

Trans - Pacific Partnership (TPP) and Data Protection Issues: Is it a Unique and Modern 21st Century Agreement?

Abu Bakar MUNIR*

Introduction

The Trans-Pacific Partnership Agreement (TPPA) was signed in Auckland, New Zealand on 4 February 2016. All twelve parties to the TPP are APEC member economies which four of them are also Member States of the Association of Southeast Asian Nations (ASEAN). Three more ASEAN members – Indonesia, Thailand and the Philippines have expressed their interest to join the TPP. Many have argued that the TPP is an initiative to counter balance the emergence of China in the world economy. The US President, Barack Obama, after the agreement was reached in Atlanta on 5 October 2015, said.¹⁾

When more than 95 percent of our potential customers live outside our borders, we can't let countries like China write the rules of the global economy. We should write those

* Professor, Faculty of Law, University of Malaya

1) <https://www.whitehouse.gov/the-press-office/2015/10/05/statement-president-trans-pacific-partnership>

rules, opening new markets to American products while setting high standards for protecting workers and preserving our environment.

Promoted as a unique and modern “21st century agreement”, the TPPA has five defining features: (i) comprehensive market access, (ii) regional approach to commitments, (iii) addressing new trade challenges, (iv) inclusive trade and (v) platform for regional cooperation.²⁾ The TPP includes 30 chapters covering trade and trade-related issues with the goal to “promote economic growth; support the creation and retention of jobs; enhance innovation, productivity and competitiveness; raise living standards; reduce poverty in our countries; and promote transparency, good governance and enhanced labor and environmental protections.”³⁾ Chapter 14 of the TPPA on electronic commerce contains some provisions concerning privacy and data protection, which is the focus of this paper. These provisions, namely Articles 14.8, 14.11 and 14.13, are critically analyzed to assess their impact on privacy and data protection. It is also aimed at determining the obligations imposed by the agreement on the member countries should it be implemented.

Personal Data Protection: The Weakest Link?

Article 14.8.2 paragraph 2 of the TPPA states that:

2) See the United States Trade Representative (USTR), “Summary of the Trans-Pacific Partnership Agreement” available at <https://ustr.gov/about-us/policy-offices/press-office/press-releases/2015/october/summary-trans-pacific-partnership>, visited on 4 March 2016. The BBC regarded it as one of the most ambitious free trade agreements ever signed. See BBC News, “TPP: What is it and why does it matter?” available at www.bbc.com/news/business-32498715, visited on % March 2016.

3) *Ibid.*

Each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce. In the development of its legal framework for the protection of personal information, each Party should take into account principles and guidelines of relevant international bodies.

Unfortunately, this provision is subject to a footnote which diluted the impact of the provision. Footnote 6 states, “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.** This last clause seems to be written with the USA’s Federal Trade Commission in mind⁴⁾ recognizing the diversity of the legal approaches to privacy protection across the TPP economies from the sectoral approach of the United States to the omnibus laws in countries such Malaysia, Singapore, Australia, New Zealand, etc.

Graham Greenleaf argues that “Given that a ‘legal framework’ is required, mere self-regulation would not appear to be sufficient.” However, he further argues that since a ‘measure’ is defined to include ‘any...practice (Article 1.3), as well as laws, even this is not completely free from doubt.⁵⁾

Debatably, the footnotes effectively means that the TPP’s privacy

4) See Graham Greenleaf, “The TPP & Other Free Trade Agreements: Faustian Bargains for Privacy”, available at file:///C:/Users/user/Downloads/SSRN-id2732386%20(1).pdf, visited on 4 March 2016.

5) Ibid.

requirements can be met without the need for a law at all.⁶⁾ Enforcing voluntary undertaking is not a privacy law, it is an anti-fraud approach that requires companies to be truthful about their privacy promises. If the law does not feature specific requirements for the consent, use, and disclosure of personal information, it is not a privacy law.⁷⁾ The TPP weakens global privacy protections by failing to establish a minimum privacy law standard and then makes matters worse by limiting the ability for member countries to establish some additional safeguards. Article 14.8.2 adopts an inert mechanism for privacy which does no more than require the presence of a legal framework for protecting privacy, seemingly allowing the U.S's patchwork approach to persist.⁸⁾

