**November 5, 2015**

# The Highlights of the Trans-Pacific Partnership E-commerce Chapter

**Burcu Kilic & Tamir Israel**[1]

The E-commerce[2] chapter of the Trans-Pacific Partnership (TPP) sets rules that, if ratified, will shape the development of the digital economy for years to come. The chapter sets rules and procedures for trade in goods and services conveyed by the Internet and other electronic means, and addresses a range of issues including duties on digital products, paperless trade administration, and rules on electronic signatures, net neutrality and data protection. The text also includes provisions limiting the ability of countries to keep data within their territorial borders.

## Scope

The chapter does not clearly define its scope of application, but rather states broadly that "[T]his Chapter shall apply to measures adopted or maintained by a Party that affect trade by electronic means."

Although it does include certain definitions, no definition is provided for key scoping terms 'e-commerce' or 'trade by electronic means'.

The Chapter explicitly notes that:

- The obligations it imposes overlap with those relating to the provision of services set out in Chapters II through KK (Investment, Cross-Border Trade in Services, and Financial Services), and are subject to any applicable exceptions or non-conforming measures (NCMs) set out in the Trans-Pacific Partnership Agreement in general.
- The obligations relating to non-discriminatory treatment of digital products, cross-border trade in services, location of computer facilities and source code and financial services are also subject to exceptions and non-confirming measures attached to Chapters II through KK and should be read in conjunction with any other relevant provision in the Trans-Pacific Partnership Agreement in general.
- The chapter does not apply to government procurement or information held or processed by or on behalf of a Party or measures related to such information and its collection, e.g. health data collected by the Governments.

[1] Burcu Kilic, Public Citizen (bkilic@citizen.org) & Tamir Israel, Canadian Internet Policy & Public Interest Clinic (CIPPIC) at the University of Ottawa Faculty of Law (tisrael@cippic.ca)

[2] Chapter 14, Electronic Commerce, http://www.mfat.govt.nz/downloads/trade-agreement/transpacific/TPP-text/14.%20Electronic%20Commerce%20Chapter.pdf

The exclusion of government procurement and data practices narrows the application of the e-commerce chapter from what had been previously indicated in public discussion and from what is currently proposed in similar e-commerce chapters in other multilateral trade agreements under negotiation, such as the Trade in Service Agreement (TISA).

## Non-conforming Measures

The obligations on non-discriminatory treatment of digital products, cross-border trade in services, location of computer facilities and source code are subject to non-conforming measures. Each Party has schedules listing NCMs, which can exclude any law, regulation, procedure, requirement or practice that is adopted[3] or maintained, from rules on non-discriminatory treatment of digital products, cross-border transfer of information by electronic means and location of computing facilities and source code. This is known as a 'negative list' approach, which has the effect of "locking in" current protections by prohibiting future reforms and preventing expansion of existing restrictive measures. With the negative list NCM approach, governments ultimately forgo the right to introduce measures in the future if said measures implicate the non-discriminatory or access-impairing provisions in the Chapter – even in sectors that do not yet exist or are not regulated at the time of the Agreement's entry into force. NCMs are subject to negotiations, a Party cannot simply claim an NCM unilaterally without persuading other Parties to agree.

It should be noted that the NCMs of the e-commerce chapter are limited in application to obligations within that chapter relating to non-discriminatory treatment of digital products, cross-border trade in services, location of computer facilities and source code, while other obligations within the Chapter are not subject to NCMs at all. It should also be noted that elements of the e-commerce chapter are subject to applicable NCMs adopted in other chapters such as the Chapter on Cross Border Trade in Services.

## Selected Provisions

### Cross-Border Data Transfers by Electronic Means (Article 14.11)

The first paragraph of the Article recognizes that each Party may have its own regulatory requirements concerning the transfer of information. However, this should not be interpreted as an exception that can override the substantive obligations of this Article. This paragraph should be read alongside each Party's schedule of non-conforming measures, which applies to this provision.

[3] Some NCM formats allow governments who successfully negotiate some specific existing mechanisms that will allow for future changes. For example, Article 9.11 of the TPP's Investment chapter includes two separate Annexes. Annex I includes specific government laws that can be amended in the future, where as Annex II lists specific laws that are exempt in their current format, but can only be amended in the future in ways that increases their conformity with applicable TPP obligations.

