Analysis: Leaked TISA Annex on Electronic Commerce

Burcu Kilic & Tamir Israel[1]

Today, WikiLeaks released an updated draft of the Annex on Electronic Commerce of the proposed Trade in Services Agreement. The TISA is a trade agreement currently being negotiated by 23 countries (counting the EU as one), who call themselves "the Really Good Friends of Services".

The Annex on e-commerce includes U.S.-backed measures on e-commerce, technology transfer, cross-border data flows and net neutrality that would expand the scope and rules of the General Agreement on Trade in Services (GATS) at the World Trade Organization (WTO).

The TISA is intended as a 'gold standard' agreement that other countries can accede to, set new standards that will inform other agreements, and eventually be incorporated back into the GATS to apply to the whole WTO membership.

Selected Provisions:

Article 2: Movement of Information or Cross-Border Information Flows

Article 2: [CA/PE/US propose: Movement of Information] [JP/MX/CH propose: Cross-Border Information Flows]

[KR: Regarding the article on movement of information, Korea is of the view that any movement of information arising from the actions of a service supplier must be based on "informed consent." Informed consent refers to the idea that individuals supplying their personal information to service suppliers have full protection and recourse under the law in regards to the usage of their personal information provided to service suppliers. This should be appropriately reflected in the language of the article.

HK: The movement of information should be without prejudice to the domestic regime for the protection of personal data and be based on informed consent.]

1. [CA/TW/CO/JP/MX/US propose: No Party may prevent a service supplier of another Party [CO/JP propose: or consumers of those suppliers,] [CA/CO/JP/TW/US propose: from transferring, [accessing, processing or storing] information, including personal information, within or outside the Party's territory, where such activity is carried out in connection with the conduct of the service supplier's business.]

2. [US propose: PLACEHOLDER for financial institutions.]

3. [CH propose; CO oppose: Parties should have measures to protect consumers engaging in electronic commerce from fraudulent and deceptive commercial practices.]

[1] Burcu Kilic, Public Citizen & Tamir Israel, Canadian Internet Policy & Public Interest Clinic

4. [CH propose; CO oppose: Parties should enhance their enforcement capacity to ensure that the applicable laws and regulations concerning the protection of data and privacy are complied with.]

5. [CH propose; CO/US oppose: Parties should not prevent foreign suppliers of electronic commerce or customers of such suppliers, from electronically transferring information internally or across borders, accessing publicly available information, or accessing their own information stored abroad].

The Parties are debating the title of this provision where Canada, Peru, and the United States propose "Movement of Information" and Japan, Mexico, and China are proposing "Cross-Border Information Flows." One possible reason for this debate is that "Movement of Information" (or "Free Flow of Information") sounds more sympathetic and human-rights-related. "Cross-Border Information Flows" sound more trade oriented.

Article 2.1 proposes that "No Party may prevent the transfer, access, processing or storing of information (including personal information) outside that Party's territory if conducted in connection with a business." This provision facilitates cross border data transfers and data-processing across all services sectors, including financial services, without limitations.

Data protection laws exist to strike a balance between the rights of individuals to privacy and the ability of businesses to use data for the purposes of their business. This provision provides grant freedom to business on how they use the data (including personal information) without being subject to restrictions. Governments may not be able to ensure that data is processed fairly and lawfully or obtained only for specified and lawful purposes. Since there will be no control over the data, it will not be possible to check whether the data is kept longer than is necessary or for the purposes for which it is processed. It is not clear what would happen in case of unauthorized or unlawful processing, or accidental loss or destruction of, or damage to, personal data. This provision allows for the cross-border transfer of data to a country or territory without confirmation that the country maintains an adequate level of protection for the rights and freedoms of individuals.

Korea wants the cross-border data transfers of service providers to be based on "informed consent." Informed consent governs certain types of communication between service suppliers and consumers about the usage of their personal information.

The Switzerland proposed provision provides for transfer of information across borders within internal networks or across borders.

Article 3: Online Consumer Protection

Article 3: Online Consumer Protection
[CH prefers using "electronic commerce" rather than "online commercial activities."**]**
1. **[AU/CA/CL/TW/CO/EU/HK/IS/IL/JP/KR/LI/MX/NZ/NO/PA/PE propose:** The Parties recognize the importance of maintaining and adopting transparent and effective measures to protect consumers from fraudulent and deceptive commercial activities**] [CO/JP/MX propose:**, as well as measures conducive to the development of consumer confidence,**]** when they engage in electronic commerce.**]**

2. **[AU/CA/CL/TW/CO/EU/HK/IS/IL/JP/KR/LI/MX/NZ/NO/PA/PE propose:** To this end, each Party shall adopt or maintain consumer protection laws to proscribe fraudulent and deceptive commercial activities that [may cause harm] [cause harm or potential harm] to consumers engaged in **[CO propose:** electronic commerce**] [AU/CL/JP/KR/NZ/PE propose:** online commercial activities.**]**