As provided for in Article 14.8.2, each State party is required to take into account principles and guidelines of relevant international bodies in developing its legal framework to protect personal data. Graham Greenleaf argues:⁹⁾

However, no specific international instruments are mentioned, and there is no list of principles included in the TPP. Nor are any specific enforcement measures mentioned. These absences make the 'legal framework' required by the Article completely nebulous. These content

6) Michael Geist, "The Trouble with the TPP, Day 11: Weak Privacy Standard", available at <http://www.michaelgeist.ca/2016/01/the-trouble-with-the-tpp-day-11-weak-privacy-standards/>, visited on 4 March 2016.

7) Ibid.

8) See the Canadian Internet Policy and Public Interest Clinic (CIPPIC), "The Highlights of the Trans-Pacific partnership E-Commerce Chapter", available <https://www.citizen.org/documents/tpp-e-commerce-chapter-analysis.pdf>, visited on 4 March 2016.

9) *Supra* n. 4.

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

As mentioned above, since all twelve TPP members are APEC Member Economies, it is reasonable to assume that one of the sources for the principles and guidelines is the APEC Privacy Framework. However, the APEC Framework is widely recognized as providing weak protection for individual privacy.¹⁰⁾ In reality, many APEC Member Economies have adopted domestic legislation which is stronger than the APEC Privacy Framework. Perhaps, only Brunei and Vietnam which have yet to have a data protection law can take the benefit of this provision.

The further note to Article 14.8 provides that “Brunei Darussalam and Vietnam are not required to apply this article before the date on which that party implements its legal framework that provides for the protection of personal data of the users of electronic commerce”. The question that need to be asked is; what about the TPP’s ten remaining member economies – do their existing legal frameworks meet the requirements of the article?

Cross - Border Data Transfer: Balancing Privacy and Trade

It is recognized that the movement of information across national borders drives today’s global economy. Cross-border data transfers allow businesses and consumers access the best to the best available technology and services, wherever those resources may be located around the world.¹¹⁾ The seamless transfer of information is as

10) Supra n. 8.

11) See U.S Chamber of Commerce, “Business without Borders: The Importance of Cross-Border Data Transfers to Global Prosperity,” available at <https://www.>

critically important as it is inexorably linked to the growth and success of the global economy.¹²⁾ On the other hand, personal information of customers need to be protected. Striking the right balance between these two, however, is not easy.

The increasing presence of free flow of information language within the e-commerce chapter of trade agreements should not be a surprise, as one can construct the idea of cross-border flow of valuable data as “trade,” but it still deserves careful consideration and construction, as this is not oil, or bananas, or sugarcane. This data is not abstract – it is about people. Referring to it in purely economic terms typically elides or avoids that inconvenient truth.¹³⁾

According to the Consumers International, during the TPPA negotiations, there is no record of “free flow of information” discourse being used by the TPPA-member countries other than the US.¹⁴⁾ The US has incorporated this discourse into the foreign policy of both the US Department of State and the US Trade Representative (USTR). The USTR has said, for example, that the US wants TPP partners “to agree to not to prevent the free flow of data across borders”. This is important in particular for e-commerce companies and cloud companies, which are both key drivers in US markets and

huntonprivacyblog.com/files/2014/05/021384_BusinessWOBorders_final.pdf, visited on 5 March 2016.

12) Ibid.

13) See Consumers International, “Information Flow and Trade Agreements: History and Implications for Consumers’ Privacy”, available at http://a2knetwork.org/sites/default/files/tpp_and_free_flow.pdf, visited on 16 March 2016.

14) Ibid.

strong influencers of US policy.¹⁵⁾

Although the US trade agreements have long included language related to e-commerce, the US and Republic of Korea were the first states to include principles related to Internet openness and Internet stability in the electronic commerce chapter of the Korea/US Free Trade Agreement (KORUS).¹⁶⁾ The two countries agreed to encourage the free flow of information. Article 15.8 of the KORUS states; “Recognizing the importance of the free flow of information in facilitating trade and acknowledging the importance of protecting personal information, *the Parties shall endeavor to* refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders.”