Paragraph 2 mandates that Parties allow the cross-border transfer of data (including personal information) to a country or territory without consideration of whether said country or territory maintains an adequate level of protection for the rights and freedoms of individuals. The cross-border transfer of information must be for the conduct of an investor or service supplier's business. This suggests that it may ultimately be limited to outsourcing of internal services, but it is likely this provision would be interpreted broadly by a dispute resolution body so as to include any and all elements of a service.

The provision grants businesses the freedom to outsource data storage and processing to any other TPP jurisdiction without limitation. As the chapter does not require Parties to adopt privacy laws, this could create meaningful barriers for the protection of privacy. A country that has such laws will find it challenging to enforce data standards on a company resident in a country that does not. In addition, some companies may rely on the lack of a physical presence in a particular jurisdiction in order to argue that they need not comply with the privacy and other consumer protection laws of that country. In such instances, jurisdictions often place restrictions on cross-border data transfers as a means of ensuring a minimum level of privacy protection. This mechanism for securing privacy in cross-border contexts where jurisdiction is an issue has always been an integral component of international and domestic privacy protection. This provision therefore significantly undermines the ability of governments to secure their citizens' data against unauthorized or unlawful processing, or accidental loss or destruction of, or damage to, personal data in these contexts.

Paragraph 3 introduces an exception permitting Parties to adopt or maintain measures inconsistent with the cross-border transfer of information. The 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. The language has many layers of qualifications, which are similar to the general exceptions adopted in Article XIV of the General Agreement on Trade in Services (GATS).[4] However, there is a key difference: while the GATS provision allowing exceptions in the absence of discrimination or trade restrictions are included in the chapeau, paragraph 3 of the TPP encodes the exception independently, placing the burden of showing that the measure meets all of its requirements on the government taking the measure.

Moreover, the exception is negatively worded; it does not recognize that 'a Party has the right to adopt or maintain' restrictions on the data localization granted to companies in paragraph 2. Rather, it is drafted so that the data localization restrictions apply unless it can be

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

> (c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to:
>
> > (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;

demonstrated that a government's "legitimate public policy objective" (e.g. its privacy laws) can justify a departure from the general restriction. Therefore, not only does the government bear the burden of demonstrating that the restriction does not restrict trade or discriminate, but it must also prove that its chosen public policy objectives are 'legitimate'. Overall, the provision places a high burden of proof onto governments, forcing them to rigorously justify any restrictions on trans-border data transfers.

There are three thresholds that must be met for the government's defense to succeed. First, the measure must achieve a legitimate public policy objective. "Legitimate public policy objective" is not self-defining and the Party would have to justify the policy objective if it is challenged in a dispute. There are two further elements, both of which must be satisfied.

The application of the measure (or the measure itself, if it is discriminatory) must not "constitute a means of arbitrary or unjustifiable discrimination" (the same term used in the GATS general exception), which requires a rational connection to the objective and can be unpredictable. The application of the measure must not be a disguised restriction on trade, so if there is some benefit to domestic interests, even if not the goal or intended consequence of the measure, it could fall outside that requirement[5]. The measure must be the least burdensome, and it must not impose any restrictions on transfers of information. - If there is arguably another way to achieve the stated policy objective that is less onerous, then the government should have adopted that one. In other words, if there is another option that is less burdensome to cross-border transfers of data online, but that option has an undesirable impact (not necessarily related to the policy objective) and the government therefore wants to avoid it, it cannot choose to do so.

While earlier, public discussions of this provision considered imposing obligations for cross-border data transfers on governments as well as businesses, this is no longer the case. This will allow data localization obligations such as the Canadian province of British Columbia's *Freedom of Information and Privacy Act* to persist, as it imposes no direct obligations on the private sector. However, any legal system that imposes limits on private sector data transfers to jurisdictions for the purpose of safeguarding citizens' data against foreign government intelligence agencies, as was recently accomplished by the Court of Justice of the European Union in *Schrems v Facebook Inc*, 2015 Case C-362/14, could contribute to violation of Section A of the TPP's Investment chapter and be subject to sanction and heavy penalties through the investor-state dispute mechanism.

