Republic–Central America Free Trade Agreement (DR-CAFTA) - 2004; European Economic Area (EEA; European Union–Norway–Iceland–Lichtenstein) - 1994; European Free Trade Association (EFTA) - 1960; Gulf Cooperation Council (GCC) - 1981; North American Free Trade Agreement (NAFTA) - 1994; Pacific Alliance - 2012; South Asia Free Trade Agreement (SAFTA) - 2004; Southern African Development Community (SADC) - 1980; Southern Common Market (MERCOSUR) - 1991; Trans-Pacific Strategic Economic Partnership (TPP) – 2005.

[7] See, for an incomplete list, *List of bilateral free trade agreements* (Wikipedia) <https://en.wikipedia.org/wiki/List_of_bilateral_free_trade_agreements>.

[8] GATS further requires in art. VI (1) that '[i]n sectors where specific commitments are undertaken, each Member shall ensure that all measures of general application affecting trade in services are administered in a reasonable, objective and impartial manner'. There is also a need to comply with art. II (1) of GATS, requiring that '[w]ith respect to any measure covered by this Agreement, each Member shall accord immediately and unconditionally to services and service suppliers of any other Member treatment no less favourable than that it accords to like services and service suppliers of any other country'.

[9] New Zealand Law Commission (NZLC), *Privacy Concepts and Issues: Review of the Law of Privacy, Stage One* (Wellington, New Zealand, 2008), para. 7.69.

[10] Colin Bennett and Charles Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (MIT Press, 2006), p. 111.

[11] G. Shaffer, 'Globalization and social protection: The impact of EU and international rules in the ratcheting up of US privacy standards' (2000) 25 *Yale Journal of International Law* pp. 1–88.

[12] Bennett and Raab, *The Governance of Privacy*, p. 111.

example, Australia) the same opportunity to negotiate such an agreement'.[13] Reyes is of similar view.

In a detailed assessment of the position of the EU privacy Directive in light of GATS, Reyes[14] concludes that, despite the apparent clarity of the GATS exception for privacy protection, 'the possibility that any given measure will withstand GATS exceptions analysis is unpredictable'. 'Unfortunately, the latitude given to the WTO DSB [Dispute Settlement Bodies] in interpreting the general exceptions may allow a challenge to the Privacy Directive to overcome the EU's reliance on GATS art XIV(c)(ii).' The *US–Gambling decision*[15] by the WTO Appellate Body in 2005 is the only one to yet consider Article art XIV(c) (although not a privacy exception), and it imposed a more stringent (and unpredictable) analysis of 'necessity' than privacy scholars had expected. Reyes concludes that, in relation to any proposed measure, an 'in-depth analysis of necessity and the chapeau must be undertaken', and that an initially compliant measure can also 'mutate into a WTO-inconsistent measure if the implementing agency fails to consider the effects of their chosen method of application'. Bygrave[16] and Weber[17] conclude similarly, that there is a degree of unpredictability of WTO jurisprudence, and thus of whether a challenge at the WTO against EU or national data export restrictions would succeed.

Despite statements by US officials that the EU's requirements in the EU privacy Directive are contrary to WTO commitments, neither the US nor any other country has yet challenged them in that forum. After two decades of GATS, perhaps a practical conclusion is that GATS is not a threat to all data export or data localisation restrictions, but that it could be (in light of the arguments raised by scholars) be used to challenge some ill-considered or over-broad restrictions.

Regional trade agreements – examples

Regional FTAs are not known to have had any significant effect on data privacy prior to 2016. Early agreements such as the North American Free Trade Agreement (NAFTA, 1994)[18] had no relevant clauses. Some regional Asia-Pacific agreements do include clauses but they do not go beyond GATS.

SAARC trade agreements

The only reference to privacy protection in the SAARC (South Asia Area of Regional Cooperation) agreements and conventions is in the SAARC Agreement on Trade in Services,[19] made in 2010. That agreement allows for exceptions to be made in the domestic laws of SAARC countries for measures for the protection of data privacy which might otherwise be contrary to its free trade requirements. Clause 23 is in all relevant respects the same as article XIV(c)(2) of the GATS, except that it only applies as between the SAARC countries. While this

---

[13] Lee Bygrave *Data Privacy Law: An International Perspective* (OUP, 2014), p.198. The Safe Harbor agreement is no longer functioning, following the *Schrems* decision, but the point is still valid.

[14] Carla Reyes '"WTO-Compliant Protection of Fundamental Rights: Lessons from the EU Privacy Directive" [2011] MelbJlIntLaw 5; (2011) 12(1) *Melbourne Journal of International Law* 141 <http://www.austlii.edu.au/au/journals/MelbJIL/2011/5.html>.

[15] Appellate Body Report, *US — Gambling*, WTO Doc WT/DS285/AB/R, [338]–[369].