3. **[CO propose:** Under non-discriminatory terms and conditions, each Party shall grant consumers engaged in electronic commerce with its own service suppliers, access to existing consumer protection mechanisms provided by their respective national consumer protection authorities.**]**

4. **[AU/CL/CO/JP/MX/NZ/PE propose:** The Parties**] [AU/CL/JP/MX/NZ/PE propose:** recognise the importance of**] [CO propose:** shall endeavour to promote the**]** cooperation between their respective national consumer protection agencies or other relevant bodies on activities related to **[AU/CL/NZ/PE propose:** cross-border**]** electronic commerce in order to enhance consumer [welfare] **[MX propose:** confidence**].]**

5. **[CO/MX propose:** The Parties shall, in accordance with its laws and regulations, allow persons to mutually determine the appropriate methods for resolving disputes arising from their electronic commerce transactions. Such methods may include, but are not limited to, online dispute resolution mechanisms.**]**

Sub-clause 5 of Article 3 raises specific concerns regarding a common and important feature of many consumer protection laws. This clause prohibits governments from interfering with individual attempts to "mutually determine the appropriate methods for resolving disputes arising from their electronic commerce transactions…includ[ing]… online dispute resolution mechanisms." A number of consumer protection frameworks have adopted prohibitions on the use of dispute resolution clauses in consumer contracts. The impetus for such regulation is that such clauses are often unilaterally imposed in consumer contracts of adhesion and used to effectively prevent any access to the courts and, in particular, to class action mechanisms for adjudication of small claims in aggregate. Yet Article 3.5 would appear to preclude the use of provisions guaranteeing access to the courts and to class action mechanisms, as this could constitute an interference with mutually determined dispute resolution mechanisms in spite of the reality that 'agreement' from consumers is in the form of a non-negotiable clause in a broader contract of adhesion.

Article 4: Personal Information Protection

Article 4: Personal Information Protection
1. **[AU/CA/CL/TW/CO/IL/JP/KR/MX/NZ/NO/PA/PE propose:** 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.**]**

2. **[AU/CA/CL/TW/CO/IL/KR/MX/NZ/NO/PA/PE propose:** To this end, each Party shall adopt or maintain a domestic legal framework that provides for the protection of the personal information of the users of electronic commerce. In the development of these personal information protection frameworks, each Party should take into account principles and guidelines of relevant international bodies.**]**

[CA propose: Each Party shall ensure that its domestic legal framework for the protection of personal information of users of electronic commerce is applied on a non-discriminatory basis.**]**
3. **[AU/CA/CL/TW/CO/IL/JP/KR/MX/NZ/NO/PA/PE propose:** Each Party should publish information on the personal information protections it provides to users of electronic commerce, including:

(a) how individuals can pursue remedies; and

(b) how business can comply with any legal requirements.**]**

The Parties recognize the economic and social benefits of protecting the personal information of users of electronic commerce and are required to adopt or maintain a domestic legal framework that provides for the protection of the personal information of the users of electronic commerce. To this end, a majority of the negotiating parties propose that domestic laws to protect personal information should follow the principles and guidelines of relevant international bodies. The US, for example, 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.

Canada proposes a non-discriminatory basis for the protection of personal information. Noticeably absent is the US. The US takes no position on the protection of personal information. This may be due to the US having no single comprehensive system to protect personal information. Instead, it 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.

Article 5: Unsolicited commercial electronic communications

Article 5: Unsolicited Commercial Electronic [AU/CO/NZ propose: Messages] [EU propose; NO considering: Communications]
1. **[AU/CA/CL/CO/CR/EU/IL/JP/KR/MX/NZ/NO/PE propose:** Each Party shall **[TW/TR propose:** endeavour to**]** adopt or maintain measures regarding unsolicited commercial electronic [messages] **[EU propose:** communications**]** that:**]**
(a) require suppliers of unsolicited commercial electronic messages to facilitate the ability of recipients to

stop such messages; or **[EU/NO propose; AU oppose:** and**]**

(b) require the consent, as specified according to the laws and regulations of each Party, of recipients to receive commercial electronic messages; **[EU/NO oppose:** or

(c) otherwise provide for the minimization of unsolicited commercial electronic messages.**]]**
2. **[AU/CA/CL/CO/IL/JP/KR/NZ/NO/PE propose:** Each Party shall **[TW/TR propose:** endeavour to**]** provide recourse against suppliers of unsolicited commercial electronic messages who do not comply with its measures implemented pursuant to paragraph 1.**]**

3. **[AU/CA/CL/CO/CR/EU/IL/KR/JP/NZ/NO/PE propose:** The Parties shall endeavour to cooperate in cases of mutual concern regarding the regulation of unsolicited commercial electronic messages.**]**

Article 5 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 measures that would minimize unsolicited commercial messages.

