The Role of the Trans-Pacific Partnership Agreement in the Internet Ecosystem: Uneasy Liaison or Synergistic Alliance?

Neha Mishra*

JOURNAL OF INTERNATIONAL ECONOMIC LAW (FORTHCOMING)

Abstract:

The Trans-Pacific Partnership Agreement ('TPP') is the first trade agreement that comprehensively deals with contemporary policy issues in digital trade. It introduces new disciplines on issues such as cross-border data flows, online privacy, network neutrality, cybersecurity, regulation of spam, and safe harbour protection for internet intermediaries. These provisions are atypical of trade agreements, and are particularly significant as they have a direct impact on internet policy. In this article, I evaluate these new disciplines in the TPP to assess the extent to which the TPP is suitably placed in the internet eco-system. After a comprehensive legal assessment of these disciplines, I argue that the TPP does not effectively fit into the broader internet ecosystem, as it fails to synergize the goal of trade liberalization with important internet policy concerns such as facilitating consumer trust and digital innovation. However, despite its deficiencies, the TPP sets a new benchmark for rules on digital trade, as its provisions address several contemporary issues in the digital economy. Therefore, the provisions on digital trade within the TPP will be instrumental in future negotiations at the World Trade Organization ('WTO') and other regional bodies. More importantly, the TPP is a reminder of the increasing significance of trade agreements in influencing critical aspects of internet policy. Particularly, in developing rules on digital trade that affect issues such as cross-border data flows, online privacy and consumer protection, net neutrality and cybersecurity, trade negotiators/lawyers need to comprehensively assess the relevance of these rules in the liberalization of digital trade, and its broader impact on the internet ecosystem.

* PhD Candidate, Melbourne Law School; MPP (NUS), LLM (LSE), B.A. LL.B. Hons (NLSIU); Email: nmishra@student.unimelb.edu.au. I gratefully acknowledge the support of the Australian Government Research Training Program Scholarship. I thank Tania Voon, Andrew Mitchell, the editors of Journal of International Economic Law and two anonymous reviewers for their very helpful comments and insights on earlier drafts of the article. All errors and omissions in this article are my own.

I INTRODUCTION

The *Trans-Pacific Partnership Agreement* ('TPP'),[1] touted as the 'gold standard'[2] for '21st century agreements',[3] is arguably the most comprehensive trade agreement to date with regard to digital trade, both in terms of depth and breadth of covered issues. In this article, 'digital trade' is understood broadly and refers to the 'full range of cross-border electronic commerce issues, from online commercial transactions to the ancillary aspects of protection of intellectual property rights, privacy, and the protection of national interests'.[4] The TPP contains several new provisions relating to digital trade on issues such as cross-border data flows, online privacy, cybersecurity, trade secrets and network neutrality, which were typically absent in previous trade agreements.[5] These new disciplines are controversial as they directly or indirectly influence critical aspects of internet policy, an area in which trade experts/negotiators do not possess any specific expertise. While certain scholars[6] and tech giants such as Google have come out in strong support of the TPP,[7] many civil society bodies have expressed concerns regarding the brazen manner in which

[1] *Trans Pacific Partnership Agreement*, text released following legal review 26 January 2016 (signed 4 February 2016, not yet in force) ('TPP').

[2] Referring to the use of the phrase 'gold standard', see Hillary Rodham Clinton, 'Remarks at Techport Australia', Speech delivered at Techport Australia, Adelaide (15 November 2012). However, in the 2016 US Presidential elections both presidential candidates, Hillary Clinton and Donald Trump (the elected President), took a stance against the TPP. See Nick Timiraos and Richard Rubin, 'Debate Cheat Sheet: Donald Trump and Hillary Clinton on the Economy', *The Wall Street Journal*, 26 September 2016, http://blogs.wsj.com (visited 21 December 2016).

[3] United States Trade Representative ('USTR'), 'Trans-Pacific Partnership (TPP): Unlocking Opportunity for Americans through trade with the Asia Pacific', https://ustr.gov (visited 20 September 2016).

[4] See Lee Branstetter, 'TPP and Digital Trade' in Jeffrey J Schott and Cathleen Cimino-Isaac (eds), *Assessing the Trans-Pacific Partnership Vol-2: Innovations in Trading Rules* (Peterson Institute for International Economics, PIIE Briefing 16-4, March 2016) 72-81, at 72. This broad definition of 'digital trade' also aligns with the definition of electronic commerce in the World Trade Organization's ('WTO') Work Programme on Electronic Commerce. See General Council, *Work Programme on Electronic Commerce*, adopted 25 September 1998, WT/L/274 (30 September 1998)), para 1.3.

[5] For eg, the language of the TPP Electronic Commerce Chapter does not significantly overlap with the language of previous US FTAs – a textual analysis by Allee and Lugg found a 27% similarity between the Electronic Commerce Chapter of the TPP and previous UF Free Trade Agreements ('FTAs'). See Todd Allee and Andrew Lugg, 'Who Wrote the Rules for the Trans-Pacific Partnership?' (July-September) Research and Politics 1(2016), at 4-5. However, the *Free Trade Agreement between the United States of America and the Republic of Korea* ('KORUS FTA') can be considered to be an important precursor to the TPP, as it contained non-binding provision on cross-border data flows and provisions on access and use of the internet for e-commerce. See *Free Trade Agreement between the United States of Amercia and the Republic of Korea*, signed 30 June 2007 (entered into force 15 March 2012) ('KORUS FTA') art 15.7, art 15.8.

[6] See, eg, Joshua P Meltzer, 'The Trans-Pacific Partnership is a Win for All Parties', *Future Development*, 9 December 2015, http://brookings.edu (visited 20 September 2016).

[7] Kent Walker, 'The Trans-Pacific Partnership: A Step Forward for the Internet', 10 June 2016, https://blog.google/topics/public-policy (visited 20 September 2016). See also Michaela Ross, 'Tech Sector Urges Congressional Leaders to Ratify TPP', *International Trade Daily* (15 September 2016); Letter from Allied for Startups et al to Speaker Ryan, Leaders McConnell, Pelosi and Reid (13 September 2016); Alexis Kramer, 'TPP Debate Includes Split on Data Provisions', *Electronic Commerce & Law Report* (17 August 2016). However, within the tech industry, certain companies raised objections regarding the TPP, namely 'threat to fair use', 'expensive and harmful costs of online enforcement [of intellectual property ('IP')]' and 'criminalizing journalism and whistleblowing'. See Letter from Industry Coalition to Members of Congress, 20 May 2015, https://www.eff.org (visited 20 September 2016).

the TPP sidelines important policy goals of the internet community.[8] However, in order to arrive at a conclusive finding regarding the impact of the TPP on the internet ecosystem, it is important to assess the legal ramifications of these provisions, particularly since these provisions are mostly new to trade agreements.

The provisions on digital trade in the TPP were largely influenced by United State Trade Representative's ('USTR') agenda on digital trade.[9] The issues placed by the USTR on the TPP negotiating agenda primarily reflect concerns that American companies had been facing in foreign markets such as forced disclosure of source code and encryption keys in China,[10] regulation of over-the-top services in Vietnam,[11] restrictions on cross-border movement of data in several countries,[12] development of local/regional cloud networks in Europe,[13] and blocking of various internet services in Turkey and China.[14] The proactive and predominant role of the United States ('US') in the TPP negotiations was not surprising since the US is the global leader in digital products and services, and the Asia-Pacific region is the fastest growing e-commerce market in the world (and hence, an extremely attractive market for American tech companies).[15] Further, with the decline of the relevance of the WTO for promoting rapid trade liberalization, the TPP emerged as a viable alternative.[16] Ironically, inspite of the predominant influence of the US in the negotiation of the TPP, the next US President, Donald Trump, has expressed strong disapproval of the TPP (although his disapproval was largely unrelated to digital trade issues),[17] and threatened

[8] See, eg, Steve Anderson and David Christopher, 'The Secretive Deal That Could Undermine Our Democratic Rights and Change How We Use the Internet Forever' 21 CCPA Monitor 17 (2014); Timothy Vollmer, 'Trans Pacific Partnership Would Harm User Rights and the Commons', *Creative Commons Blog*, 16 November 2015, https://blog.creativecommons.org (visited 20 November 2016); Electronic Frontier Foundation, 'Prominent Academics Respond to the TPP', 30 August 2012, https://www.eff.org (visited 20 November 2016). See also Internet Governance Forum, 'Trans-Pacific Partnership: Good or Bad for the Internet?', Workshop no 60, 8 December 2016, https://www.youtube.com/watch?v=pCGknvL5OBs (last visited 15 December 2016).

[9] USTR, 'TPP: Summary of US Objectives', https://ustr.gov (last visited 20 September 2016).

[10] USTR, '2015 Special 301 Report', April 2015, https://ustr.gov (visited 20 September 2016) 23.

[11] USTR, '2015 Section 1377 Review', March 2015, https://ustr.gov (visited 20 September 2016) 8, 9.

[12] USTR, 'Fact Sheet: Key Barriers to Digital Trade', Press Release, March 2016, https://ustr.gov (visited 20 September 2016).

[13] USTR, 'USTR Targets Telecommunications Barriers', Press Release, April 2014, https://ustr.gov (visited 20 September 2016)..

[14] USTR, 'USTR Targets Telecommunications Barriers', Press Release, April 2014, https://ustr.gov (visited 20 September 2016) ; USTR, 'The 2016 National Trade Estimate Report', 23 May 2016, https://ustr.gov (visited 20 September 2016) 91.

[15] James Crisp, 'Asia-Pacific outstrips Europe as world's largest e-commerce market',18 June 2014, *Euractiv*, https://www.euractiv.com (visited 20 September 2016); Ecommerce Europe, 'With a turnover of 567.3 billion, Asia-Pacific is the largest e-commerce market in the world', 10 February 2015, http://www.ecommerce-europe.eu (visited 20 September 2016). For understanding economic opportunities in the Asia-Pacific region, including e-commerce, see Fraser Thompson et al, *No Ordinary Disruption: The Forces Reshaping Asia*, Special Report for the Singapore 2015 Summit (McKinsey Global Institute, 2015).

[16] Allee and Lugg, above n 5, 1, 8.