[16] Bygrave, previous citation.

[17] Rolf Weber 'Regulatory Autonomy and Privacy Standards Under the GATS' *Asian Journal of WTO & International Health Law and Policy*, Vol. 7, No. 1, pp. 25-48, March 2012

[18] NAFTA Secretariat < https://www.nafta-sec-alena.org/Home/Welcome>

[19] SAARC Agreement on Trade in Services, 2010; see discussion on SAARC website at <http://www.saarc-sec.org/areaofcooperation/detail.php?activity_id=46>.

is essentially a negative measure, it is an important one, allowing SAARC member states to impose restrictions on data exports, and on outsourced data processing to other SAARC member states, in order to protect data privacy.

ASEAN trade agreements (ASEANFAS and AANZFTA)

The ASEAN (Association of South East Asian Nations) Framework Agreement on Services (1995) provides in effect[20] that the exemption for laws protecting data privacy in article XIV(c)(2) of the GATS also applies under the ASEAN Framework, in default of specific provisions, and that there is, therefore, no impediment to data export restrictions resulting from ASEAN agreements. The position is therefore essentially the same as in the SAARC region.

The Agreement Establishing the ASEAN-Australia-New Zealand Free Trade Area (AANZFTA),[21] signed in 2009, was Australia's first multi-country FTA. It is now in force for all parties.[22] In the chapter on electronic commerce, Art. 7[23] includes a very general obligation to 'protect the personal data of the users of electronic commerce' (but without any obligation until it enacts laws to do so), and in doing so to 'consider the international standards and criteria of relevant international organisations'. No provision deals explicitly with data export restrictions. AANZFTA includes an investor-state dispute resolution mechanism, but it does not apply to the e-commerce chapter.[24] AANZFTA therefore has little effect on data privacy laws.

The impact of multilateral FTAs on privacy prior to 2016

Regional FTAs, or bilateral FTAs, completed prior to 2016, have rarely included significant restrictions on the enactment of data privacy laws by countries parties to them. However, this matters less than it might, because most countries are parties to GATS.[25] Although the interpretation of the privacy-related provisions in GATS, particularly Article XIV(c)(ii), is still uncertain (despite being unchallenged for twenty years), we can say that GATS imposes on most countries a minimum level of restriction on enactment of data privacy laws, irrespective of other multilateral or bilateral agreements.

This position has potentially changed in late 2015 with the completion of the Trans-Pacific Partnership (TPP) Agreement, which if it comes into effect will impose what appear to be a higher level of restrictions on countries which are parties to it. Will it set a pattern for a higher

---

[20] *ASEAN Framework Agreement on Services* art. XIV(1) provides that '[t]he terms and definitions and other provisions of the [General Agreement on Tariffs and Trade] GATS shall be referred to and applied to matters arising under this Framework Agreement for which no specific provision has been made under it' and Article IX(1) provides that '[t]his Framework Agreement or any action taken under it shall not affect the rights and obligations of the Member States under any existing agreements to which they are parties'.

[21] DFAT Australia, AANZFTA page <http://dfat.gov.au/trade/agreements/aanzfta/Pages/asean-australia-new-zealand-free-trade-agreement.aspx >

[22] DFAT, AANZFTA Resources <http://dfat.gov.au/trade/agreements/aanzfta/resources/Pages/resources.aspx>

[23] AANZFTA Chapter 10, Article 7 'Online Data Protection' provides: ' 1. Subject to Paragraph 2, each Party shall, in a manner it considers appropriate, protect the personal data of the users of electronic commerce. 2. A Party shall not be obliged to apply Paragraph 1 before the date on which that Party enacts domestic laws or regulations to protect the personal data of electronic commerce users. 3. In the development of data protection standards, each Party shall consider the international standards and criteria of relevant international organisations.'

[24] AANZFTA, Chapter 10, Art. 10.

[25] All members of the WTO are signatories to the GATS, and the WTO had 162 members as of December 2015 <https://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm>.

level of restrictions than GATS in other FTAs still being negotiated? The TPP will now be discussed.

The Trans-Pacific Partnership (TPP) Agreement[26]

Twelve Pacific-rim nations accounting for 40 per cent 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)[27] was agreed to in Atlanta, Georgia on 5 October at the conclusion of eight years of negotiation, and signed in Auckland, New Zealand on 4 February 2016.[28]

The TPP is primarily an agreement 'to establish a free trade area',[29] an agreement which 'will strip thousands of trade tariffs in the region and set common labour, environmental and legal standards among signatories.'[30] 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: Nearly 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 Viet Nam. Five more APEC member countries have stated they wish to join the TPP: Indonesia, the second most populous country in APEC;[31] South Korea, the third-largest economy in East Asia;[32] as well as Taiwan;[33] Thailand, [34] the Philippines,[35] and even

---

[26] A shorter version of this section 'The TPP Agreement: An anti-privacy treaty for most of APEC' is in (2015) 138 *Privacy Laws & Business International Report*, December 2015

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

[28] Claire Reilly 'Pacific Grim: How the controversial TPP signed away your digital rights' C|Net, 4 February 2016 < http://www.cnet.com/au/news/pacific-grim-how-the-controversial-tpp-signed-away-your-digital-rights/>

[29] TPP, Article 1.1.