Since the terms used are “shall endeavor to”, arguably, that provision is not binding. This has raised protests from the US corporations, which look for stronger, legally binding language that would empower them to enforce free trade obligation against local privacy protection. Interestingly, what the US did not manage to get from a country, she managed to get in from a group of eleven countries. The TPPA employs stronger terms than the terms in the KORUS. Article 14.11.2 of the TPPA provides:

Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a

15) Ibid.

16) See Elliot School of International Affairs (The George Washington University) and MacArthur Foundation, “Trade and the Internet: The Challenge of the NSA Revelations Policies in the US, EU, and Canada,” available at http://www.gwu.edu/~iiep/assets/docs/papers/Aaronson_Maxim_Trade_Internet.pdf, visited on 11 March 2016.

covered person.

More interestingly, the TPPA in the first paragraph of this Article recognizes that each Party may have its own regulatory requirements concerning the transfer of information by electronic means. Makes no mistake – this provision should not be interpreted as an exception that can override the substantive obligation in the subsequent provision of Article 14.11.2.

The usage of the word “shall” obligates the TPP member economies to ensure the free flow of information including personal data across their borders. Remarkably, the draft of the TPPA is very much like the provision in the KORUS which simply says, “Parties shall refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders.”

Carl Schonander, the Director of International Public Policy at the Software & Information Industry Association (SIIA) states that article 14.11 on “Cross-Border Transfer of Information by Electronic Means” is perhaps the core element in the new digital trade architecture forged by TPP. Article 14.11.2, according to him, “... gets to the heart of what the TPP negotiators have achieved” and it is groundbreaking in trade terms.¹⁷⁾ Meanwhile, the Canadian Internet Policy and Public Interest Clinic (CIPPIC) asserts that this provision grants businesses the freedom to outsource data storage and processing to any other TPP jurisdiction without limitation.¹⁸⁾

During the negotiation process, the US encountered significant

17) See Carl Schonander, “Text Release Shows TPP Countries Get Cross Border Data Flows Right”, available at <http://www.siia.net/blog/index/Post/62751/Text-Release-Shows-TPP-Countries-Get-Cross-Border-Data-Flows-Right>, visited on 5 March 2016.

18) *Supra* n. 8

opposition on this free flow provisions because of the different approaches adopted by the US and other countries in protecting privacy and personal data.¹⁹⁾ As mentioned earlier, the US wanted to ensure data can flow freely across borders with only narrow exceptions. However, Australia, New Zealand, and Canada have made protection of privacy rather than the flow of information a top priority for international rules governing cross border information flows.²⁰⁾ Australia attempted to table alternative language to ensure that this data flow provision would be consistent with its privacy law which has received support from a number of countries. The US responded to the Australian demands by proposing a more ad hoc strategy, which adheres to the APEC Privacy Framework.²¹⁾

As mentioned earlier, the TPPA in Article 14.8.2 requires each state Party to adopt a legal framework to protect privacy and personal information. The question is how this Article should be reconciled with Article 14.11.2. On the one hand, the TPPA requires the member states to have a data protection legal framework, on the other, they should allow the cross-border transfer of data. Should Article 14.11.2 be interpreted to mean that member states should allow cross-border of data to a country or territory regardless of whether the said country provides an adequate level of protection? Burcu Kilic, a policy director with the Public citizen's information society programme said:²²⁾

19) Supra n. 13.

20) Ibid.

21) Ibid.

22) See Public Citizen Press Room, "TPP Text Reveals Risk for Consumer Privacy Reform," available at <https://www.citizen.org/pressroom/pressroomredirect.cfm?ID=5723>, visited on 11 March 2016.

Through these provisions in the TPP, the United States appears to be moving to limit policy options for safeguarding privacy across borders, even while the European Union moves to expand them. The TPP could limit the ability of the United States and other countries to follow Europe's path, or to protect privacy by conducting the movement of data across borders in compliance with the host country's privacy rules for personal information. The memory of misuse of data and National Security Agency surveillance is so fresh, and we should be careful about giving up control of our data.