[17] For Trump's position on technology issues, see generally Information Technology and Information Foundation, 'President-Elect Trump's Positions on Technology and Innovation Policy', November 2016, http://www2.itif.org (visited 20 December 2016) 1, 9-11.

to withdraw from the TPP, on the first day of office.[18] This may effectively result in the demise of the TPP, at least in its current shape and form, as the TPP will need to be ratified either by all the 12 signatory countries[19] or by 'at least six of the original signatories, which together account for at least 85 per cent of the combined gross domestic product of the original signatories in 2013' in order to come into force.[20] The latter condition effectively implies that both the US and Japan must ratify for the TPP to come into force.[21]

Despite the political uncertainty clouding the implementation of the TPP, a study of the provisions on digital trade in the TPP is both timely and meaningful. Firstly, given the scope and depth of issues covered under the TPP, it is likely to remain a benchmark for trade agreements in the near future.[22] For instance, the Australian government in its recent amendment of the *Singapore – Australia Free Trade Agreement*[23] introduced provisions on electronic commerce identical to TPP Chapter 14.[24] Further, in the ongoing trade negotiations such as the *Transatlantic Trade and Investment Partnership* ('TTIP')[25] and *Trade in Services Agreement* ('TISA')[26] countries have recommended or are likely to recommend provisions on digital trade similar to the TPP rules. However, the disagreement between the European Union ('EU') and the US on issues of data transfer and privacy, may lead to different outcomes in these FTAs.[27] Even in the *Regional Comprehensive Economic Partnership* ('RCEP'), which is currently under negotiation amongst 16 countries in the Asia-Pacific region, including China, the negotiating parties are considering provisions related to cross-border data flows, online personal data protection, spam, etc.[28] At the

[18] Nicky Woolf et al, 'Trump to Withdraw from Trans-Pacific Partnership on First Day in Office', 22 November 2016, The *Guardian*, https://www.theguardian.com (visited 20 December 2016).
[19] TPP art 30.5.1.
[20] TPP art 30.5.2.
[21] The Japanese Parliament recently ratified the TPP, despite the low chances of ratification of the TPP by the US. See Len Bracken, 'Japan Ratifies Trans-Pacific Partnership Pact', *International Trade Daily* (12 December 2016).
[22] Amitendu Palit, 'A Stalled TPP Means Bad News for Liberalisation', *The Telegraph*, 21 September 2016, http://www.telegraph.co.uk (visited 20 December 2016).
[23] *Singapore – Australia Free Trade Agreement*, signed 17 February 2003 (entered into force 28 July 2003) ('SAFTA').
[24] *Agreement to Amend the Singapore – Australia Free Trade Agreement* (signed 13 October 2016), Chapter 14 ('Amendment to SAFTA')
[25] Greenpeace Netherlands, TTIP Consolidated Proposed Electronic Communications/Telecommunications Text https://www.ttip-leaks.org (visited 20 December 2016).
[26] Wikileaks, 'TISA Annex on Electronic Commerce', May 2016, https://wikileaks.org/tisa (visited 20 December 2016). See also Wikileaks, 'TISA Localization Provisions', June 2016, https://wikileaks.org/tisa (visited 20 December 2016).
[27] See for eg, TTIP, art X.10.3.
[28] RCEP Working Group on Electronic Commerce, 'Terms of Reference', February 2015, http://www.bilaterals.org (visited 20 December 2016).

WTO, different countries, including the EU,[29] the US[30] and China[31] have shown willingness to advance discussions on issues related to electronic commerce at the next WTO Ministerial Conference.

Secondly, member countries have already started amending their domestic laws to be in compliance with TPP rules on digital trade, even before the TPP has come into force.[32] As a result, even if the TPP fails, these countries are likely to support provisions that are aligned with the existing provisions of the TPP. Finally, even if the US decides to withdraw from the TPP and take the route of bilateral negotiations, or renegotiate the TPP, under the Trump administration, many of the existing rules on digital trade in the TPP are likely to be re-proposed as they largely reflect the interests of the American digital industry.[33] Despite the unclear position of Trump on digital trade issues to date,[34] it appears unlikely that even under the Trump administration, the US government would take a position radically different from that of TPP in future negotiations, given the commercial interests of the American digital industry, particularly in relation to free data flows.

In this article, I evaluate whether the TPP strikes an appropriate balance between liberalizing digital trade and protecting important regulatory goals with respect to the internet, and whether the disciplines on the new-age digital trade issues covered under the TPP fit appropriately into the larger internet ecosystem. Section II discusses the new disciplines on digital trade in the TPP, focusing on data flows and data localization, privacy, cybersecurity, net neutrality and safe harbours for online intermediaries, and how these rules fit into the larger internet ecosystem. With respect to intellectual property ('IP') related issues, this article addresses rules regarding safe harbours for online intermediaries, in so far as it relates to the issue of data flows and privacy,[35] but does not deal with other issues such as the balance between fair use and protecting commercial interests of innovators, appropriate term for enforcement of online copyright etc, which has been

[29] Communication from Canada, Chile, Colombia, Côte d'Ivoire, the European Union, the Republic of Korea, Mexico, Paraguay and Singapore, *Work Programme on Electronic Commerce – Trade Policy, the WTO and the Digital Economy*, WTO Doc JOB/GC/97/Rev.1 (22 July 2016). See also See also Non-paper from Brazil, *Work Programme on Electronic Commerce* WTO Doc JOB/GC/98 (20 July 2016).

[30] Non-paper from the United States, *Work Programme on Electronic Commerce*, WTO Doc JOB/GC/94 (1 July 2016).

[31] Communication from the People's Republic of China, *Work Programme on Electronic Commerce: Aiming at the 11th Ministerial Conference*, WTO Doc JOB/GC/110, JOB/CTG/2 JOB/SERV/243, JOB/DEV/39 (4 November 2016).

[32] See for eg, Section IIB (privacy), Section IIC4 (trade in encrypted products) and Section IIC3(trade secrets).

[33] In relation to digital trade, during his election campaign, Trump advocated for weakening of encryption standards for purposes of surveillance by the US Government, and opposed net neutrality rules. On other digital trade issues related to data flows, innovation in digital services, and online consumer protection and data protection, Trump's position has remained unclear to date. Other aspects of his campaign also focused on user rights, such as maintaining an online database of Muslim immigrants, which may potentially raise privacy concerns. See Cindy Cohn and Karen Gullo, 'EFF to Tech Leaders: Stand with Users and Tell Trump We Need Strong Encryption, Internet Freedom', 13 December 2016, https://www.eff.org (visited 20 December 2016); Information Technology and Information Foundation, above n 17, 10-11.

[34] Ibid.

[35] See also, brief discussion on trade secrets in Section IIC3.

discussed extensively elsewhere.[36] Section III provides a broad overview of why misfits occur between trade agreements and the internet eco-system, and identifies important considerations for creating a better balance in trade agreements.

The article concludes that the trade liberalization provisions in the TPP are in an 'uneasy liaison' rather than in a 'synergistic alliance' with the ecosystem of the internet economy. This is because the TPP fails to adequately synergize the liberalization of digital trade with other critical issues related to consumer trust and digital innovation. However, the TPP cannot be conclusively dismissed as a failure; compared to past FTAs, the TPP has taken a bold first step in addressing delicate issues of the modern internet economy driven by technologies such as Big Data, cloud computing and Internet of Things, and created an important platform for trade lawyers to closely think about inter-linkages between trade and internet policy. Moving forward, trade negotiations at the WTO and other regional bodies can be informed by the deficiencies in the TPP to work towards a more robust and well-balanced digital trade regime. The other important lesson from the TPP is to take a step back and engage more deeply with the expertise of the internet policy community while setting rules to facilitate digital trade.

II NEW DISCIPLINES ON DIGITAL TRADE IN THE TPP

A *New Disciplines on Data Flows and Data Localization in the TPP*

Free flow of data across the internet enables users to transfer digital content across borders. Not only digital services and e-commerce businesses, but even traditional manufacturing and logistics industry rely on free data flows to optimize their operations and improve their productivity.[37] When a country imposes restrictions on cross-border transfer of data, either by restricting information flows directly,[38] or requiring local storage of all or some categories of digital data,[39] it results in causing inefficiencies for digital service providers, fragmentation of the internet network, and reduced choices for consumers, both within and outside that country.[40] Therefore,

---

[36] Kimberlee G Weatherall, 'JSCOT Submission on TPP', http://works.bepress.com/kimweatherall/34/ (visited 15 August 2016).; Matthew Rimmer, 'A Mercurial Treaty: the Trans-Pacific Partnership and the United States', *The Conversation*, 15 June 2012, http://theconversation.com (visited 13 August 2016); Sean M. Flynn et al, 'The US Proposal for an Intellectual Property Chapter in the Trans Pacific Partnership Agreement' 28 American University Law Review 112 (2012).

[37] James Manyika et al, 'Digital Globalization: The New Era of Global Flows' , McKinsey Global Institute, March 2016, http://www.mckinsey.com (visited 20 September 2016) 1; Matthieu Pélissié du Rausas et al, 'Internet matters: The Net's sweeping impact on growth, jobs, and prosperity,', McKinsey Global Institute, May 2011, http://www.mckinsey.com (visited 20 September 2016) 1; UNCTAD, 'Data protection regulations and international data flows: Implications for trade and development' , UNCTAD/DTL/STICT/2016/1 (April 2016), http://unctad.org (visited 20 September 2016) xi.

[38] For eg, Computer Information Network and Internet Security, Protection and Management Regulations (China) Ministry of Public Security, 30 December 1997, art 4-6.

[39] For eg, Federal Law No. 242-FZ of July 21, 2014 on Amending Some Legislative Acts of the Russian Federation in as Much as It Concerns Updating the Procedure for Personal Data Processing in Information-Telecommunication Networks (Russia) Federal Law No. 242-FZ, Adopted 4 July 2014, Approved 9 July 2014.

[40] See generally Matthias Bauer et al, 'The Costs of Data Localization: Friendly Fire on Economic Recovery', ECIPE Occasional Paper 3/2014, European Centre for International Political Economy (2014) 2.

restrictions on data flows are a major barrier to digital trade, and expectedly, received significant attention during the TPP negotiations.

During the seventh round of TPP negotiations in 2011, the US tabled the draft text on mandatory cross-border data flows for the very first time.[41] The main purpose behind this provision was to undercut policies such as data localization, protection of indigenous technologies, and blocking of foreign digital services in many countries.[42] This proposal was however unacceptable to several of the negotiating countries for different reasons. Australia, New Zealand and Canada wanted to safeguard regulatory space in the TPP to restrict cross-border data transfers to address privacy concerns regarding their citizens' data.[43] I discuss this in greater detail in Section B below. On the other hand, Vietnam was opposed to the US proposal as it would conflict with its domestic law which restricts internet use and data transfer on grounds of national security.[44] Malaysian law also contained certain restrictions on cross-border data transfers.[45] Singapore sought an exemption from this provision, in order to be able to restrict data flows on grounds of public morality.[46] As late as 2013, a leaked draft of the TPP Electronic Commerce Chapter indicated that the countries had not arrived at a consensus regarding the provision on data flows.[47]

The above disagreement between the TPP countries was ultimately resolved (although the details of the trade-offs are not public knowledge yet) and the TPP became the first trade agreement to incorporate a binding provision on cross-border data flows and prohibition of server localization measures in TPP arts 14.11 and 14.13 respectively. These two provisions have attracted strong academic and industry support.[48]

1 *Mandatory Nature of Provisions on Data Transfer and Data Localization*

TPP art 14.11.2 requires all TPP parties to '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'. The definition of 'covered person' excludes any kind of 'financial institutions' or 'cross-border supplier of financial services' but broadly covers all other service suppliers and investments.[49] The exclusion of financial services from this provision attracted

[41] 'Official Says US Tabled Text on Free Data Flow at Vietnam TPP Round' 29.29 *Inside US Trade* (22 July 2012).
[42] Ibid.
[43] Ibid. See also 'TPP Countries to Discuss an Australian Alternative to Data Flow Proposal' 30.27 *Inside US Trade* (6 July 2012).
[44] Decree on the Management, Provision and Use of Internet Services and Online Information (Vietnam), Decree No. 72/2013/ND-CP, 15 July 2013.
[45] See Personal Data Protection Act 2010 (Malaysia), Act No. 709 (Adopted 2 June 2010) Section 129(1).
[46] 'Vietnam Seeks Delay on Enforceability of TPP E-Commerce Commitments') 32.44 *Inside US Trade* (7 November 2014).
[47] Wikileaks, 'TPP Country Positions', 6 November 2013, http://big.assets.huffingtonpost.com/1296_001.pdf (visited 20 September 2016).
[48] Branstetter, above n 4, 72; Walker, above n 7.
[49] TPP, art 14.1, definition of 'covered person'.

strong criticism,[50] and the USTR has since advocated for preventing data localization in the financial sector in future trade deals. [51] Further, these provisions do not apply to government data as the Electronic Commerce Chapter does not apply to 'government procurement' or 'information held or processed by or on behalf' of a government for 'collection' or 'processing' of data.[52]

TPP art 14.11.2 has a very broad scope of application – potentially, most data that is transferred over the internet, including personal communication over social networking sites, emailing services, etc. is arguably *for* the 'conduct of the business of a covered person'. The word 'for' indicates, that in the least, there must be a certain degree of causal relationship between the flow of data (i.e. activity) and the business of the covered business (i.e. provider of any digital service). In practice, it is not only expensive but also infeasible to establish causal linkages between the data transfer and the covered business, and thereby, distinguish 'information' covered under this provision from 'general data' that flows through internet networks. The internet functions on an end-to-end functionality and the network infrastructure itself does not read the content of data transferred,[53] unless internet service providers ('ISPs') filter the data. Such actions by ISPs also raise other policy concerns such as privacy intrusions, which I discuss later in Section E.