[30] 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>

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

[32] 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/>

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

[34] Kiyoshi Takenaka 'Thailand 'highly likely' to decide to join TPP: deputy prime minister' *bilaterals.org*, 27 November 2015 <http://www.bilaterals.org/?thailand-highly-likely-to-decide>

[35] 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/>

Papua New Guinea.[36] That leaves just five of the twenty-one APEC member economies not involved at present. Neither China nor the Hong Kong SAR, both APEC members, are parties to the TPP,[37] although significant opinion-makers in China are open to joining the TPP.[38] The other 'missing' APEC member economy is Russia. In effect, all of APEC wants to join TPP.

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.[39] 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. There are two methods by which the TPP may come into force. It can come into effect 60 days after the 12th ratification by the original signatories. Alternatively, if, after two years (ie about December 2017), all 12 signatories have not ratified the TPP, it may still come into force if at least 6 original signatories have ratified it, and between them they represent 85% of the total GDP of the 12 original signatories. Assessments indicate that requires ratification by both the USA and Japan.[40] Many politicians on both sides of US politics have expressed opposition to the TPP, and there is still some opposition in Japan. A report by World Bank staff estimates that the TPP will only boost the Australian economy by 0.7 percent by 2030,[41] making it difficult to regard the Australian government's fervent support anything more than ideological.

Provided they are willing to comply with its requirements, the TPP is open to accession by (a) any State or separate customs territory that is a member of APEC, and (b) such other State or separate customs territory as the Parties may agree (Article 30.4). TPP therefore has ambitions to be a global agreement.

Scope includes any measures affecting trade

Chapter 14 ('Electronic Commerce') applies to 'measures adopted or maintained by a Party that *affect* trade by electronic means' (Article 14.2.2, emphasis added), so the scope may be much broader than measures that govern or 'apply to' trade, and broader than the normal meaning of 'electronic commerce' (the Chapter title). The key terms 'trade by electronic means', and 'affecting' remain undefined, as does the less important 'e-commerce'.[42]

The wide scope of the TPP in relation to electronic services is confirmed by Article 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),'

---

[36] Saul Laob 'Papua New Guinea Leader Confident Country Able to Join TPP Deal' *Sputnik News*, 17 November 2015 <http://sputniknews.com/politics/20151117/1030233189/papua-new-guinea-leader-tpp-deal.html#ixzz3xZPzEEWd>

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

[38] 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>

[39] ibid

[40] Ankit Panda 'Here's What Needs to Happen in Order for the Trans-Pacific Partnership to Become Binding' *The Diplomat* 8 October 2015 <http://thediplomat.com/2015/10/heres-what-needs-to-happen-in-order-for-the-trans-pacific-partnership-to-become-binding/>

[41] Peter Martin 'Trans-Pacific Partnership will barely benefit Australia, says World Bank report' *Sydney Morning Herald*, 12 January 2016 <http://www.smh.com.au/federal-politics/-gm3g9w.html>.

[42] Burcu Kilic & Tamir 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>

However, Chapter 14 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 14.2.3). Although government owned or controlled enterprises may be subject to the TPP,[43] 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 (eg health data held by governments) is exempt from the TPP. In such cases, there is no need to consider the restrictions in Articles 14.11 and 14.13 (discussed below). Areas of uncertainty include whether State-owned enterprises (SEOs), regional and local governments etc are included as 'Parties'.[44]

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

Vague and unenforceable requirements for personal information protection

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',[45] (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 personal data need not be included unless it comes within 'electronic commerce', and even then might fall outside Article 14.2.2 discussed above. Because this Article is so weak and unimportant (as explained below), the lack of definition of 'electronic commerce' does not matter much.

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 USA's 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,[46] albeit a small one. 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

---

[43] 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.'

[44] Thanks to Sanya Reid Smith for pointing out these issues.

[45] 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'.

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

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. These content provisions are even weaker than the APEC Privacy Framework,[47] which is ridiculous given that TPP parties are also APEC member economies, and that the APEC Framework standards are very low.

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'. No standards for such 'interoperability' are provided, and this is likely to be, in effect, an anti-privacy provision which supports 'lowest common denominator' downward compatibility.

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.