**Location of Computing Facilities (Article 14.13)**

The Office of the United States Trade Representative (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 use local network

[5] See, WTO Secretariat's summary of jurisprudence on this phrase to 30/9/2011: https://www.wto.org/english/res_e/booksp_e/analytic_index_e/gatt1994_07_e.htm#article20C2b

infrastructure or local servers as non-tariff barriers that amount to discriminatory restrictions on trading rights.. The U.S. also feels that localization requirements would undermine the advantage currently enjoyed by U.S. cloud-based services, since most, if not all, corporations that utilize cloud-based services are currently located in the U.S.

This provision prohibits requirements that servers be located (or data stored) locally. The location of data often determines which laws on how data is stored and processed are applicable. The majority of American information and communications technology (ICT) companies store data in the U.S., which makes U.S. rules applicable to the storage, processing and transfer of data in the conduct of their business.

Article 14.13 includes an exception permitting Parties to adopt or maintain measures inconsistent with the cross-border transfer of information to achieve a legitimate public policy objective. The exceptions language mirrors that of Article 14.11, which would likely be difficult to use and insufficient to protect the policies, laws and regulations that Parties have or may consider in the future to safeguard privacy.

**Personal Information Protection (Article 14.8)**

This provision also appears in the TISA e-commerce chapter. In TISA negotiations, this provision is supported by most of the Parties. However, the support of the US, notably, is y absent; it took no position on the protection of personal information. This may be due to the lack of a single comprehensive system to protect personal information in the US. Rather, the US has a patchwork system of federal and state laws, and regulations for the collection and use of personal data, which can overlap, dovetail and may contradict one another. The US system is based on self-regulation by the companies, the Federal Trade Commission (FTC) only steps in when companies fail to self-regulate.

Instead of addressing this shortcoming in privacy protection, the TPP 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.

The provision follows other regional Free Trade Agreements in requiring Parties to adopt or maintain that domestic laws to protect personal information should follow the principles and guidelines of relevant international bodies. For the TPP region, this will be primarily that Asia Pacific Economic Cooperation (APEC) privacy framework, which is widely recognized as providing weak protection for individual privacy. Footnote eight clarifies that a comprehensive privacy, personal information, or personal data protection law, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy may satisfy this requirement. The US, for instance, is not likely to adopt a privacy law or series of laws, but will continue to rely on ad hoc FTC regulations and voluntary rules of conduct.

The provision requires that Parties "*endeavor* to adopt non-discriminatory practices in protecting users of electronic commerce from personal information protection violations occurring within its jurisdiction" (emphasis added). In contrast with other paragraphs, this is a soft-provision. This may be due to the lack of a single comprehensive system to protect personal information in the U.S.. It also encourages interoperability of privacy regimes, an approach that has been used in the past to initiate a 'race to the bottom' whereby the lowest standards from each jurisdiction are adopted

**Principles on Access to and Use of the Internet for Electronic Commerce – Net Neutrality (Article 14.10)**

This is a soft obligation couched in language of 'recognition' that consumers are ability to access any services and applications on the Internet, subject to reasonable management of the network; connect whatever devices they want, provided that doing so doesn't harm the network; and access information on network management practices of those who supply their access to the Internet.

This provision mirrors its counterpart provision in the Trade in Services Agreement, which is currently being negotiated. However, where TISA requires the adoption of such net neutrality protections, the TPP only encourages governments to 'recognize' the benefits of consumers' having them. The protections themselves seek to address net neutrality in a minimalistic, yet nonetheless problematic manner. Article 14.10 (a) is against blocking access to content. Paragraph (a) suggests providers may block access to content for 'reasonable network management' purposes. Reasonable network management' is a more permissive standard than that adopted by other jurisdictions. Many jurisdictions prohibit the blocking of services or content in all but exceptional circumstances. It is unclear how the TPP's 'reasonable network management' exception will ultimately be interpreted by an oversight body. Moreover, the TPP net neutrality rules are highly deficient as they focus on the blocking of access to content, ignoring the most frequent types of threats to net neutrality – economic incentives, traffic degradation short of blocking and traffic prioritization. Footnote 9 clarifies that Internet service providers that offer their subscribers content on an exclusive basis would not be acting contrary to reasonable network management. This will apply to converged ISPs which provide broadcasting content over the Internet.