The challenge in distinguishing 'information' from 'data' raises important questions regarding enforcement of this provision. For instance, can personal information such as religious, sexual or political preferences (which appears unrelated to any business activity) be excluded from this provision? Can a service provider (foreign or domestic) argue that this data may be helpful to provide suggestions for lifestyle products (for eg, *halal* or *kosher* food products) or customized reading/news lists (for eg, discussing LGBT issues or video recommendations on YouTube)? The privacy laws of a country may play an instrumental role in deciding these questions (see Section B below). Yet, in countries with weak privacy regimes, or in case of a conflict in privacy laws of different TPP countries, legal uncertainty may arise regarding information transfers and subsequent use/processing of user data.

The most common regulatory tool used to restrict flow of data outside a country's borders is enforcement of data localization laws.[54] Data localization laws require any foreign or domestic service provider to store all information of residents of a country (or frequently, certain categories of information) in servers located within the borders of the country. Data localization is especially detrimental to efficient growth of cloud computing, which is premised on economies of scale and seamless transfer of information around the world. TPP art 14.13.2 prohibits TPP parties from

[50] See for eg, Nigel Cory and Robert D Atkinson, 'Financial Data Does Not Need or Deserve Special Treatment in Trade Agreements', Information Technology and Information Foundation Report, April 2016, http://www2.itif.org (visited 20 September 2016).
[51] Len Bracken, 'Treasury Financial Services Industry Agree on Data Proposal' *International Trade Daily* (25 May 2016); Lew Floats Possibility of Side Deal to Address TPP Data Localization' *World Trade Online* (7 March 2016); 'Lew Reiterates Possibility of TPP Side Deal, But Emphasizes Future Fix' *World Trade Online* (23 March 2016).
[52] TPP, art 14.8.3.
[53] See discussion in Section IID below.
[54] See generally, Anupam Chander and Uyen P Le, 'Data Nationalism' 64 (3) Emory Law Journal 677 (2014).

requiring a 'covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory'. As a result of this provision, a TPP country cannot require service providers from other TPP countries to store all their data locally, unless it is covered under the exception in TPP art 14.13.3.

2 *Vaguely Worded Exception to Data Transfer and Data Localization*

TPP art 14.11.3 and art 14.13.3 set out a legal exception for cross-border transfer of information and localization of computing facilities respectively. As per the wording of this exception, countries can 'adop[t] or maintain[n] measures' inconsistent with art 14.11.2 and art 14.13.2 in order to achieve a 'legitimate public policy objective', provided that such measure is 'not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or disguised restriction on trade' and 'does not impose restrictions on (transfers of information)/ (the use or location of computing facilities) greater than required to achieve the objective'.[55] The words 'adopting' or 'maintaining' refer to both existing measures and future measures.

Unlike the general exceptions in *General Agreement on Trade in Services* ('GATS') art XIV[56] and *General Agreement on Tariffs and Trade* ('GATT') art XX,[57] where specific policy objectives have been identified, TPP art 14.11.3 and 14.13.3 refers to an undefined 'legitimate public policy objective'. Perhaps, such a wording might have been deliberate to safeguard the regulatory autonomy of countries to take necessary steps to protect user interests in a rapidly evolving internet economy; however it creates significant legal uncertainty. For instance, what happens when a particular policy objective (such as censorship or restraint on expression) is legitimate in some TPP countries, and considered illegitimate in others? What is the connection between acknowledging a country's 'own regulatory requirement' under art 14.11.1 and art 14.13.1 and 'legitimate public policy objective' in the exception? Is it one and the same thing, or is it different? Would principles recognized in international declarations/treaties (such as *Universal Declaration on Human Rights*) have any relevance in interpretation of a 'legitimate public policy objective'? What is the relationship between the exception contained in TPP art 14.11.3 and 14.13.3 and GATS art XIV, which is incorporated *mutatis mutandis* into the TPP?[58] Can the latter provision inform the interpretation of these exceptions – for instance, can considerations related to public health, public order, online consumer protection (i.e. 'preventing fraudulent and deceptive practices') and privacy be considered as 'legitimate public policy objective'? These questions are not answered by the existing wording of the TPP provisions – yet, similar language is being introduced in other trade agreements.[59]

---

[55] TPP, art 14.11.3 and art 14.13.3.
[56] *Marrakesh Agreement Establishing the World Trade Organization*, opened for signature 15 April 1994, 1869 UNTS 183 (entered into force 1 January 1995), annex 1B ('*General Agreement on Trade in Services*') ('GATS'), art XIV.
[57] *Marrakesh Agreement Establishing the World Trade Organization*, opened for signature 15 April 1994, 1867 UNTS 187 (entered into force 1 January 1995) annex 1A ('*General Agreement on Tariffs and Trade*') ('GATT'), art XX.
[58] TPP, art 29.1.3.
[59] See for eg, TISA, art X.3.5 *bis* (as proposed by Australia); Amendment to SAFTA, art 14.13.3, 14.15.3.

While it is understandable that the TPP negotiators did not want to produce an exhaustive list of 'legitimate public policy objective[s]', providing certain examples (such as in an explanatory footnote) may have been instructive in the interpretation of these exceptions. In case of a dispute, the TPP tribunals will face an uneasy task of identifying whether a particular measure is for a 'legitimate public policy objective'. Two approaches are possible in such a scenario: (a) to adopt a deferential standard and not interfere/question the intended policy goals of the government, which may be self-defeating when cross-border data flows are unnecessarily interrupted; or (b) to conduct a detailed assessment in light of a country's domestic laws and its international treaty commitments if a certain policy objective is for a 'legitimate public policy objective', which may result in judicial activism. Both these approaches are imperfect, and are likely to attract criticism.

Other interpretive complications may also arise in interpretation of this exception. First, determination of a rational nexus between the 'measure' and 'legitimate public policy objective' is not straightforward. Considerable dispute exists whether specific measures such as restrictions on data transfer across borders can effectively 'achieve' important public policy goals such as protection of privacy and security. The TPP tribunals will need external expertise to conclusively decide on such questions. Further, in practice, political incentives driving data localization measures are not always straightforward, particularly when pursuance of legitimate goals results in creating opportunities for protectionism.[60]

Secondly, the TPP incorporates GATS art XIV-type and GATT art XX-type chapeau language in art 14.11.3(a) and (b) and art 14.13.3(a) and (b). The existing WTO jurisprudence provides informative jurisprudence on the meaning of 'arbitrary or unjustifiable discrimination' or a 'disguised restriction on international trade'.[61] In assessing whether a measure is 'not more trade restrictive than necessary to achieve the objective', the TPP tribunal can also adopt a test similar to the 'weighing and balancing test' under GATT art XX.[62] However, the TPP tribunals will still need to answer some difficult questions such as whether to accept the importance of a policy objective that violates established human rights law, and how to assess the restrictive impact of a data localization measure (given that data flows are not perfectly measurable).

Cumulatively, art 14.11 and art 14.13 enables free data flows across an integrated internet network, and provides greater choice to both service providers and consumers. Therefore, several experts have welcomed the positive contributions made by these provisions to both digital trade and the

[60] Neha Mishra, 'Data Localization Laws in a Digital World' *Public Sphere* 137 (2016), 151.
[61] See WTO Appellate Body Report, *United States — Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WT/DS285/AB/R, adopted 20 April 2005 , paras 339, 344, 356 ('*US — Gambling*'); WTO Appellate Body Report, *United States — Import Prohibition of Certain Shrimp and Shrimp Products*, WT/DS58/AB/R, adopted 6 November 1998, paras 156, 159; WTO Appellate Body Report, *United States — Standards for Reformulated and Conventional Gasoline*, WT Doc WT/DS2/AB/R. adopted 20 May 1996, pp. 22-24; WTO Panel Report, *Brazil — Measures Affecting Imports of Retreaded Tyres*, WT Doc WT/DS332/R, circulated 12 June 2007, adopted 17 December 2007, paras 7.272-7.273 ('*Brazil — Retreaded Tyres*').
[62] See WTO Panel Report, *Brazil — Retreaded Tyres*, paras 7.379–7.380. See also WTO Appellate Body Report, *US — Gambling*, paras 239-242; WTO Appellate Body Report, *Korea — Measures Affecting Imports of Fresh, Chilled and Frozen Beef*, WTO Doc WT/DS161/AB/R, adopted 10 January 2001, paras 164, 166.

ideal of a 'free and open internet'.[63] However, the weakly-worded exceptions in art 14.11.3 and art 14.13.3 fail to provide sufficient legal certainty regarding the legitimacy of interference with data flows. The policy balance intended to be struck through these exceptions between safeguarding data flows and protecting user data provides a site ripe for ideological conflict between the various TPP countries.[64]

B *Mandating Legal Framework for Personal Information Protection in the TPP*

Privacy and/or data protection issues are often viewed very differently among countries due to their specific cultural, religious and political contexts.[65] As a result, privacy requirements often vary across jurisdictions. However, such variations usually raise the compliance costs for cross-border service providers since they need to customize their websites, data collection methods, etc. Such requirements also impede on digital innovation and can affect the adoption/use of new technologies.[66] Further, complicated privacy requirements deter small and medium enterprises ('SMEs') from engaging in digital trade, as they may not have the resources required to implement customized digital solutions for such requirements.[67] Therefore, privacy laws are potentially a discriminatory barrier to trade. At the same time, sound privacy laws enhance the confidence of internet users that their data is being safely collected, used and stored by service providers, and thereby, is an important goal in internet policy-making.[68] Further, a sound privacy framework is Further, a sound privacy framework is also fundamental to secure data flows across the internet network.