The article also encourages countries to publicise how their legal frameworks operate.[48] Although increased transparency is valuable, this is probably another useless provision given that similar attempts via the APEC Privacy Framework have been largely ignored.[49]

All but two of the current parties to the TPP already have a 'legal framework' in force. Article 14.8 has a note that 'Brunei Darussalam and Viet Nam are not required to apply this Article before the date on which that Party implements its legal framework that provides for the protection of personal data of the users of electronic commerce'. There is no such exemption from immediate application of the two restrictions discussed below. Brunei does not at present have a data privacy law, only a self-regulatory scheme,[50] so it appears they intend to

---

[47] G. Greenleaf 'Five Years of the Apec Privacy Framework: Failure or Promise?' (2009) 25 *Computer Law & Security Report*, 28-43.

[48] Article 14.8.4 says 'Each Party should publish information on the personal information protections it provides to users of electronic commerce, including how: (a) individuals can pursue remedies; and (b) business can comply with any legal requirements.' The note to the Article also says that 'the Parties shall endeavour to exchange information on any such [compatibility] mechanisms applied in their jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility between them.'

[49] APEC 'Data Privacy Individual Action Plan' <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Data-Privacy-Individual-Action-Plan.aspx>; Only fourteen of 21 APEC economies have lodged such plans, of which only three (Singapore, Hong Kong and Mexico) have been updated since 2011.

[50] G. Greenleaf 'ASEAN data privacy developments 2014-15' (2015) 134 *Privacy Laws & Business International Report,* 9-12.

legislate. Vietnam already has extensive e-commerce legislation,[51] but this implies it intends to legislate further.

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 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 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.[52] It has been argued that 'it is likely this provision would be interpreted broadly by a dispute resolution body so as to include any and all elements of a service', and not restricted to outsourcing of internal services.[53]

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.'[54] While these requirements all have some lineage in other FTAs, they are presented here in a much stronger form.[55] What are stated here as conditions (ii) and (iii) that the party imposing a restriction has the onus to prove, are in GATS only found in the chapeau (introductory text), without such an onus arising. That requirements to prove that the restriction is 'to achieve a legitimate public policy objective', and is being achieved in the least burdensome way, can both be interpreted in different and unpredictable ways, imposing a difficult burden to discharge. 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',[56] particularly when coupled with ISDS provisions (as discussed below).

---

[51] Greenleaf *Asian Data Privacy Laws*, Chapter 13 'Vietnam and Indonesia: ASEAN's Sectoral Laws'; see also Greenleaf 'ASEAN data privacy developments 2014-15' for subsequent developments.

[52] 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'.

[53] Kilic and Israel, above.

[54] 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.''

[55] Kilic and Israel, above, make the points following.

[56] 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>

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. Aspects of this four-step-test are typical of conditions to allow exceptions in trade agreements, and do not at first sight appear to be extreme restrictions on data exports or localisation (at least not compared with what might have been included). However, the TPP versions are even more difficult tests than their WTO predecessors, and start from the assumption that any such restrictions are illegitimate. The weaker WTO versions have been shown to have been successfully satisfied (for all steps) in only one of 44 challenges, and attempts to satisfy the 'least burdensome way' test (described as a necessity test by the WTO Secretariat) fail in 75% of attempts.[57]

Prohibitions on data localisation

Post-Snowden, everyone knows, and the European Court of Justice has confirmed,[58] 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',[59] for this Article, only include those 'for commercial use', but whether that means exclusively or only primarily for such use is unclear.

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 condition for conducting business in that territory' (Article 14.13.2). In other words, data localisation is *prima facie* banned. Then, the same notoriously difficult to satisfy 'four step test' of justification for any exceptions is applied as was the case for data export limitations.[60]

Data localisation requirements in the laws of various Asian countries will have to meet the four step test or breach TPP. These include Vietnam and (if they wish to join TPP) Indonesia and China.[61] Russia's sweeping data localisation requirements would have little chance of passing these tests, if it became a TPP party. While even some large US companies are offering services which purport to be 'local clouds' (but this might be ineffective in the face of US law), such market practices are not directly relevant here: legal localisation requirements by state parties are the target.

---

[57] 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.>.

[58] *Schrems v. Data Protection Commissioner* (6 October 2015) Court of Justice of the European Union (Case C-362/14)

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

[60] 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. '

[61] In its draft Cyber-security Law and health data guidelines.

Dispute settlement

State parties to the TPP can use the dispute settlement provisions of Chapter 28 to resolve disputes concerning interpretation or application of the TPP, and whenever they consider that another party's 'actual or proposed measure' does not comply with its TPP obligations. If such disputes cannot be resolved by consultations between the parties, the complaining party can request establishment of a panel of three members to arbitrate the dispute (Articles 28.7-9). Other state parties can request to attend and make submissions (Article 28.13). The panel is to determine in a draft report whether the party's measures are inconsistent with the TPP, make recommendations, and give reasons (Article 28.16). After the parties have time to comment, it makes a final report (Article 28.17). If a party found to be in breach does not 'eliminate the non-conformity' in an agreed reasonable period of time, the other party may require negotiations for 'mutually acceptable compensation', failing which it may 'suspend benefits' under the TPP (ie institute trade counter-measures, such as raising tariffs) (Article 28.19). Complex procedures follow, beyond the scope of this article, but they can result in a panel awarding monetary assessments against a party, *in lieu* of the suspension of TPP benefits. These Chapter 28 procedures between states will apply to any disputes concerning the Electronic Commerce provisions of Chapter 14.