On the secondary issue, the TPPA does not define "for the conduct of the business." This could leave the door open for a broad interpretation that could encompass a wide variety of purposes. The financial services industry is not covered by the cross-border data rules and Australia has been given an exemption for medical records. On the impact of this free flow of data provision on privacy protection, the Consumers International remarks:²³⁾

Countries involved in the TPPA negotiations have significant differences in the level of protection they provide to personal information. Applying the methodology used in a 2005 U.S. government study to updated information on protection to consumers' privacy among TPPA countries, we find that: for consumers in countries with higher level of protection to privacy (such as Canada, New Zealand, Mexico, and Peru), the free flow of information may imply a significant risk of defeating their domestic privacy poli-

23) *Supra* n. 13.

cies by exporting data to countries with lower or no protection. Even for consumers in countries that provide some protection (such as the U.S. and South Korea), there is a risk of allowing exportation of their information to overseas facilities in countries with uncertain protections for their privacy.

Oddly, on 12 January 2016, the US Representative Mike Kelly (R-PA) – a member of the House Ways and Means Subcommittee on Trade together with other 63 Members of Congress sent a bipartisan letter to the Obama Administration expressing their concern with the data flow and data localization provisions in the TPP which excludes the financial services companies. The letter states, “As in every sector, US financial services companies depend on the free flow of data to run operations on a global basis. ...Omission of these disciplines in the TPP is a missed opportunity to ensure that all US companies benefits from strong rules prohibiting localization requirements. We note that such disciplines can be included in trade agreements while maintaining the ability of US regulators to protect consumers through prudential regulations.”²⁴⁾

Simply put, these US Congressmen are saying that what the US has gotten is not enough. The lawmakers argued that banking, insurance and securities industries are not different from other sectors that depend on the unimpeded flow of data to keep their businesses running in vast global market place. They wrote, “We request that your agencies use available measures to address the existing gaps

24) The letter is available at <http://kelly.house.gov/sites/kelly.house.gov/files/documents/Kelly%20Paulsen%20Moulton%20Kuster%20Data%20Localization%20Letter%20to%20USTR%20Treasury%20NEC%20SIGNED%201-11-2016.pdf>, visited on 16 March 2016.

in the TPP.”²⁵⁾

Prohibition on Data Localization: The First of Many in the Future?

The TPPA in Article 14.13.1, on the one hand, recognizes that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications. Article 14.13.2 on the other hand, provides that no party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory. This provision is inter-related with the free flow of data discussed earlier. Data localization restricts data flow because companies would be forced to invest in additional data centers. The TPPA seeks to give the freedom to companies to choose where to store their data and they can transfer data collected in that Party's borders to their servers at home or wherever.

According to the US Trade Representative (USTR), this is the first US free trade agreement ever to include an explicit commitment against forced localization of computing facilities. Many argue that the restriction on data localization originates from the Silicon Valley tech company frustration with a growing number of governments that want local data to remain within their jurisdiction.²⁶⁾ The USTR claims that localization requirements are trade protectionist strategies that disadvantage foreign goods, services, or IP compared to domestic goods, and has long considered any requirements to

25) Ibid.

26) See e.g. Michael Geist, “How the TPP Puts Canadian Privacy at Risk,” available at <http://www.michaelgeist.ca/2015/10/how-the-tpp-puts-canadian-privacy-at-risk/>, visited on 15 March 2016.

use local network infrastructure or local servers as non-tariff barriers that amount to discriminatory restrictions on trading rights.²⁷⁾ The US also feels that localization requirements would undermine the advantage currently enjoyed by US cloud-based services, since most, if not all, corporations that utilize cloud-based services are currently located in the US.²⁸⁾ By having this ban on data localization, the US managed to get what she wanted from other TPP member states.

In reality, as Professor Michael Geist has said, “Data localization has emerged as an increasingly popular legal method for providing some additional assurances about the privacy protection for personal information. Although heavily criticized by those who fear that it harms the free flow of information, requirements that personal information be stored within the local jurisdiction is an unsurprising reaction to concerns about the lost privacy protections if the data is stored elsewhere.”²⁹⁾ Data localization requirements are popping up around the world with European requirements in countries such as Germany, Russia, and Greece; Asian requirements in Taiwan, requirements in Brazil. Canada has not been immune to the rules either with both British Columbia and Nova Scotia creating localization requirements for government data.³⁰⁾

In contrast, the USTR states that, “The cloud should be global,

27) *Supra* n. 8.