Since the early stages of the TPP negotiations, the US was keen on a flexible mechanism for protection of personal information, by allowing self-certifying mechanisms for data transfer, and adoption of self-regulatory frameworks.[69] In 2004, the Asia-Pacific Economic Co-operation ('APEC') had adopted a similar privacy framework, which appears to have informed the US position during the TPP negotiations.[70] On the other hand, countries such as Australia and Canada were opposed to a lenient privacy framework, since it could have restricted their ability to disallow cross-border data transfers on grounds of privacy.[71] Australia was particularly concerned about

---

[63] See above n 48.
[64] See for eg, Burcu Killic and Tamir Israel, 'The Highlights of the Trans-Pacific Partnership E-Commerce Chapter', *Public Citizen*, 5 November 2015, https://www.citizen.org (visited 20 September 2012).
[65] See James Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' 113 Yale Law Journal 1153 (2004), at 1153-54.
[66] Avi Godfarb and Catherine Tucker, 'Privacy and Innovation' in Joshua Lerner et al (eds), *Innovation Policy and the Economy, Vol- 12* (National Bureau of Economic Research: University Presses Marketing, 2012) 65-89 at 66.
[67] Ibid.
[68] *Declaration of Principles – Building the Information Society: A Global Challenge in the New Millennium*, WSIS-03/GENEVA/DOC/4-E, 12 December 2003, art 35. See also IGF, 'The 4th Internet Governance Forum: Chair's Summary',15-18 November 2009, http://www.intgovforum.org/ (visited 30 September 2016) 7.
[69] 'U.S. Examining How APEC Work Could Inform TPP Negotiations' 28.5 *Inside US Trade* (5 March 2012).
[70] APEC, *APEC Privacy Framework* (November 2004).
[71] 'Official Says US Tabled Text on Free Data Flow at Vietnam TPP Round', 29.29 *Inside US Trade* (22 July 2011); 'TPP Countries to Discuss an Australian Alternative to Data Flow Proposal' 30.27 *Inside US Trade* 30.27 (6 July 2012).

maintaining the privacy of the e-health records of its residents, if it could be freely transferred abroad to other TPP countries.[72] At the Dallas negotiating round in 2012, Australia proposed alternate language to the provision on data flows to allow more flexibility to TPP countries to ensure that data transfers are compliant with their domestic privacy regime.[73] Although the Australian proposal was eventually rejected, Australia got an exemption from allowing transfer of e-health records of its citizens abroad.[74]

TPP art 14.8.2 requires every TPP party to 'adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce'. However, the provision does not prescribe any standards or benchmarks for the legal framework, but sets out a broader and more general requirement that TPP parties 'take into account principles or guidelines of relevant international bodies'.[75] Footnote 6 to art 14.8.2 provides further clarification:

> For 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.[76]

This footnote paves the path for TPP countries to adopt their own version of a privacy law without having to comply with any specific international standards. Given that online privacy is increasingly recognised in the international community as a fundamental human right,[77] the ambiguous wording of this footnote can be contentious in two ways. Firstly, countries may raise the argument that the boundaries of 'legitimate public policy objective' in TPP arts 14.11.3 and 14.13.3 is circumscribed by TPP art 14.8.2 and the accompanying footnote, discussed above. In other words, the policy space for countries to restrict data flows on grounds of privacy will be determined by the interpretation of what constitutes a 'legal framework' for 'protection of personal information' under art 14.8. Particularly, if member countries or future TPP tribunals take a narrow view of this provision, the impact on online privacy issues may be significant.

Secondly, the provision, in its current form does not provide sufficient clarity on the relevance of well-accepted international standards in defining the scope and applicability of TPP art 14.8.2. For instance, 'voluntary undertakings by enterprises relating to privacy', recognised in footnote 6, may not necessarily be in compliance with 'principles or guidelines' in international human rights

---

[72] 'TPP Countries to Discuss an Australian Alternative to Data Flow Proposal' 30.27 *Inside US Trade* 30.27 (6 July 2012).
[73] Ibid.
[74] 'US Yields to Australian Data Flow Exemption in TPP, Mulls Demands by Others' 33.8 *Inside US Trade* (27 February 2015).
[75] TPP art 14.8.2.
[76] TPP art 14.8.2, n 6.
[77] See, for eg, *GA Res 68/167: The Right to Privacy in the Digital Age*, Resolution adopted by the General Assembly on 18 December 2013, 68th session, UN Doc A/RES/68/167 (21 January 2014); *The Right to Privacy in the Digital Age*, 69th session, Third Committee, Agenda Item 68 (b), UN Doc A/C.3/69/L.26/Rev.1(19 November 2014); *The Right to Privacy in the Digital Age*, 71st session, Third Committee, Agenda Item 68(b), UN Doc A/C.3/71/L.39/Rev.1 (16 November 2016).

instruments. Similarly domestic laws that provide ad hoc or sector-specific mechanisms for protection of privacy may not always adequately protect privacy of individuals in all aspects of life. Does this mean that TPP countries can justify their privacy laws based on rules in a trade agreement, even if it does not arguably meet the required thresholds in international law? Perhaps not, but as a result of the conflicting wording of this provision, the internet community has expressed strong reservation against this provision.[78]

TPP art 14.8.3 states that all TPP countries 'shall endeavour to adopt non-discriminatory practices in protecting users of electronic commerce from personal information protection violations occurring within its jurisdiction'. The non-binding nature of art 14.8.3 is surprising, given that protection of privacy of internet users is an important policy goal, and instrumental in achieving consumer trust in internet services. TPP art 14.8.4 requires each TPP party to publish information on how consumers can pursue violations for privacy breaches, and how businesses can comply with the legal framework for personal information protection. This ties in with another non-binding provision that states that TPP countries 'shall endeavour' to provide assistance to SMEs in the use of e-commerce on issues related to privacy, online consumer protection etc.[79] Finally, art 14.8.5 recognizes that parties should 'promote compatibility' between their privacy regimes through various mechanisms such as 'autonomous' or 'mutual' recognition of each other's regulations, or through 'broader international frameworks'.

Inspite of duly recognizing the important policy goals of privacy laws in TPP art 14.8.1,[80] the TPP fails to effectively realise these goals.[81] Vietnam's new law on protection of personal information is a case-in-point.[82] This law appears to be rudimentary, undetailed and adopts a minimalist approach, while privileging national security over privacy in an indiscriminate manner.[83] It is possible that the clarifying regulations and guidelines may provide more substance to the generic principles laid down in this Vietnamese law. However, this example brings out basic deficiencies in the wording of the provision – even a weak domestic law on protection of personal information can be considered sufficient to satisfy the legal requirement under TPP art 14.8.2.

One of the most important questions arising from TPP art 14.8.2 is the extent to which trade agreements should deal with online privacy issues. In my view, free flow of information via the internet and online privacy are parallel issues, as any kind of uninterrupted flows of personal information through internet networks should be complemented with adequate levels of protection

[78] See eg, Internet Governance Forum, above n 8 (Comments of Burcu Killic).
[79] TPP, art 14.15.
[80] TPP, art 14.8.1 reads as follows: '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'.
[81] Graham Greenleaf, 'The TPP Agreement: An Anti-Privacy Treaty for Most of APEC' 138 Privacy Laws & Business International Report 21 (2015); Sam Klein, 'The Data is in the Details: Cross-border data flows and the Trans Pacific Partnership', *The Diplomat*, 23 November 2015, http://thediplomat.com (visited 30 November 2016).
[82] Law on Network Information Security (Vietnam), Law no.: 86/2015/QH13, 1 July 2016, art 16 – art 20 ('*Law on Network Information Security*).
[83] Ibid. See also *Law on Network Information Security*, art 4.1.

of user trust, through appropriate privacy/data protection rules. In that sense, high-level regulatory coordination amongst TPP countries on principles of privacy/data protection can be effectively considered as a 'precondition' for enabling data flows.[84] In order to facilitate interoperability of privacy regimes, TPP art 14.5 requires mutual or autonomous recognition of privacy regimes or 'promoting compatibility' through 'other international frameworks' (possibly referring to APEC) among TPP countries so as to enable free data flows across these countries. However, the problem with this provision arises because there is no internationally established consensus on privacy issues, not even amongst the TPP countries. Should TPP countries be under an obligation to recognize privacy frameworks that are extremely weak or disproportionate, such as the new data protection law in Vietnam? What should be the bare minimum standard to assess compatibility of a country's privacy law with the framework in TPP art 14.8.2? The TPP does not provide any concrete answers to these questions.[85]

TPP art 14.8 also needs to be viewed in context of the ideological divide between TPP and non-TPP countries on issues of privacy and data protection. The divide between the EU and the US on development of privacy standards and cross-border transfer of data is evident in the TTIP negotiations.[86] Further, the privacy law of potential new entrants to the TPP such as South Korea and Philippines could be in conflict with the existing framework in TPP art 14.8.[87] New entrants to the TPP can execute side agreements with existing countries to address data flow issues arising from variable privacy standards[88] - however, this approach can only partially solve the indeterminacy of data flows arising from the conflict in different privacy regimes.

C *New Disciplines on Cybersecurity-Related Issues in the TPP*

Issues related to cybersecurity hold central importance in regulation of the internet. Cybersecurity is a complex, multi-faceted mechanism meant to 'protect computers [including any digital or smart device], networks, programs and data from unintended or unauthorized access, change or destruction'.[89] Cybersecurity may relate to multiple policy goals such as protection of national

[84] See generally, for relevance of regulatory cooperation in services trade, Aaditya Mattoo, 'Services Trade and Regulatory Cooperation', E15 Expert Group on Services - Think piece, 2015, http://e15initiative.org (visited 30 September 2016).

[85] Another relevant example, which is outside the scope of this article, is the legal requirement under TPP art 18.28 for each TPP country to maintain 'online public access to a reliable and accurate database of contact information concerning domain name registrants'. Although the application of this provision is subject to 'relevant administrator policies regarding protection of privacy and personal data', application of this provision raises concerns regarding whether privacy rights may be breached, particularly in countries with weak privacy/data protection laws.

[86] See above n 27.

[87] Branstetter, above n 4, 80. Recently implemented data protection law in Philippines is also in line with EU and Korea data protection law. See Mark and Parsons and Louis Crawford, 'The Philippines Finalizes Its Data Privacy Act 2012 Implementing Rules: Another High Bar for Data Protection Set in the Asia-Pacific Region' *World Data Protection Report* (13 October 2016).

[88] Lee Branstetter, 'TPP and the Conflict Over Drugs TPP and Digital Trade', Presentation at Peterson Institute of International Economics (28 March 2016).

[89] University of Maryland University College, 'Cybersecurity Primer' http://www.umuc.edu (visited 30 September 2016).

security, preventing online thefts of trade secrets, protection of sensitive personal information such as financial and personal identification details, and preventing cyber-crimes and fraudulent practices on the internet.