The spectre of ISDS

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 (Article 9.1 definition 'investor of a Party'). The essence of Chapter 9 is that a party must give investors from other Parties 'National Treatment' (ie treatment no less favourable than it accords its own investors) and 'Most-Favoured-Nation Treatment' (ie treatment no less favourable than it accords investors of any other state). In addition, it must accord such investments 'fair and equitable treatment and full protection and security' (Article 9.6.1). These provisions pose few problems for privacy protection.

The most significant investment protection relevant to data privacy is the prohibition of direct or indirect expropriation of investments,[62] 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.

There are some superficially appealing limits on the scope of Chapter 9. 'A determination that there has been a breach of another provision of this Agreement, or of a separate international agreement, does not establish that there has been a breach of this Article' (Article 9.6.3). Therefore, 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 in, say, the USA.

However, what if the main benefit to a company in the USA in setting up e-commerce facilities in another country A was the transfer of personal data to the USA where data privacy laws posed far less interference in what could be done with the data than under the laws of country A? Could breaches of the data export limitation or data localisation provisions then constitute an indirect expropriation of the investment (allowing reliance on Article 9.7.1)? The ISDS possibilities should frighten every country that has a data privacy law but has a smaller litigation budget than Google or Facebook.

---

[62] 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) …'

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.

Some scholars argue that concerns about ISDS are exaggerated, and that 'regulatory chill' is not borne out in at least one study,[63] but this is disputed in numerous studies recognizing such effects.[64] Also, privacy protection usually has few friends in government, and regulatory chill can easily turn to pneumonia.

Conclusions: A Faustian bargain

These TPP requirements seem to embody the type of binding international privacy treaty that the USA (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, both involving uncertain outcomes from dubious tribunals[65] and potentially very large damages claims. This approach is consistent with the 2013 revisions to the OECD privacy Guidelines,[66] but with much sharper teeth.

For the USA, 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[67]), because it will now be more difficult to prevent most personal data from being exported to the USA, 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 USA 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.

Treaties are always bargains. International privacy agreements since the 1980 OECD Guidelines and the 1981 Council of Europe Convention 108 have always sought guaranteed and consistent free flow of personal data (with trade benefits) in return for a required international minimum standard of privacy protection. In comparison, 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

---

[63] See Nottage and Trakman, above, for discussion.

[64] See numerous studies cited by Sanya Reid Smith, cited earlier, section 'Chilling Effects; Jess Hill 'ISDS: The devil in the trade deal', *Background Briefing* (transcript), ABC Radio National, 14 September 2014 <http://www.abc.net.au/radionational/programs/backgroundbriefing/isds-the-devil-in-the-trade-deal/5734490>.

[65] Hill, above.

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

[67] 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.

agreements, where their inclusion requires that states decide what their protection is worth compared with greater access to trade in bananas.

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, and some privacy experts are not overly concerned. But should this risk be taken?

The TPP is the first multilateral trade agreement with detailed provisions relating to privacy protection that go beyond the GATS provisions. 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.

FTAs in progress

It may be years before we know whether the TPP will 'fall over' and never come into effect. In the meantime, free trade agreements are proliferating, and overlapping in confusing ways. Although details are only known intermittently of their content, because of the secrecy in which negotiations are usually cloaked, there are some exceptions. Speculation is possible on whether they might follow or go further than the TPP in their treatment of privacy issues, or might allow privacy to be treated as a right to be protected. Where the USA is a party, we can assume with confidence that its negotiating position will be at least as strong as the TPP result.

There are a very large number and variety of multilateral FTAs concerning services (and therefore relevant to data privacy) which are currently being negotiated, mainly at the regional level, but effectively global in the case of TISA. One admittedly incomplete list has 24 proposed multilateral agreements.[68] Since the possible texts of most of these agreements are unknown, it would be pointless to attempt cover all of them here. Some of the more important, particularly those of which the likely terms are known, are discussed.