28) *Ibid.*

29) Michael Geist, “The Trouble with the TPP, Day 12: Restricting on Data Localization Requirements, available at <http://www.michaelgeist.ca/2016/01/the-trouble-with-the-tpp-day-12-restrictions-on-data-localization-requirements/>, visited on 16 March 2016.

30) *Ibid.*

and you should be able to choose where you store your data. We have already seen a troubling trend of countries practicing “digital protectionism”, and trying to make keeping data onshore the cost of doing business. That is not just costly for small business, it will also have the effect of leaving countries behind. TPP prevents those kinds of arbitrary requirements.”³¹⁾ Further, according to the USTR, TPP ensures that companies can locate servers where they choose based on cost, efficiency, and security, rather than being subject to forced localization rules that raise costs and reduce the efficiency of investment.³²⁾

Exceptions to the Data Flow and Data Localization Requirements: An Illusion?

There are a number of exceptions allowed by the TPPA. Under Article 14.2.3, the exceptions are: (i) government procurement, or (ii) information “held or processed by or on behalf of a Party, or measures related to such information, including measures related to its collection.” These could be significant exclusions and might, for instance, allow TPP governments to require that processing or storage of government data occur on domestic computing facilities.

The financial institutions are also excluded. The definition of “covered person” in Article 14.1 excludes “financial institution[s]” and any “cross-border financial service supplier of a Party” as defined in Chapter 11 (Financial Services). The financial institutions will be forced to rely on the commitments specifically applicable to financial service suppliers set forth in Chapter 11 and other chapters of the

31) See the USTR’s Fact Sheet, “Trans-Pacific Partnership”, available at <https://ustr.gov/sites/default/files/TPP-Promoting-Digital-Trade-Fact-Sheet.pdf>, visited on 16 March 2016.

32) Ibid.

TPP. As mentioned earlier, this has led some lawmakers in the US expressed their concern and sent a letter to the Obama Administration.

Another exception is in relation to the national security as provided for in Article 29.2(a). It states that nothing in the TPP, including Chapter 14, precludes a Party from applying measures that “it considers necessary for the fulfillment of its obligations with respect to the maintenance or restoration of international peace or security, or the protection of its own essential security interests.” Historically, security exceptions based on similar text often have been considered to be largely self-justifying, under the view that they can be invoked by a Party whenever “it considers” the exception to apply. This could make it difficult for Parties to challenge measures that facially violate one or more Chapter 14 commitments, but which a Party justifies as necessary to protect national security.³³⁾

The TPPA also incorporated the General Agreement on Trade in Services (GATS) exception into Chapter 14. This is specifically provided for in Article 29.1.3 which states that paragraphs (a), (b), and (c) of Article XIV (General Exceptions) are incorporated into and made part of this Agreement, *mutatis mutandis*. These GATS paragraphs permit measures necessary to protect public morals or maintain public order; protect human, animal, or plant life or health; or to secure compliance with laws or regulations that are not inconsistent with the GATS. The exceptions are provided for in Articles 14.11.3 and 14.13.3 which are similar, words for words. Article 14.11.3, concerning free flow of data states:

33) See Marty Hansen and Gabriel Slater, “The TPP’s Electronic Commerce Chapter,” Covington Global Policy Watch, available at <https://www.globalpolicywatch.com/2015/11/the-tpps-electronic-commerce-chapter/>, visited on 23 March 2016.

Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:

- (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and
- (b) does not impose restrictions on the transfers of information greater than are required to achieve the objective.

As for the data localization exception, the words “transfers of information” in (b) are replaced by “on the use or location of computing facilities.” The TPPA defines “measure” to include any law, regulation, procedure, requirement or practice. Comparatively, the GATS adopted a very specific but broad definition in its Article XXVIII (a) which provides that “measures” means any measure by a Member, whether in the form of a law, regulation, rule, procedure, decision, administrative action, or any other form.

The exceptions mean that in certain circumstances the member states may deviate from their obligation to ensure the free flow of data. A State party may also impose data localization provided the conditions can be satisfied. The USTR notes that the General Exceptions of chapter 14 ensures that the United States and the other TPP Parties are guaranteed the full right to regulate in the public interest, including for national security and other policy reasons.