In digital trade, cybersecurity is becoming the 'emerging' issue due to the presence of a variety of trade-restrictive or economically harmful practices such as digital surveillance and spying/stealing of confidential business information and trade secrets, and stealing customer details through targeted attacks on e-commerce websites.[90] In adopting/implementing technical standards to protect security and integrity of digital networks and devices, due caution is needed to ensure that cybersecurity laws do not create opportunities for protectionism or unnecessarily obstruct foreign service providers.[91] However, cybersecurity issues should not be simply viewed as a barrier to trade.[92] Like sound privacy requirements, cybersecurity mechanisms play a critical role in enabling digital trade. By providing a secure and resilient network infrastructure, cybersecurity laws can enable better protection of both consumer and business interests, and facilitate a better online trading environment for all.[93]

1 *Weak Rules on Cybersecurity Cooperation and Online Consumer Protection*

Due to the relevance of cybersecurity as an important digital trade issue, TPP art 14.16 sets out a provision on cybersecurity cooperation which reads as follows:

> The Parties recognise the importance of:
>
> (a) building the capabilities of their national entities responsible for computer security incident response; and
>
> (b) using existing collaboration mechanisms to cooperate to identify and mitigate malicious intrusions or dissemination of malicious code that affect the electronic networks of the Parties.

Besides being non-binding in nature (when it should have been made binding), the above provision identifies a limited scope of activities for cooperation, namely 'malicious intrusions' or 'dissemination of malicious code' and capacity-building of governmental bodies dealing with cybersecurity incidents – thus, focusing on a narrow scope of cybersecurity-related concerns in digital trade.

TPP art 14.16 also fails to identify possible mechanisms for countries to collaborate. Cybersecurity standards have traditionally been developed by private bodies and multistakeholder institutions

---

[90] See generally, Shin-yi Peng, 'Cybersecurity Threats and the WTO National Security Exceptions' 18 Journal of International Economic Law 449 (2015), at 449-50.
[91] Ibid.
[92] Besides GATS general exception (Art XIV), TPP art 29.2 (security exceptions) will be relevant in justifying trade-restrictive cybersecurity measures.
[93] See generally, Pricewater House Coopers, 'Moving Forward with Cybersecurity and Privacy: Key Findings from the Global State of Information Security', 2016, https://www.pwc.com (visited 10 November 2016) 2-4; Bieron Brian and Usman Ahmed, 'Regulating E-commerce through International Policy: Understanding the International Trade Law Issues of E-commerce' 46 (3) Journal of World Trade 545 (2012), at 568.

such as the Internet Engineering Task Force.[94] Although governments have recently started developing policies and national strategies to deal with cybersecurity issues, they do not play a central role in standard-setting, with the exception of certain countries like China.[95] The term 'existing collaborative mechanisms' in TPP art 14.16(b) could have been explained to include multistakeholder, multilateral and industry mechanisms, other than inter-state mechanisms, to better reflect the institutional mechanism of standard-setting on cybersecurity issues.

Another missed opportunity in the TPP is to explicitly identify the relationship between online consumer protection (TPP art 14.7) and cybersecurity. Consumer protection is typically a domestic law issue; however, protection of consumer interests holds special importance in facilitation of digital trade across countries, due to the immediate proximity of sellers/service providers and the consumers. Online consumer protection involves a broad range of issues, from traditional issues of misrepresentation or failed deliveries (which are traditional contractual issues, and cannot be addressed specifically in a trade agreement), to more contemporary issues such as data breaches resulting in stealing of customer data and privacy breaches (which are more pertinent in trade agreements such as the TPP, in light of the legal requirement to facilitate cross border data flows, as discussed in Section IIA). [96]

TPP art 14.7.2 states as follows:

> Each Party shall adopt or maintain consumer protection laws to proscribe fraudulent and deceptive commercial activities that cause harm or potential harm to consumers engaged in online commercial activities.

TPP art 14.7.3 'recognizes' the importance of cooperation between different consumer protection bodies across TPP countries, including 'online consumer activities'. Again, being non-binding, this provision has limited significance in promoting cooperation on cross-border consumer protection issues in digital trade. Instead, if the TPP had contained a legal requirement for all countries to provide a dispute resolution system for 'online commercial activities', it may have been more effective in creating consumer confidence in cross-border trade.[97]

---

[94] Abraham D. Soefer et al, 'Cyber Security and International Agreements' in National Research Council, *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy* (Washington: The National Academic Press, 2010) 179 -206 at 182-84.

[95] Eva Dou, 'Untangling China's Cybersecurity Laws', *The Wall Street Journal (China Real Time Report)*, 3 June 2016, http://blogs.wsj.com (visited 30 August 2016).

[96] Some scholars however argue that rules on consumer protection do not traditionally 'belong in trade agreements'. See Daneil J Ikenson et al, 'Should Free Traders Support the Trans- Pacific Partnership? An Assessment of America's Largest Preferential Trade Agreement', CATO Institute, CATO Working Paper 39 (12 September 2016) 48.

[97] See, eg, Joshua P Meltzer, 'A New Digital Trade Agenda', E15 Expert Group on the Digital Economy, Overview Paper, August 2015, http://e15initiative.org (visited 30 September 2016) 13. Similar initiatives have also been introduced in the WTO recently, see WTO documents, above n 29-31.

2 *Weak and Unambitious Provision on Spam*

The regulation of 'unsolicited commercial electronic messages' or 'spam' is also closely linked to online consumer protection. Regulation of spam pertains to prevention of unsolicited messages (often in bulk) either for purposes of advertising or for more nefarious activities such as phishing and malware attacks, botnets, etc.[98] Therefore, anti-spam laws effectively result in service providers blocking certain kinds of harmful or unsolicited messages.[99]

TPP art 14.14.1 requires all TPP parties to 'adopt or maintain measures regarding unsolicited commercial electronic messages' that:

> (a) require suppliers of unsolicited commercial electronic messages to facilitate the ability of recipients to prevent ongoing reception of those messages;
> (b) require the consent, as specified according to the laws and regulations of each Party, of recipients to receive commercial electronic messages; or
> (c) otherwise provide for the minimisation of unsolicited commercial electronic messages.

TPP art 14.14.1 sets out a bare-bones legal framework for regulation of spam. This is understandable, as international consensus on legal standards to regulate spam is lacking, and international cooperation on this issue has generally been limited.[100] Largely, regulation of spam is managed through self-regulatory standards in the private sector, and often, through very informal mechanisms. For example, spam blacklists are maintained by private organizations such as Spam and Open Relay Blocking System, Spamhaus, Webron LLC etc., and are often used by ISPs and companies to protect their users.[101]

The TPP recognizes that spam raises transnational policy issues by providing that TPP parties 'shall endeavour to cooperate in appropriate cases of mutual concern regarding the regulation of unsolicited commercial electronic messages'.[102] Yet, this provision only provides a very weak mechanism for achieving cooperation amongst TPP countries on regulation of spam. This is particularly surprising, as the largest number of spam messages is generated from countries within the TPP region. For instance, as per data collected by ICSA Labs, the largest number of spam

---

[98] Vint Cerf et al, 'Internet Governance is Our Shared Responsibility' 10 (1) *I/S: A* Journal of Law and Policy for the Information Society 1(2014), at 24-25.

[99] Van Den Hende argues that in circumstances where a country has offered full commitments for cross-border supply of advertising services, blocking of spam is unlikely to constitute a violation of market access requirements such as under GATS art XVI, if there are no constraints on the general use of 'international communication facility for the supply of advertising services'. See Lode Van Den Hende and Herbert Smith LLP, 'GATS Article XVI and National Regulatory Sovereignty: What Lessons to Draw From US—Gambling?' in Kern Alexander and Mads Tønnesson Andenæs (eds), *The World Trade Organization and Trade in Services* (Leiden: Martinus Nijhoff Publishers, 2008) 475-496 at 479.

[100] Shen Zao Hui, 'Why is there no International Law on Anti-Spam?' 3 Sungkyunkwan Journal of Science and Technology Law 81 (2009), 85-89. Certain regional initiatives such as the APEC Anti-Spam Strategy, London Action Plan, Seoul-Melbourne Anti-Spam Memorandum, which seek to establish multistakeholder frameworks for regulation of spam. See Cristina Bueti, 'Countering Spam', World Summit on the Information Society, Tunis, (11 October 2005).

[101] For discussion, see Milton L Mueller, *Networks and States: The Global Politics on Internet Governance* (MIT Press Online, 2010) 166.

[102] TPP, art 14.14.3.

messages in the world is generally generated from United States, while Vietnam and Mexico also have a large number of spam suppliers.[103]

Finally, the TPP fails to contextualize spam-related regulation issues in the current digital economy, such as by providing due attention to cybersecurity threats arising from botnet/malware attacks via spam,[104] and potential breach of due process or privacy laws in monitoring content of spam. This effectively makes art 14.14 a stand-alone provision in the TPP, disconnected from the larger agenda of facilitating high-quality digital trade between TPP countries.

3 *Protecting Proprietary Interests of Digital Industry: Involuntary Disclosure of Source Code and Trade Secret Thefts*

TPP art 14.17.1 imposes a prohibition on all TPP parties from 'requir[ing] the transfer of, or access to, source code of software owned by a person of another Party, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory'. Source code is not defined in the TPP, but usually refers to the human-readable instructions which are written in any programming language, which is executed by computers.[105] TPP art 14.17.1 applies to 'mass-market software or products containing such software' but excludes 'software used for critical infrastructure'.[106] Further, this provision is not applicable to 'commercially negotiated contracts' which require for the 'provision of source code', or in circumstances, where a TPP country may 'requir[e] the modification of source code of software necessary for that software to comply with laws or regulations which are not inconsistent with this Agreement'.[107] The latter will possibly include situations where owners of source code are required to modify their source code to comply with national security requirements in the domestic laws of a country. Finally, the prohibition on involuntary disclosure of source code will also not apply to provision of source code for 'patent applications', 'granted patents', including 'in relation to patent disputes', provided that there are 'safeguards against unauthorised disclosure under the law or practice of a Party'.[108]

The purpose behind TPP art 14.17 is to protect the commercial interests of companies selling their software across TPP markets, without unduly worrying about loss of IP or compromising the security of the proprietary code. In particular, this will prevent TPP countries from following policies similar to that of China, where the government requires access to proprietary source code

---

[103] ICSA Labs, 'Spam Data Centre', https://www.icsalabs.com/spam-data-center (visited 15 November 2016). From time to time, other countries also may be producing more spam.
[104] Susan Ariel Aaronson, 'What does TPP mean for the Open Internet?', Policy Brief on Trade Agreements and Internet Governance Prepared for the Global Commission on Internet Governance, International Institute for Economic Policy (16 November 2015), https://tpplegal.files.wordpress.com/2015/12/iiep-paper.pdf (visited 20 September 2016).
[105] Java, 'What is Source Code?', http://java.about.com/od/s/g/sourcecode.htm (visited 23 September 2016).
[106] TPP, art 14.17.2.
[107] TPP, art 14.17.3.
[108] TPP, art 14.17.4.

from software manufacturers selling within their market.[109] In the past, big American companies such as International Business Machines and Microsoft have been pressurized by the Chinese government to provide access to source code of their software products, as a condition of access to domestic market.[110]

However, TPP art 14.17 is likely to have a limited scope of application because the exemption for 'software used in critical infrastructure' can be interpreted very broadly. For example, in the US, 16 sectors are identified as 'critical infrastructure sectors', namely chemical, communications, dams, emergency services, financial services, government facilities, IT, transportation systems, commercial facilities, critical manufacturing, defence industries, energy, food and agriculture, healthcare, nuclear sector and waste and water.[111] This list applies to a wide range of digital services. Further, any software or digital services such as cloud computing used in a 'critical infrastructure' sector is also likely to be used in non-critical sectors, for instance, apparel manufacturing.[112]