Transatlantic Trade and Investment Partnership (TTIP) – The EU/USA FTA

The EU is negotiating what it describes as 'a trade and investment deal with the US', the Transatlantic Trade and Investment Partnership (TTIP).[69] Unlike most other FTAs, the EU's position in the negotiations is disclosed,[70] following disquiet with secret negotiations.[71]

---

[68] List of multilateral free trade agreements - Proposed agreements (Wikipedia) <https://en.wikipedia.org/wiki/List_of_multilateral_free_trade_agreements>: Commonwealth of Independent States Free Trade Agreement (CISFTA); Union of South American Nations (USAN); 2021 Pacific Island Countries Trade Agreement (PICTA); African Free Trade Zone (AFTZ) between SADC, EAC and COMESA; Arab Maghreb Union (UMA); Asia-Pacific Economic Cooperation (APEC); Association of Caribbean States (ACS); Bolivarian Alternative for the Americas (ALBA); Bay of Bengal Initiative for MultiSectoral Technical and Economic Cooperation (BIMSTEC); Community of Sahel-Saharan States (CEN-SAD); Economic Community of West African States (ECOWAS); Euro-Mediterranean free trade area (EU-MEFTA); Economic Community of Central African States (ECCAS); Free Trade Area of the Americas (FTAA); Free Trade Area of the Asia Pacific (FTAAP); GUAM Organization for Democracy and Economic Development (GUAM); Intergovernmental Authority on Development (IGAD); Pacific Agreement on Closer Economic Relations (PACER and PACER Plus); People's Trade Treaty of Bolivarian Alternative for the Americas (ALBA); Regional Comprehensive Economic Partnership (RCEP) (ASEAN plus 6); Shanghai Cooperation Organisation (SCO); Transatlantic Free Trade Area (TAFTA); Tripartite Free Trade Area (T-FTA); China–Japan–South Korea Free Trade Agreement.

[69] EU Commission's TTIP pages http://ec.europa.eu/trade/policy/in-focus/ttip/documents-and-events/index_en.htm

Although the final decisions are made by the States of the EU and the European Parliament, the European Commission can 'negotiate' with the USA concerning data protection provisions in the TTIP. However, it can only do so within the parameters of, and according to the procedures of, Article 25 of the EU data protection Directive, as interpreted in *Schrems*. The Council of the EU confirmed in December 2015 that the Commission cannot negotiate away privacy rights in trade agreements: 'The Council stresses the need to create a global level playing field in the area of digital trade and strongly supports the Commission's intention to pursue this goal *in full compliance with and without prejudice to the EU's data protection and data privacy rules, which are not negotiated in or affected by trade agreements*'[72] (emphasis added).

The EU's negotiation position in relation to Trade in Services, Investment and E-commerce[73] includes in Chapter V "Regulatory Framework), Article 5 - 33 'Data processing', which is limited in its scope to the supply of financial services. These provisions are of little assistance to privacy protection. Article 33(2) requires 'appropriate safeguards for the protection of privacy … in particular with regard to the transfer of personal data ', but does not even require legislation to protect privacy, let alone set any standard.[74] Article 33(1), on the other hand, is an unrestricted requirement to allow transfer of personal data necessary for financial services supply,[75] and any privacy protections must come from the exceptions provisions.

The significant provision for protection of data privacy laws is Article 7-1 'General exceptions'[76] which attempts to exempt measures for 'the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts'. This exception is subject to three similar qualifications as those found in GATS, namely that the measures must be necessary, and two requirements in the chapeau to Article 7-1, that they must not constitute 'arbitrary or unjustifiable discrimination between countries where like conditions prevail'

---

[70] The EU's position in the negotiations <http://ec.europa.eu/trade/policy/in-focus/ttip/documents-and-events/index_en.htm#eu-position>

[71] Decision of the European Ombudsman closing the inquiry into complaint 119/2015/PHP on the European Commission's handling of a request for public access to documents related to TTIP http://www.ombudsman.europa.eu/en/cases/decision.faces/en/61261/html.bookmark

[72] Council of the European Union *3430th Council meeting OUTCOME OF THE COUNCIL MEETING Brussels, 27 November 2015* December 2015 <http://www.consilium.europa.eu/en/meetings/fac/2015/11/st14688_en15_pdf/>

[73] *The European Union's proposal for services, investment and e-commerce text*, tabled 31 July 2015 <http://trade.ec.europa.eu/doclib/docs/2015/july/tradoc_153669.pdf>.

[74] 2. Each Party shall adopt appropriate safeguards for the protection of privacy and fundamental rights, and freedom of individuals, in particular with regard to the transfer of personal data.

[75] 1. Each Party shall permit a financial service supplier of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is necessary in the ordinary course of business of such financial service supplier.

[76] 1. Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on establishment of enterprises, the operation of investments or cross-border supply of services, nothing in Chapter II Section 1, Chapter III, Chapter IV, Chapter V and Chapter VI shall be construed to prevent the adoption or enforcement by any Party of measures:
(a) necessary to protect public security or public morals or to maintain public order;
(b) necessary to protect human, animal or plant life or health; …
(e) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Title including those relating to: …

(ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;

and must not be 'a disguised restriction on establishment of enterprises, the operation of investments or cross-border supply of services'.