The measure adopted by the country, however, must be undertaken: (i) to achieve a legitimate public policy objective, (ii) it is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination, (iii) it is not applied so as to be a disguised

restriction on trade, (iv) it does not impose restrictions on transfers of information greater than are required to achieve the objective or it does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective. There is a need to be emphasized here that it is not just public policy objective but “legitimate public policy objective.” The Party would have to justify the public policy objective is legitimate if it is challenged in dispute. Besides, the Party must also justify the other conditions mentioned above.

The CIPPIC states that this exception appears to be difficult to use and insufficient to protect the policies, laws and regulations that Parties have or may have in the future to safeguard privacy.³⁴⁾ The language has many layers of qualifications, which are similar to the general exceptions adopted in Article XIV of the GATS³⁵⁾. However,

34) *Supra* n. 8.

35) Article XIV of the GATS – “Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures:

- a) necessary to protect public morals or to maintain public order,
- b) necessary to protect human, animal or plant life or health; c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to:
 - i) the prevention of deceptive and fraudulent practices or to deal with the effects of a default on services contracts;
 - ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts; iii) safety;
- d) inconsistent with Article XVII, provided that the difference in treatment is aimed at ensuring the equitable or effective imposition or collection of direct

according to the CIPPIC, there is a key different: while the GATS provision allowing exceptions in the absence of discrimination or trade restrictions are included in the chapeau, the TPPA encodes the exception independently, placing the burden of showing that the measure meets all of its requirements on the government taking the measure.³⁶⁾

According to the Public Citizen, “The exceptions language for the TPP is based on the same construct used in Article XX of the World Trade Organization’s (WTO) General Agreement on Tariffs and Trade (GATT) and Article XIV of the GATS. This is alarming, as the GATT and GATS exceptions have only ever been successfully employed to actually defend a challenged measure in one of 44 attempts. That is, the exceptions would, in fact, not provide effective safeguards for domestic policies.³⁷⁾ In other words, the exceptions are illusory since the requirements are so complex (each aspect must be met) that countries relying on the exception have failed in 43 out of 44 cases.³⁸⁾

taxes in respect of services or service suppliers of other Members;

e) inconsistent with Article II, provided that the difference in treatment is the result of an agreement on the avoidance of double taxation or provisions on the avoidance of double taxation in any other international agreement or arrangement by which the Member is bound.

36) *Supra* n. 8

37) See Public Citizen, “Only One of 44 Attempts to Use the GATT Article XX/GATS Article XIV “General Exception” Has Ever Succeeded: Replicating the WTO Exception Construct Will Not Provide for an Effective TPP General Exception”, available at <https://www.citizen.org/documents/general-exception.pdf>, visited on 22 March 2016.

38) *Ibid.*

Concluding Remarks

As the British Broadcasting Corporation puts it, “The TPP is one of the most ambitious free trade agreements ever signed.”³⁹⁾ It may not be an agreement for the 21st century but rather an expanded and improved 12 – country version of the Free Trade Agreements (FTAs) recently concluded by the US (in particular with Australia, South Korea, and Singapore).⁴⁰⁾ Of course, those bilateral FTAs are quite ambitious in their own right, and there are some areas in which the TPP exceeds them in the level of ambition. However, the TPP is no different from the existing FTAs in its basic framework for rules.⁴¹⁾

Jeffrey D. Sachs, a world-renowned professor of economics, leader in sustainable development, senior UN advisor, described by the New York Times as, “probably the most important economist in the world,” and by Time Magazine as “the world’s best known economist” has stated:⁴²⁾

Globalization is a positive and powerful force for good, if it is embedded in the right kind of ethical and legal framework. Yet the current draft of the Trans - Pacific Partner-

39) See British Broadcasting Corporation, “TPP: What is it and why does it matter?”, available at <http://www.bbc.com/news/business-32498715>, visited on 22 March 2016.

40) Tsuyoshi Kawase, “The TPP as a set of International Economic Rules”, available at <http://www.voxeu.org/article/tpp-set-international-economic-rules>, visited on 26 March 2016.

41) Ibid.