Further, TPP art 14.17 is not complemented by a strong provision on cybersecurity and consumer protection. Several of the TPP countries have weak cybersecurity standards – for example, Vietnam, Peru, Mexico and Brunei have been ranked very low in the Global Cybersecurity Index.[113] Aaronson argues whether software products produced in such countries can be considered secure enough to be used in other TPP countries, without a comprehensive assessment of the proprietary source code of those products.[114] Even products such as routers, which are often manufactured in developing countries, can be infested with malware.[115] It is possible, that in many of such scenarios, governments will resort to the 'critical infrastructure' exemption to demand access to source code,[116] thus limiting the application of this provision.[117]

---

[109] See, eg, Cybersecurity Multi-Level Protection Scheme (China); Notice on the Promotion Guidelines for Banking Applications of Secure and Controllable Information Technology, CBRC Notice 317, 2014-15.
[110] Theodore H. Moran, 'Should US Tech Companies Share Their "Source Code" with China?', *Real Time Economic Issues Watch*, 27 October 2015, https://piie.com (visited 20 September 2016).
[111] Department of Homeland Security, 'Critical Infrastructure Sectors' (27 October 2015).
[112] Stewart Baker, 'Cybersecurity and the TPP' *The Washington Post*, 6 November 2015, https://www.washingtonpost.com (visited 20 September 2016).
[113] International Telecommunications Union, *Global Cybersecurity Index* (2014) (see global ranking).
[114] Aaronson, above n 104.
[115] Lucian Constantin, 'Malware implants on Cisco routers revealed to be more widespread', *InfoWorld*, 21 September 2015, http://www.infoworld.com (visited 20 September 2016).
[116] Although the US is unlikely to go through with the TPP under the Trump administration, Trump's position on protection of critical infrastructure is noteworthy. See Harriet Taylor, 'Cybersecurity Experts See Grounds for Worry in Trump's Cabinet Picks', *CNBC*, 13 December 2016, http://www.cnbc.com (visited 20 December 2016).
[117] Other provisions such as TPP Chapter 11, Annex 11B, footnote 34 and TPP art 18.80, can also be used by TPP Governments to require software manufacturers to provide their proprietary source codes. See Software Freedom Law Centre, 'TPP Article 14.17 and Free Software: No Harm, No Foul', *Software Freedom Law Centre*, 23 November 2015, https://www.softwarefreedom.org (visited 20 September 2016).

Source code is a critical 'trade secret' in digital products/services. With the escalation of cyber-espionage through hacking of websites/networks or through coordinated cyber-attacks,[118] protection of 'trade secrets' has become a key concern in the digital sector (including vital information regarding source code), as it results in 'unfair competition' in the global marketplace.[119] During the negotiation of the TPP, the USTR was pressurized by leading US companies to include criminalization of trade secret thefts in the TPP negotiating agenda.[120] In the TPP region, Vietnam was the main concern for the digital industry.[121] The US tabled the provision on trade secrets in 2012 in the TPP negotiations, but initially met with strong opposition from other TPP members.[122] Digital rights groups also expressed concern that the provision would prejudice the interests of whistle-blowers who used hacking.[123]

However, after extensive negotiations, the TPP countries agreed to include a provision on criminalizing theft of trade secrets, the first-of-its-kind in a trade agreement.[124] TPP art 18.78 provides that all persons within the TPP region will be provided with 'legal means' to safeguard trade secrets 'lawfully in their control', and cannot be 'disclosed to, acquired by, or used by others (including state-owned enterprises) without their consent in a manner contrary to honest commercial practices'.[125] TPP art 18.78.1 also states that 'trade secrets, encompasses, at a minimum undisclosed information as provided for in art 39.2 of the TRIPS'. While not referring to trade secrets as such, TRIPS art 39.2 requires signatories to protect against the disclosure of information that meets certain criteria, one of which is that the information has 'commercial value' because it is a 'secret'. The application of art 18.78 is 'without prejudice to a Party's measures protecting good faith lawful disclosures to provide evidence of a violation of that Party's law', as outlined in a footnote to art 18.78.[126] Critics have argued that this footnote is insufficient to safeguard the interests of journalists or other individuals who hack into systems to expose facts, which while not illegal, are pertinent for public scrutiny.[127] Others argued that the provision on trade secrets would force many TPP countries to develop 'draconian anti-hacking laws' such as

---

[118] David Talbot, 'Cyber-Espionage Nightmare' *MIT Technology Review*, 10 June 2015, https://www.technologyreview.com (visited 20 September 2016).
[119] The concept of 'trade secrets' is related to 'unfair competition'. See Paris Convention, art 10 bis.
[120] 'US Industry Groups Push USTR to Strengthen TPP Trade Secret Proposal' 30.10 *Inside US Trade* (9 March 2012).
[121] 'Chamber Identifies India, Thailand, Vietnam amongst Worst IPR Offender' 32.5 *Inside US Trade* (31 January 2014).
[122] 'Chamber Steps Up Efforts to Criminalize Trade Secret Thefts in TPP' 33.35 *Inside US Trade* (6 September 2013).
[123] 'US Gets Camcording Penalties, Broad Scope of Measures in the TPP' 33.40 *Inside US Trade* (16 October 2015).
[124] For further details, TPP art 18.78.3. Another example where IP infringement was criminalized was the *Anti-Counterfeiting Trade Agreement*, which was rejected by the EU.
[125] The term 'honest commercial practices' should in the minimum include practices 'such as breach of contract, breach of confidence and inducement to breach, and includes the acquisition of undisclosed information by third parties that knew, or were grossly negligent in failing to know, that those practices were involved in the acquisition'. See TPP, art 18.78.1 read with n.137.
[126] TPP, art 18.78, n 136. See also 'TPP Countries Debate Whistleblower Protections in Trade Secrets Provision' 33.31 *Inside US Trade* (7 August 2015).
[127] Jeremy Malcolm and Maira Sutton, 'Latest TPP Leak Shows US Still Pushing Terrible DRM and Copyright Term Proposals—and New Threats Arise', 16 October 2014, https://eff.org (visited 20 September 2016).

the *Criminal Fraud and Abuse Act* in the US.[128] However, these fears appear to be largely misplaced as the footnote covers 'good faith lawful disclosures'.

Some experts have argued that the provision on trade secrets has nothing to do with free trade, but is intended to 'consolidate the monopoly position of companies'.[129] Further, the scope of 'trade secret' is also important – a very broad scope of trade secrets will be inimical to promoting digital innovation, as it may include several routine business ideas that are generic to an industry. Further, hacking of products may be necessary at times to develop more secure products. The US government passed the Defend Trade Secrets Act in July 2016 to modernize their trade secrets law, including dealing with cases of misappropriation of trade secrets, and clarifying whistle-blower protection under the law.[130] It is difficult to predict whether this new provision will be effective in deterring corporate thefts, particularly when cyber-attacks can be easily executed from outside of the TPP region, and often receives complicit support of governments. Instead, measures which enable innovation in cybersecurity standards such as encryption are likely to be more meaningful in protecting proprietary source code.

4 *Enabling Innovation in Encryption Standards*

In order to develop secure and trustworthy digital products and e-commerce services, manufacturers should have freedom to innovate in cybersecurity standards, particularly encryption standards.[131] Use of end-to-end encryption in digital services enables secure and efficient cross-border data flows, and an open internet.[132] However, in the past, several countries have adopted laws that either impose direct bans on encrypted products, or set specific technical regulations that restrict the sale of encrypted products. For instance, China tried to enforce an indigenous standard for wireless networks (called WLAN Authentication and Privacy Infrastructure),[133] Vietnam banned importation and use of foreign encrypted products,[134] and Russia imposed extensive licensing requirements for foreign encrypted products.[135] In certain cases, countries also make it mandatory for foreign companies to disclose encryption keys for their products.[136] By and large, such measures create barriers to trade for companies selling their software in foreign markets, due to increase in compliance costs or delays (such as cumbersome licensing requirements or

---

[128] Ibid.
[129] Democracy Now, 'TPP Exposed: WikiLeaks Publishes Secret Trade Text to Rewrite Copyright Laws, Limit Internet Freedom', 14 November 2013 (Comments of Bill Watson (Cato Institute) and Lory Wallach (Public Citizen)).
[130] Jonathan Krause, 'Decoding the Defend Trade Secrets Act: Whistle Blowing Employees' (25 July 2016) *Privacy and Security Law Report* (online).
[131] Daniel Castro and Alan McQuinn, 'Unlocking Encryption: Information Security and the Rule of Law', Information Technology and Information Foundation, March 2016, http://www2.itif.org (visited 30 September 2016) 9, 35.
[132] Ibid 2.
[133] Sumner Lemon, 'Controversy over Chinese WLAN Standard Deepens', *MacWorld*, 10 December 2003, http://www.macworld.com (visited 20 September 2016).
[134] Draft Law on Information Security (Vietnam), Released on 22 May 2013.
[135] USTR, '2015 Report on the Implementation and Enforcement of Russia's WTO Commitments', December 2015, http://ustr.gov (visited 30 June 2016) 14, 15.
[136] See Zunyou Zhou, 'China's Comprehensive Counter-Terrorism Law', *The Diplomat*, 23 January 2016, http://thediplomat.com (visited 20 September 2016), referring to China's Counter Terrorism Law.

conformity assessment procedures), or forced disclosure of IP, or compromising security/confidentiality of their user data.

TPP directly addresses problems arising from such measures in Annex 8B, Section A.3. This provision prohibits a TPP party from 'impos[ing] or maintain[ing] a technical regulation or conformity assessment procedure' that requires companies 'as a condition of the manufacture, sale, distribution, import or use of the product' to do any of the following:[137]

> (a) transfer or provide access to a particular technology, production process or other information, for example, a private key or other secret parameter, algorithm specification or other design detail, that is proprietary to the manufacturer or supplier and relates to the cryptography in the product, to the Party or a person in the Party's territory;
>
> (b) partner with a person in its territory; or
>
> (c) use or integrate a particular cryptographic algorithm or cipher,
>
> other than where the manufacture, sale, distribution, import or use of the product is by or for the government of the Party.