Of course, this is only the EU negotiating position, not the final result. The EU already has some track record in refusing to negotiate away privacy rights in FTAs, when it declined in 2013 to grant what India called 'data secure status' (ie recognition of completely inadequate laws as being adequate) as part of a proposed EU-India FTA.[77] That FTA has not yet been completed.[78]

Depending on what the EU negotiates, this may have even more direct benefits for some other countries because of 'side letters' to the TPP. For example, such a 'side letter' between Australia and the USA provides that 'Should the Government of the United States of America undertake any relevant additional commitments to those in the TPP Agreement with respect to the treatment of personal information of foreign nationals in another free trade agreement, it shall extend any such commitments to Australia.'[79] According to Michael Geist, Canada did not obtain such a TPP concession from the US.[80] The TPP and other multilateral FTAs do not create 'level playing fields' for trade: they are more like minefields, depending on the country's 'on the side' bargaining position with other countries.

Trade in Services Agreement (TISA)

One third of WTO members are now involved ('50 countries and 68.2% of world trade in services') in the Trade in Services Agreement (TISA) negotiations, as this could not be included in the DOHA round. The main proponents are the USA and the EU, but Australia is one of three leading countries. Negotiations started in 2013.

A draft of the Financial Services Annex of TISA dated 14 April 2014 was released by Wikileaks (June 2014).[81] 'would allow uninhibited exchange of personal and financial data' (Wikileaks). The only clause included which had significant implications for privacy was Article X.11, for which the US proposal was: 'Each Party shall allow a financial service supplier of another Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the financial service supplier's ordinary course of business.' This blunt 'shall allow' (anything required in the ordinary course of business), with no exceptions stated, would prevent any party from restricting any flows of personal data that could possibly be of value in commerce – in other words, all personal data. As news reports stated, 'The changes could see Australians' bank accounts and financial data freely transferred overseas' (SMH).

The EU proposal, however, stated: 'No Party shall take measures that prevent transfers of information or the processing of financial information, including transfers of data by electronic means, into and out of its territory, for data processing or that, subject to importation rules consistent with international agreements, prevent transfers of equipment,

---

[77] Greenleaf *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (OUP, 2014), pp. 432-33.

[78] EU-India <http://ec.europa.eu/trade/policy/countries-and-regions/countries/india/>

[79] US-Australia side letter, undated <https://ustr.gov/sites/default/files/TPP-Final-Text-US-AU-Letter-Exchange-on-Privacy.pdf>

[80] Michael Geist 'The Trouble with the TPP, Day 14: No U.S. Assurances for Canada on Privacy' michaelgeist.ca Blog, 21 January 2016 <http://www.michaelgeist.ca/2016/01/the-trouble-with-the-tpp-day-14-no-u-s-assurances-for-canada-on-privacy/>

[81] (Draft) Trade in Services Agreement (TISA) Financial Services Annex ,14 April 2014 <https://wikileaks.org/tisa-financial/>

where such transfers of information, processing of financial information or transfers of equipment are necessary for the conduct of the ordinary business of a financial service supplier. *Nothing in this paragraph restricts the right of a Party to protect personal data, personal privacy and the confidentiality of individual records and accounts so long as such right is not used to circumvent the provisions of this Agreement*.' The final sentence (italicized) is diametrically opposed to the US position.

Kelsey and Kulic subsequently obtained and analysed the US government proposal put forward in the April negotiations.[82] It was even more anti-privacy than the draft text leaked in June. They interpret the US position as including (i) banning any restrictions on data transfers (X.4), including those allowed by GATS (as is the case in the leaked draft); (ii) banning any 'local presence' requirements (X.1); and (iii) banning all data localisation requirements (X.4). The exceptions provisions (X.7) do no include exceptions for privacy protection.

The leaked TISA draft includes only (i) of these three aims, whereas the TPP agreement includes both (i) and (iii), but both with exceptions provisions (albeit, ones very difficult to satisfy). The TPP therefore seems to be the high-water-mark of US negotiating success concerning privacy as yet, but not the limit of its negotiating ambitions.

However, the USA is not a party to every multilateral FTA being negotiated at present.

Regional Comprehensive Economic Partnership (RCEP)

If the TPP falls over, China is advocating an alternative, the Regional Comprehensive Economic Partnership (RCEP). RCEP is an ASEAN-centred FTA, intended to comprise the ten countries of ASEAN (Association of Southeast Asian Nations) plus the six others with which ASEAN already has FTAs (China, India, Japan, South Korea, Australia and New Zealand) – but not the USA. Negotiations started in 2012, on the overall structure ('modality'), but in 2015 becoming more concrete about market access in particular 'disciplines'. The leaders of the countries concerned had agreed on an end-2015 deadline, but this was too ambitious.[83]

Will ASEAN, China and India offer a better trade deal than the TTP, so far as privacy is concerned? No one knows, because it is still the subject of secret negotiations. No content details are yet known.