Paragraph (b), supports the allowance of blocking harmful devices from accessing networks, but does not exempt 'reasonable network management'.

Article 14.10 paragraphs (a) and (b), taken together replicate one branch of the 'Open Internet' rules recently adopted by the Federal Commination Commission, a branch that is focused on protecting against the blocking of end user access to content and services, as well as the use of non-harmful end devices.

Net neutrality as a principle protected by law is one that is rapidly evolving in many jurisdictions, and its full parameters are yet to be established. Unfortunately, the TPP fails to

effectively address existing net neutrality problems. It only meaningfully addresses the most egregious neutrality violations (those relating to blocking of access to content) and even here broadly exempts “reasonable network management”. Were its approach to become an international standard for neutral open access embedded as an international standard, it will be one that is incapable of meeting the net neutrality of today, let alone that of tomorrow. Indeed, existing net neutrality frameworks in Brazil, Canada and elsewhere adopt more stringent restrictions on service providers seeking to block customer access to downstream services or content.

Article 14.10 paragraph (a) of the TPP is also problematic because it may only apply to situations where access to applications or services are blocked. It may not include situations where traffic is unjustifiably degraded or discriminated against in an economic sense, or where a service provider prioritizes certain services, giving them significant advantages over competitors. Yet the majority of net neutrality concerns relate to economic or technical discrimination against downstream traffic.

Due to these shortcomings, the TPP’s open access framework leaves open an entire universe of discriminatory and innovation-harming activity that traffic carriers can leverage and which regulators have found objectionable. Without actually requiring any governments to adopt net neutrality protections, it legitimizes a watered down version of this critical and emerging set of principles, undermining attempts to develop meaningful net neutrality. If the TPP approach, which is already being replicated in other multi-lateral agreements such as the Trade in Services Agreement, becomes the international standard for addressing open access or net neutrality harms, it will do so in a manner that is woefully deficient.

**Custom Duties (Article 14.3)**

Article 14.3 provides that electronic transmissions are not subject to customs duties, which would prevent countries from imposing custom duties on any digital product or services (e.g., e-books, software, games, music, and video, whether distributed online or fixed on a carrier medium). Nevertheless, it does not prevent a government from imposing internal taxes or other internal charges for a delivery transmitted by electronic means provided that such taxes or charges are imposed in a manner consistent with the Agreement.

If a delivery transmitted by electronic means is exempted from customs duties, custom duties on imports will be lost. This can be particularly disruptive in developing countries where tariff revenues play a significant role in national budgets. As digital goods and services grow in importance, such countries may face serious difficulties in replacing lost revenues before locking themselves into permanent duty free status for delivery by electronic means.

**Non-Discriminatory Treatment of Digital Products (Article 14.4)**

Article 14.4 guarantees no less favorable treatment to digital products emerging from its own territory or originating from a service provider of its nationality, than to comparable digital products emerging from the territories of other Parties.

This is subject to certain exceptions like the rights and obligations in Intellectual Property Chapter or subsidies and grants provided by governments. The provision also does not apply to broadcasting. It should be read in conjunction with each Party's NCM schedules.

**Electronic Authentication and Signatures and Transactions (Articles 14.5 and Article 14.6)**

This provision aims to minimize restrictions on the use of electronic signatures. Accordingly, a government cannot deny the legal validity of a signature just because it is electronic. However, domestic law can prevent or limit legal recognition of electronic signatures as valid, so this amounts to no more than a requirement that exceptions to the general recognition of electronic signatures be set out in law.

With respect to authentication mechanisms for electronic signatures, Clause 2 of Article 14.6 holds that a government cannot introduce or keep existing requirements for authentication that would prevent parties from choosing their own methods of authentication. A government also cannot require authentication mechanisms that would prevent parties to an electronic transaction from proving to judicial or administrative bodies that their transaction complies with the law in relation to authentication.