This provision does not 'prevent a Party's law enforcement authorities from requiring service suppliers using encryption they control to provide, pursuant to that Party's legal procedures, unencrypted communications'.[138] This provision also does not apply to 'networks' 'owner or controlled by the government including those of central banks' or government measures related to supervision, investigation, or examination of 'financial institutions or markets'. More broadly, Annex 8-B also does not apply to financial instruments[139] – this exclusion is counterproductive as it can effectively compromise the security and integrity of encryption standards used in financial services products. It is also unclear why this exclusion was included, given that the US in particular, has taken strong objection to the requirement of mandatory encryption standards in the Chinese banking sector.[140] Within the TPP region, Vietnam has already reversed its previous approach, and has removed restrictions on import or sale of encrypted products (although certain confidential business information such as technical plans and information on standards still needs to be submitted for a business license).[141]

Unofficial reports suggest that the negotiation of Annex 8-B, Section A, was devised largely based on the inputs of industry leaders in the US.[142] Leading American tech companies such Apple, Microsoft, IBM and CISCO provided strong support for the US position on encryption standards, particularly given the security concerns regarding military control over encryption standards in

[137] TPP, Annex 8B, Section A.3
[138] TPP, Annex 8B, Section A.5.
[139] TPP, Annex 8B, n 10.
[140] Steve Dickinson, 'China Bank Technology Rules: Not the Same Old Thing', *China Law Blog*, 19 March 2015, http://www.chinalawblog.com (visited 20 September 2016).
[141] *Law on Network Information Security*, art 32.
[142] 'US Seeks to Limit Import Barriers to Encrypted Products in TPP Talks' 30.13 *Inside US Trade* (30 March 2012).

countries such as China.[143] By prohibiting TPP countries from forcing foreign and domestic companies to provide encryption keys, algorithms used in their encryption technologies, or mandating use of indigenous technologies or joint ventures resulting in forced technology transfer, TPP Annex 8B, Section A, provides an adequate response to important concerns in digital trade. Read along with TPP art 14.17.1 (see discussion in Section IIC3 above) and TPP art 2.10 (which prohibits export or import restrictions on 'commercial cryptographic goods'), the provisions have an effect of reducing governmental interference and will ultimately, contribute to making the internet a more secure and trustworthy trading platform.

D *Network Neutrality in the TPP*

Network neutrality can be simplistically understood as treating all internet traffic equally. However, network neutrality has multiple policy implications such as non-discrimination between various digital service providers/websites/apps, providing adequate quality of service to internet consumers and service providers, and preserving their right of choice between various services/digital products/technologies without interference of the network operator.[144] Network neutrality is also linked to 'permission-less innovation' as non-discrimination in internet networks provides equal opportunities to any service providers/app developers to innovate and develop a user base.[145] However, at the same time, 'network differentiation' may be sometimes necessary to facilitate both innovation and investment, particularly as the amount of data traffic has increased enormously.[146]

In the TPP, aspects of network neutrality are acknowledged in different provisions, although none of these provisions create strong legal obligations.[147] TPP art 14.10 reads on the 'Principles on Access to and Use of the Internet for Electronic Commerce' reads:

> Subject to applicable policies, laws and regulations, the Parties recognise the benefits of consumers in their territories having the ability to:
>
> (a) access and use services and applications of a consumer's choice available on the Internet, subject to reasonable network management;

[143] Ibid.
[144] Johannes M. Bauer and Jonathan A. Obar, 'Reconciling Political and Economic Goals in the Net Neutrality Debate' 30 The Information Society 1 (2014). For a discussion of the concept of 'permissionless innovation' as conceived by Cerf, see generally Adam Thierer, *Permissionless Innovation The Continuing Case for Comprehensive Technological Freedom* (Arlington: Mercatus Center at George Mason University, 2014).
[145] Ibid, 8.
[146] Ibid, 11.
[147] The TPP countries do not follow a uniform approach in domestic net neutrality policies. For instance, the US, Chile and Peru have net neutrality laws in place. Canada has a detailed legal framework for traffic prioritization that requires the government to balance the freedom of internet users with legitimate interests of ISPs vis-à-vis traffic management. Singapore also has a limited net neutrality policy in place. Since 2008, Japan has developed guidelines for packet shaping which allows for more efficient and fair management of internet traffic. On the other hand, other TPP countries such as Australia, New Zealand, Malaysia, Vietnam, and Brunei do not have any specific legal provisions that address net neutrality issues directly.

(b) connect the end-user devices of a consumer's choice to the Internet, provided that such devices do not harm the network; and

(c) access information on the network management practices of a consumer's Internet access service supplier.[148]

A plain reading of this provision suggests that (i) legal requirements in art 14.10 is subject to domestic laws of TPP countries; (ii) access and use of internet services and can be subject to 'reasonable network management' (which is not defined); and (iii) ISPs can 'offe[r] its subscribers certain content on an exclusive basis'.[149] The wording of this provision is very similar to art 15.7 in KORUS FTA – in this FTA, Korea and the US agreed in a side letter that contracts and commercial arrangements were sufficient to implement the parties' obligations, thereby undermining the importance of the provision. [150] Further, since the provision is non-binding, it does not create legal remedies for situations such as blocking or filtering of content or particular websites. The provision is also unclear regarding its application to both fixed and mobile internet services – this is particularly important as majority of population access the internet through mobile devices in developing countries. Therefore, to a large extent, the implementation of this provision only depends on the political will of a TPP country.

The Telecommunications Chapter (Chapter 13) also contains provisions related to network neutrality. Art 13.23.1 provides freedom of choice to all public telecommunications service providers for 'choosing the technologies that they wish to use to supply their services, subject to requirements necessary to satisfy legitimate public policy interests'. Any measure restricting this choice should not be 'prepared, adopted or applied in a manner that creates unnecessary obstacles to trade'. However, if the government itself finances development of advanced networks (includes broadband networks), it can impose conditions on the use of technologies that meet specific public policy interests.[151] The term 'legitimate public policy interests' is undefined, and is likely to reflect the regulatory culture of the country. However, unlike the public policy exception in TPP art 14.11.3 and 14.13.3 discussed in Section IIA2 above, TPP art 13.25 recognizes 'importance of international standards for global compatibility and interoperability of telecommunications networks and services' and also leaves open the possibility of institutional coordination with other bodies such as International Telecommunications Union. This may provide further guidance in interpretation of the exception laid down in art 13.23.1.

TPP art 13.4.3 requires all TPP parties to 'ensure that an enterprise of any Party may use public telecommunications services for the movement of information in its territory or across its borders'. This is subject to an exception that measures can be taken 'to ensure the security and confidentiality of messages and to protect the privacy of personal data of end-users of public telecommunications networks or services, provided that those measures are not applied in a manner that would

[148] Footnote omitted.
[149] TPP, art 14.10, n 7.
[150] USTR, Side letter between Korea and the US (30 June 2007).
[151] TPP, art 13.23.2 and n. 25 thereunder.

constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade in services'.[152] The relationship between these articles with provisions on data flows (art 14.11) and personal information protection (art 14.8) is unclear, although a logical conclusion is that the exception will apply when measures related to access/use of telecommunication services are taken to protect privacy or security breaches.

E *Safe Harbour for ISPs in the TPP*

ISPs are important players in the internet eco-system today. They are not only responsible for providing a channel for sharing and exchange of content via internet, but also control critical functions such as content management through the technical protocol that they deploy.[153] In the TPP, ISP is defined broadly as 'a provider of online services for the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing' that has the function of 'transmitting, routing or providing connections for material without modification of its content' or a 'provider of online services' undertaking either of these functions: (a) stores data at the direction of a user or (b) refers users to 'online location by using information location tools.'[154]

The TPP expands the scope of legal remedies and enforcement of intellectual property rights vis-à-vis ISPs, much beyond the requirements under the *Agreement on Trade-Related Aspects of Intellectual Property Rights* ('TRIPS Agreement').[155] The legal framework for 'legal remedies and safe harbour' in the TPP requires all countries to create 'legal incentives' for ISPs to 'deter' or 'take action' against 'unauthorized storage and copying of copyrighted materials'.[156] Further, the legal framework requires 'limitations' in domestic laws to 'preclud[e] monetary relief against Internet Service Providers for copyright infringements that they do not control, initiate or direct, and that take place through systems or networks controlled or operated by them or on their behalf'.[157] The ISPs are required to 'expeditiously remove or disable access to material residing on their networks or systems' that infringes copyright once they have received information or knowledge regarding such infringement or where there are 'facts or circumstances from which the infringement is apparent' such as when they receive a notice (popularly referred to as the 'notice and takedown mechanism').[158]

---

[152] TPP, art 13.4.4.
[153] Mike Zajko, 'Telecom Responsibilization: Internet Governance, Surveillance, and New Roles for Intermediaries' 41 (1) Canadian Journal of Communication 75 (2016), at 90; Laura DeNardis, *The Global War on Internet Governance* (New Haven: Yale University Press, 2014) 9-11.
[154] TPP, art 18.81 read with art 18.82.2.
[155] *Marrakesh Agreement Establishing the World Trade Organization*, opened for signature 15 April 1994, 1869 UNTS 299 (entered into force 1 January 1995) annex 1C ('*Agreement on Trade-Related Aspects of Intellectual Property Rights*') ('TRIPS Agreement'), art 41.
[156] TPP, art 18.82.1(a).
[157] TPP, art 18.82.1(b)
[158] TPP, art 18.82.3(a)

As long as the action of removal of content by ISPs is done in 'good faith', no legal liability arises for the ISPs, if the person posting the infringing content has been notified (also called the 'safe harbour').[159] This is problematic as many ISPs are unlikely to review each and every takedown notice.[160] The TPP does not address this deficiency, and only provides a limited and discretionary legal recourse to aggrieved persons through a system of counter-notices.[161]

After extensive negotiations, the TPP parties agreed to make an exception for 'notice and notice' mechanism (which is only followed in Canada)[162] and the existing notification system followed by Chile.[163] Other countries such as Brunei, Malaysia, Mexico, New Zealand and Vietnam do not have such a system in place, and are mostly likely to adopt a 'notice and takedown' mechanism to comply with these provisions. The 'notice and takedown' mechanism, has often been criticized by the internet community, and effectively, violates recommendations in human rights law to leave content removal issues on the internet to a court or an independent body, and not a private body such as an ISP.[164]

Several aspects of the implementation of the legal framework in the TPP on 'legal remedies and safe harbour' are also unclear. Can provisions on ISP liability be implemented without breaching privacy obligations? What happens when ISPs conduct deep packet inspections and deliberately discriminate against/monitor certain kinds of data flows (for example, from specific service providers)?[165] TPP art 18.82.7 states the legal procedures for administering ISP liability should be 'consistent with the principles of due process and privacy'; however, the same provision enables a 'a copyright owner that has made a legally sufficient claim of copyright infringement to obtain expeditiously from an Internet Service Provider information in the provider's possession identifying the alleged infringer, in cases in which that information is sought for the purpose of protecting or enforcing that copyright'. Therefore, art 18.82.7 does not reconcile privacy requirements with legal procedures for handing over personally identifiable information of an internet user from ISPs to a copyright owner. The above provisions on ISPs require consideration of two particularly important policy challenges when TPP countries implement the required legal framework domestically: (a) to maintain proportionality and balance in how content is removed for copyright infringement, and how affected parties can appeal wrongful removal of content; and

[159] TPP, art 18.82.3(b)
[160] Flynn, above n. 36, 202. See also Jonathan Band, 'SOPA-TPP Nexus' 28 American University Law Review 31(2012).
[161] TPP, art 18.82.4.
[162] TPP, Annex 18-E.
[163] TPP, Annex 18-F.
[164] Urs Gasser and Wolfgang Schulz, 'Governance of Online Intermediaries: Observations from a Series of National Case Studies', Berkman Center Research Publication No. 2015-5 (18 February 2015) 8. See also Electronic Frontier Foundation, 'The Impact of Trade Agreements on Innovation, Freedom of Expression and Privacy: Internet Service Providers' Safe Harbors and Liability**',** https://www.eff.org (visited 10 December 2016)**.**
[165] See also discussion on net neutrality in Section IID above.