42) Jeffery D. Sachs, “TPP is too Flawed for a Simple ‘yes’ Vote,” available at <https://www.bostonglobe.com/opinion/2015/11/08/jeffrey-sachs-tpp-too-flawed-for-simple-yes-vote/sZd0nlnCr18RurX1n549GI/story.html>, visited on 24 March 2016.

ship is not worthy of a simple thumbs-up by the Congress. Without jettisoning the purported goals of TPP, the 12 signatories should slow down, take the pieces of this complex trade agreement in turn, and work harder for a set of international standards that will truly support global sustainable development.

From the human rights perspective, the UN's independent expert on the promotion of democratic and equitable international order, Alfred de Zayas, argues that the TPP "is fundamentally flawed and should not be signed or ratified unless provision is made to guarantee the regulatory space of States."⁴³⁾ He further states that trade is not an end in itself, but must be seen in the context of the international human rights regime, which imposes binding legal obligations on States. Trade agreements are not 'stand-alone' legal regimes, but must conform to the fundamental principles of international law, including transparency and accountability.⁴⁴⁾ They must not delay, circumvent, undermine or make impossible the fulfilment of human rights treaty obligations. Interestingly, Alfred de Zayas suggested that the TPP can legally be contested.⁴⁵⁾

Should the TPP ever enter into force, its compatibility with the international law should be challenged before the International Court of Justice (ICJ). Already now, the ICJ

43) See The United Nations Human Rights (Office of the High Commissioner), Statement by the Independent Expert on the promotion of a democratic and equitable international order, Alfred de Zayas, on the upcoming signing the Trans-Pacific Partnership, available at <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17005&LangID=E>, visited on 24 March 2016.

44) Ibid.

45) Ibid.

could be called upon to issue an advisory opinion stating that in case of conflict between trade agreements and the UN Charter, including its provisions on State sovereignty, human rights and development, it is the Charter that prevails.

Chapter 14 of the TPPA seeks to achieve multiple objectives. The USTR provides the following rationales and objectives - "TPP will help preserve the open Internet and prevent its breakup into multiple, balkanized networks in which data flows are more expensive and more frequently blocked. The Electronic Commerce chapter, according to the USTR, will ensure the free flow of data (subject to public-interest regulation, for example to prevent spam, protect privacy, and fight cyber-crime); prevent the spread of 'forced localization' of technologies and servers; and help to more effectively guarantee the security and privacy of internet users. All this will help to unlock the promise of digital trade through rules that keep the Internet free and open, set digital trade rules-of-the-road, and provide the incentives and a stable framework that can nurture a healthy environment for companies and individuals as they create and use content."⁴⁶⁾

Remarkably, in the negotiations between the US and the EU on the Transatlantic Trade and Investment Partnership (TTIP), the EU trade negotiators have been telling their US counterparts to keep data protection out of trade talks. The EU negotiators said that they have no mandate to negotiate over data protection rules. In fact, data

46) See USTR, available at <https://ustr.gov/sites/default/files/TPP-Chapter-Summary-Electronic-Commerce.pdf>, visited on 17 March 2016.

protection issue is one of the stumbling block for the negotiation to proceed further. The EU Justice Commissioner, Viviane Reding during a speech in Washington in October 2013, said:⁴⁷⁾

There are issues that will easily derail TTIP. One such issue is data and the protection of personal data. This is an important issue in Europe because data protection is a fundamental right... This is why I am against bringing data protection to the trade talks. Data protection is not red tape or a tariff. It is a fundamental right and as such it is not negotiable.

According to Timothy B. Lee, like most parts of the TPP, the new rules on electronic commerce largely reflect the priorities of companies. He argues further that like other recent trade deals, the TPP is a vehicle for helping powerful US interests write the rules of the global economy. With US technology firms becoming increasingly powerful in Washington and increasingly influential at the Office of the US Trade Representative, which negotiates trade deals – it's not surprising that the TPP included many provision favored by US technology companies.⁴⁸⁾

47) See Ralf Bendrath, "TTIP and TiSA: Big Pressure to Trade Away Privacy," available at <http://www.statewatch.org/analyses/no-257-ttip-ralf-bendrath.pdf>, visited on 15 March 2016.

48) See Timothy B. Lee, "How the TPP Could Impact Regulation of Everything from Cars to Medical Devices", available at <http://www.vox.com/2015/11/29/9760918/tpp-ecommerce-chapter>, visited on 28 March 2016.