Clause 3 of Article 14.6 permits parties to establish performance standards for authentication and requirement for certification by an accredited authority. These performance and certification measures can operate even if they operate to prevent parties from determining their own authentication method or from proving legal compliance to a judicial or administrative body. However, in such instances, these performance measures and or certification requirements cannot be applied to electronic transactions in general. They can only be applied to 'particular categories of transactions', but it is not clear by what mechanism these categories might be chosen or justified.

Governments are encouraged to use interoperable electronic authentication, but there is no requirement to do so.

Finally, with respect to electronic transactions, Article 14.5 obligates governments to maintain frameworks for electronic transactions that are consistent with either the UNCITRAL Model Law on Electronic Commerce 1996 or the UN Convention on the Use of Electronic Communications in International Contracts 2005. This effectively renders the mechanisms in those treaties enforceable through TPP's heavy handed international enforcement mechanisms.

**Unsolicited Commercial Electronic Messages (Article 14.14)**

Article 14.14 requires the Parties to adopt measures regulating unsolicited commercial electronic communications. Sub-clause (a) proposes an opt-out in which a recipient may stop messages. Sub-clause (b) proposes that unsolicited commercial communications require the user to consent or opt in. Further, sub-clause (c) proposes the adoption of other, unspecified measures that would minimize unsolicited commercial messages.

Currently, these three measures are presented as alternative options, leaving Parties with significant latitude in how they choose to regulate electronic spam.

The TPP would, however, obligate Parties to cede a level of control over how key terms in spam control are internationally interpreted. While the provision expressly reserves to domestic governments the determination over how to define 'consent', it does not do so with respect to determining what granting end users the right to stop messages might mean in this context.

**Publicizing Source Code (Article 14.17)**

Article 14.17 prevents governments from requiring the disclosure of source code as a condition of import, distribution, sale or use of software or of products containing software. This prohibition only applies to "mass-market" software or products and does not include software used for "critical infrastructure". Neither term is defined.

The Article also does not operate so as to prevent a government from obligating specific modifications of source code in order to ensure software complies with legal requirements. Moreover, the Article does not apply to the inclusion of source code disclosure obligations in commercially negotiated contracts or in patent applications. It also permits courts to order disclosure of source code in patent disputes as long as sufficient safeguards are in place to prevent unauthorized disclosure of said source code.

It is concerning that other types of legal disputes are not mentioned, as access to source code might be necessary in resolving legal matters unrelated to patents, such as discrimination disputes, privacy disputes, etc. Moreover, while the Article excludes disclosure obligations in commercially negotiated contracts, it does not exempt source code disclosure provisions imposed by means of a software license. It is not uncommon for open source licenses to obligate third parties using such code in future projects to make derivative source code public. This is how authors of open source code keep their code 'open'. As open source licenses are not 'commercially negotiated' but rather imposed on others, there is concern that any attempt to enforce such licenses against third parties by means of the courts would amount to a violation of this Article, opening the country whose court system carried out such enforcement to heavy-handed penalties through the investor-state dispute enforcement mechanisms.

In addition, as noted above, the Article exempts source code disclosure requirements for critical infrastructure. However, this is at once overly broad and overly narrow. Forcing

disclosure of source code for critical infrastructure can allow governments to undermine the privacy and security of communications networks by allowing them to find avenues for state exposition of such systems. On the other hand, mandating publication of course code in non-critical infrastructure components such as routers can benefit significantly in terms of security. Indeed, the Federal Communications Commission is currently considering a proposal to mandate publication of router source code as a means of addressing the sorry state of router security.[6] Finally, addressing cybersecurity breaches can require mandating the publication of source code so as to facilitate fixing of security flaws. The TPP's prohibition on such requirements could undermine security measures of this type.

[6] Jeremy Malcolm, "TISA: Yet Another Leaked Treaty You've Never Heard of Makes Secret Rules for the Internet", May 27, 2015, *Eff.org* , <https://www.eff.org/deeplinks/2015/05/tisa-yet-another-leaked-treaty-youve-never-heard-makes-secret-rules-internet>.