(b) that ISPs do not become 'choke-points' for governmental control over data flows and content control, thus disrupting the very basic goal of a free, open and trustworthy internet.[166]

III EVALUATING THE ROLE OF TPP IN THE INTERNET ECOSYSTEM

The preceding discussion in Section II suggests that the implementation of the TPP entails difficult policy challenges in striking the right balance between liberalization in digital trade and the fundamental policy goals in internet governance such as data protection/privacy, cybersecurity, net neutrality, maintaining an undivided internet etc. In this section, I use the preceding discussion in Section II as a basis to develop an assessment of whether the TPP is a case of synergy or disjuncture with the internet ecosystem. The term 'synergistic alliance' refers to synergy between trade disciplines and the internet ecosystem i.e. when trade rules do not interfere with goals of internet policy, while facilitating digital trade. The term 'uneasy liaison' refers to disharmony between trade disciplines and the internet ecosystem i.e. when provisions in trade agreements intrude into/ adversely affect internet policy-making while attempting to create rules that facilitate digital trade. In undertaking this assessment, it is also important to consider the extent to which specific internet policy issues are relevant to digital trade liberalization.

On the positive side, the TPP can be considered to be a significant improvement over previous FTAs and WTO agreements dealing with digital trade issues. The TPP facilitates free data flows and prohibits data localization policies, which benefits the development of digital trade, improves opportunities for innovation, and helps maintain a free, open and undivided internet. The TPP also takes a positive step by precluding governments from imposing onerous and disproportionate compliance requirements to engage in digital trade, such as by prohibiting forced disclosure of source code and encryption keys. The TPP recognizes important goals for an undivided and secure internet such as network neutrality, importance of cybersecurity, regulation of spam, and online consumer protection. As a result of these provisions, TPP countries will be compelled to adopt at least some basic legal frameworks on online consumer protection, privacy and spam.

However, the provisions in the TPP do not strike a balance between promoting certain important policy goals beneficial for tech companies (such as free flow of data, prohibition of data localization, ban on forced disclosure of source code and encryption keys etc) and important goals of internet policy (such as protection of privacy, guaranteeing security of data flows, protection of rights of online users, non-discriminatory access to content for all users etc). This imbalance may have resulted from excessive influence of the US digital industry in the TPP negotiations and the lack of any input from internet multistakeholder bodies at the stage of negotiations. For instance, why should a country be under a legal obligation to allow data flows without corresponding obligations in relation to privacy and cybersecurity?[167] Why should internet users feel safe to use

[166] See Andrei Robachevsky et al, 'The Danger of the New Internet Choke Points', Internet Society, February 2014, https://www.internetsociety.org (visited 30 September 2016) 6, 7.
[167] See for eg, the EU has taken this position in the TISA negotiations. Brett Fortnam, 'EU Hopes to Table Language on Data Flows by Next TISA Round' 34.40 *Inside US Trade* (13 October 2016).

digital services, when ISPs have disproportionate influence in monitoring their content, and when non-discriminatory access to digital services is not guaranteed? What happens when TPP countries have conflicting views on how to manage cybersecurity or privacy risks? What policy goals will be considered 'legitimate' in that context?

The TPP reveals the complex relationship between trade and internet policy issues. Trade agreements are not equipped to deal with the above dilemmas in internet policy, which largely fall outside its expertise. Cybersecurity, net neutrality, and privacy/data protection mechanisms are essential to enable free data flows. However, given the lack of international consensus on these internet policy issues, the TPP understandably adopts a weak mechanism to deal with these issues, while still requiring mandatory cross-border data flows. As a result, the legal impact of these provisions on internet policy-making tends to be unclear at best and counterproductive at worst. Further, some of the discussed provisions either appear to have a weak connection to digital trade liberalization (for instance, how does criminalization of corporate trade secrets help in digital trade liberalization?) or present weak outcomes for promoting digital trade (for instance, the lack of a mandatory requirement for countries to adopt an online e-commerce dispute mechanism).

The TPP also fails to tie in many of the key provisions on digital trade with realities in the internet economy – for example, as discussed in Section IIC1, the TPP fails to establish sufficient connections between consumer protection, cybersecurity and digital trade. The ambiguous wording of the exceptions to data flows creates regulatory uncertainty, making it harder for governments to determine whether certain measures taken for domestic regulatory goals meet the threshold requirement for 'legitimacy' under the exception. The wholesale import of GATT/GATS related language in the exceptions without identifying policy objectives specific to the new digital economy and the internet governance space is inutile. These exceptions grant excessive discretion to TPP tribunals to assess regulatory measures of a country. As discussed earlier, this is likely to result in either blind deference to regulatory goals of a country or intrusive judicial activism. The internet community is, therefore, very critical of how TPP tribunals will decide future disputes relating to such measures.

While the TPP provides avenues for regulatory cooperation for important issues such as cybersecurity, online consumer protection, net neutrality etc., the established mechanism is mostly voluntary in nature. In such a scenario, the level of engagement would depend on the political will of the countries, and possibly, the consensus of powerful lobbies. The TPP, for instance, provides no mandatory mechanism for countries to provide support to SMEs to achieve compliance with complicated regulatory requirements. The TPP also does not acknowledge the important role of multistakeholder bodies in the internet community in achieving collaboration on several of these issues. These bodies could have not only played an important role at the stage of negotiations, but also as external experts during disputes, and as platforms for collaboration among TPP countries. For all the reasons discussed above, I conclude that the TPP is currently in a state of 'uneasy liaison' with the internet economy, and these deficiencies within the TPP need to be better addressed to create synergies between trade disciplines and the broader internet ecosystem.

Based on this study of the TPP, three key factors stand out with respect to how issues/rules related to digital trade should be addressed: (i) rules on digital trade should specifically address issues directly related to reduction of barriers to trade or facilitating trade flows; (ii) these rules should preserve and enhance opportunities for innovation by tech companies and internet users at large; and (iii) these rules should be geared towards building the trust of the consumer/internet users. These three factors are indivisibly linked, and would together result in a 'synergistic alliance' between trade rules and the broader internet ecosystem. In practice, it may not always be easy to formulate appropriate rules that achieve all these three goals, particularly given, (i) the lack of consensus amongst countries on achieving policy outcomes such as digital innovation and building consumer trust, and (ii) the limited understanding of the connection between trade and internet policy. However, these factors, may serve as a useful benchmark in assessing both the extent to which certain issues are appropriate in a trade agreement, and the manner in which the trade agreement deals with these issues.

Whether or not the TPP comes into force, it presents an important lesson for trade lawyers, i.e. to take a step back and involve the internet community in areas where their expertise is necessary and appropriate. To that extent, a higher degree of transparency in negotiation of trade agreements is vital and meaningful. The transparency initiative taken by the EU in the TTIP negotiations is a welcome development, as it provides a chance to the internet community to study the country position and provide valuable and timely inputs. As the WTO embarks on exploring the 21st century digital trade issues in its coming meeting,[168] it has an opportunity to take a more informed and transparent approach in setting digital trade rules. The same holds true for other ongoing negotiations at the TISA and the TTIP.

IV CONCLUSION

A study of the TPP represents more generally several of the policy challenges before trade agreements dealing with contemporary issues of the digital economy. The TPP, as discussed in Section III, does not effectively fit into the broader internet ecosystem, as it fails to synergize the goal of trade liberalization with important internet policy concerns such as facilitating consumer trust and digital innovation. Effective digital trade is premised on the existence of a well-functioning internet which is free, open, and secure. The key lesson that can be derived from the TPP is that trade agreements should either preserve these core values of the internet or in the very least, not interfere with them. While making an assessment regarding the suitability of policy areas within the domain of trade agreements addressing digital trade issues, three factors will be critical – the extent to which rules related to those areas are related to digital trade liberalization, and the impact of the rules on consumer trust and digital innovation.

In practice, synergizing trade and internet policy goals is not always easy, given that trade lawyers/negotiators do not always understand how provisions in trade agreements affect internet

[168] 'Azevêdo Urges WTO Members to Deepen Engagement for MC11 Outcomes', *Bridges Africa*, 7 October 2016, http://www.ictsd.org (visited 30 November 2016).

policy, and because of the ideological conflict between countries/institutions on appropriate standards for internet policy issues such as privacy, cybersecurity, net neutrality, online consumer protection, and so on. In light of such complex policy environment, in the negotiation/implementation of trade agreements such as the TPP, the best approach possible is for countries to identify and implement regulations necessary for suitable and effective trade liberalization in the digital sector, as well as take 'good faith' measures towards building cooperation mechanisms in those areas.[169] In this process, countries should maintain transparency regarding their negotiating positions to the greatest extent possible, as well as appropriately engage with the expertise of the internet technical/policy community.

Conclusively, the significance of internet-related policy issues in digital trade can also be understood through the assessment of a scenario where governments do not commit to 'new' provisions on digital trade (such as data flows, data protection, security etc.). Uncertainties regarding openness and security of digital data flows is detrimental to digital trade, as it stifles innovation, reduces consumer confidence, and thereby, reduces opportunities for offering digital services on a global internet marketplace. It is possible to argue that GATS disciplines may be applicable, at least to some regulatory barriers to digital data flows – however, considerable legal and political uncertainty exists regarding whether a country could successfully pursue such a case before the WTO.[170] Further, despite the presence of GATS disciplines, the extent of protectionism in the digital industry is increasing in the recent years,[171] through adoption of policy measures related to the internet such as the rapid increase in data localization policies,[172] forced imposition of technical standards related to data security/protection,[173] and arbitrary blockage/surveillance of internet services across countries.[174] Whether all aspects of these policy measures can be addressed in a trade agreement is debatable. However, at least, to some extent, trade agreements will remain instrumental in addressing several of these 'newer' policy measures to negate the wave of protectionism pervasive in the digital sector today – therefore, developing 'synergistic alliance' between trade law and internet policy will continue to be a central policy consideration in the coming years.

---

[169] See Aaronson, above n 104.

[170] See for eg, 'USTR Unsure WTO Challenge of Chinese Firewall Would Succeed' *Inside US Trade* (17 June 2016); Sarah Joseph, *Blame it on the WTO? A Human Rights Critique* (Oxford: Oxford University Press, 2013) 138-40. Contra, Daniel Crosby, 'Analysis of Data Localization Measures under WTO Services Trade Rules and Commitments', Policy Brief, E15Initiative (March 2016), http://e15initiative.org (visited 20 December 2016).

[171] See generally, USTR, 'Fact Sheet: Key Barriers to Digital Trade', Press Release, March 2016, https://ustr.gov (visited 20 December 2016).

[172] See generally, Albright Stonebridge Group, 'Data Localization: A Challenge to Global Commerce and the Free Flow Of Information', September 2015, http://www.albrightstonebridge.com (visited 20 December 2016).

[173] See text accompanying nn 133 to 136 above.

[174] Darell M West, 'Internet shutdowns cost countries $2.4 billion Last Year' (Centre for Technology Innovation at Brookings, October 2016) 1, 3-5; Shaun Walker, 'Russia Blocks Access to LinkedIn over Foreign-held Data', *The Guardian*, 16 November 2016, https://www.theguardian.com (visited 20 December 2016).