Pacific Agreement on Closer Economic Relations (PACER) Plus

PACER includes most Pacific Island countries and PNG, plus New Zealand and Australia. It originated in the Pacific Islands Forum in 2011, with negotiations starting in 2012. Australia states that its objective is to foster greater regional integration, stability and economic growth and to assist Aust business interests. It expects trade-in-services benefits, and investment benefits. Services account for 65% of all economic activity in Pacific Island countries.[84] No drafts are available, and whether it covers privacy issues is unknown. No Pacific Island countries nor PNG have data privacy laws.[85]

---

[82] Prof Jane Kelsey (University of Auckland) and Dr Burcu Kilic (Public Citizen, Washington) *Briefing on US TISA Proposal on E-Commerce, Technology Transfer, Cross-border Data Flows and Net Neutrality*, 17 December 2014 <http://www.world-psi.org/en/briefing-us-tisa-proposal-e-commerce-technology-transfer-cross-border-data-flows-and-net-neutrality>

[83] Notes – Australia Department of Foreign Affairs and Trade, *Trade in Services Negotiations briefing* 11 March 2015, Sydney.

[84] Notes – Australia Department of Foreign Affairs and Trade, *Trade in Services Negotiations briefing* 11 March 2015, Sydney.

[85] Vanuatu has provision for rules to be made in its e-commerce law.

Multilateral FTAs in other regions

One of the main features of current FTA developments is the attempt to merge the effects of existing FTAs into larger regional agreements. In Latin America, progress on regional FTAs (aside from the TPP) is occurring at the sub-regional level, but is not known to affect data privacy. Plans for comprehensive FTAs in the Americas as a whole have stalled.[86] The Pacific Alliance[87] (Chile, Colombia, Mexico and Peru, with Costa Rica in progress, and other observers) has followed up its 2012 Framework Agreement with an Additional Protocol defining the terms of free trade within the bloc in 2015,[88] and most of national implementation procedures are well underway and may be completed by early 2016.[89] Mercosur has as full members Argentina, Brazil, Paraguay, Uruguay and Venezuela, plus associate members and observers.[90] It is attempting to negotiate FTAs with other trade blocs such as the EU and the Pacific Alliance. Whether similar developments are occurring in Africa and other regions has not been assessed.

Concerning APEC, it is reported that 'There is even more to come. The TPP is a stepping stone to an even bigger Asian Pacific trade agreement among all 21 members of APEC, and in particular China. It is now under active consideration in APEC.'[91] We know what to expect some countries will aim for in the privacy clauses from that agreement (more TPP), but not whether China will agree. Other possible agreements may take a different path, and the differences may be significant.

Conclusions: Future FTAs and global privacy laws

Free Trade Agreements have not yet had a major effect on the development or implementation of data privacy laws, but that could change. The untested Article XIV(c)(ii) of the GATS is will remain the global base-line for the relationship between free trade and data privacy, but its meaning is uncertain. The best-case scenario for data privacy is that the EU holds to that GATS position in the TTIP negotiations (and in its other FTA negotiations), that the TPP falls over, and that data privacy laws are not successfully challenged at the WTO (continuing the position of the last 20 years). Other agreements such as RCEP may than take the same approach. The worst-case scenario for data privacy is that the TPP comes into force quickly, that other TPAs (possibly including RCEP) emulate it since so many of their parties are also TPP parties, and that challenges to privacy laws start to emerge from the WTO or under these stronger agreements. One way or another, FTAs are likely to be one of the defining factors in the future evolution of data privacy laws.

---

[86] See for example Free Trade Area of the Americas (Wikipedia) <https://en.wikipedia.org/wiki/Free_Trade_Area_of_the_Americas>.

[87] Pacific Alliance website <https://alianzapacifico.net/en/>; Pacific Alliance Blog < http://pacificallianceblog.com/>; Pacific Alliance (Wikipedia) <https://en.wikipedia.org/wiki/Pacific_Alliance>

[88] 'Pacific Alliance Trade Pact Enters into Force' DataMyne Blog, 20 July 2015 <http://www.datamyne.com/blog/markets/pacific-alliance-trade-pact-enters-into-force/

[89] Pacific Alliance Blog <http://pacificallianceblog.com/>.

[90] Mercosur (Wikipedia) <https://en.wikipedia.org/wiki/Mercosur>

[91] Alan Oxley 'TPP trade deal is just the beginning, APEC and China are next' *Australian Financial Review*, 6 October 2015 <http://www.afr.com/opinion/tpp-trade-deal-is-just-the-beginning-apec-and-china-are-next-20151006-gk24mn#ixzz3ruzhIRpr>