Currently, these three measures are presented as alternative options, leaving signatories with significant latitude in how they choose to regulate electronic spam. An EU proposal to render sub-clauses (a) through (c) overlapping obligations would significantly strengthen the provision which, in its current form, only really requires state Parties to "provide for the minimization of unsolicited commercial electronic messages" in any way they deem fit. If the EU proposal is adopted, however, a number of existing anti-spam regimes will need to be significantly overhauled to impose a prior consent obligation. Moreover, TISA would cede a level of control over how key terms in spam control are internationally interpreted.

While Article 5 expressly reserves to domestic governments 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.

Article 6: Transfer of Access to Source Code

Article 6: [JP propose; CO oppose: Transfer or Access to Source Code
1. No Party may require the transfer of, or access to, source code of software owned by a person of another Party, as a condition of providing services related to such software in its territory.

2. For purposes of this Article, software subject to paragraph 1 is limited to mass-market software, and does not include software used for critical infrastructure.]

Japan's proposal aims to prohibit governments from requiring a firm that supplies a service related to software to transfer or provide access to source code of software. Critical infrastructure is categorically exempted from this prohibition.

As with many other parts of TISA's e-commerce annex, this provision is ill-thought-out and is at once over-and under-inclusive. There are many situations other than in the critical infrastructure context in which it might be desirable from a public policy perspective to require access to software, such as with consumer routers, whose lax security poses an ongoing issue for home networks. An un-nuanced and categorical prohibition on requiring access to source code can prejudice transparency as well as the use of open source offerings in government contracting. A government requiring publication of source code as an essential condition in a service proposal – a mechanism that would enhance public transparency in government services as well as encourage open source in general – could readily be construed as a violation of Article 6 by any service provider wishing to maintain their source code proprietary.

On the other hand, the prohibition in Article 6 is also under-inclusive. There could be good reasons to prevent a particular government from accessing source code for software used in critical infrastructure. To give just one example, a regulator may wish to impose audit obligations in order to check the filtering or monitoring capacities of Deep Packet Inspection equipment installed in a mobile or wireline service provider's network. This might be necessary to understand potentially privacy invasive or censoring network activities.

A more nuanced approach to regulating source code transfer or access obligations would eschew TISA's categorical prohibition and instead encode objectives or purposes under which it is or is not acceptable for such conditions to be imposed.

Article 7: Interoperability

Article 7: [CO propose: Interoperability] **[CO propose:** Each Party shall endeavor to promote the interoperability between their governmental online procedures and services supplied by electronic means.**]**

Colombia's proposal aims to ensure interoperability between governmental online procedures and services supplied by electronic means. Achieving interoperability requires stewardship and dedication, in terms of practical implementation, of services at the operational levels across sectors. As the "Really Good Friends" of the service industry lack the cooperative infrastructure of other governance bodies such as the OECD, APEC and the IGF, it is not clear by what mechanism they intend to realize this mandate.

Article 8: Open Networks, Network Access and Use

Article 8: Open Networks, Network Access and Use 1. **[AU/CA/CL/CO/IL/JP/NO/PE/US propose:** Each Party recognizes that consumers in its territory, subject to applicable laws, and regulations, should be able to: (a) access and use services and applications of their choice available on the Internet, subject to reasonable network management;

(b) connect their choice of devices to the Internet, provided that such devices do not harm the network; and

(c) have access to information on network management practices of their Internet access service suppliers.**]**

2. **[KR oppose: [CO/CH propose:** Parties, preferably through relevant regulators, should promote the ability of consumers legitimately to access, share and distribute information as well as running applications and using services of their choice.**] [CO/JP propose:** Each Party shall endeavour not to**] [TR propose:** Without prejudice to the applicable legislation,**] [CH propose:** Parties should not**] [CO/JP/CH propose:** restrict the ability**] [JP propose:** of service suppliers to supply services**] [CO/CH propose:** to supply services**] [CO/JP/CH propose:** over the Internet**] [CH propose:** including**] [CO/JP/CH propose:** on a cross-border and technologically neutral basis, and**] [JP propose:** shall endeavour to**] [CO/CH propose:** should**] [CO/JP/CH propose:** promote the interoperability of services and technologies, where appropriate.**] [JP propose:** Each Party shall endeavour to ensure that internet access providers avoid unreasonable discrimination in transmitting lawful network traffic.**]]**

This provision is very similar to Article X.5 of the US proposal dated 25 April 2014. This is a soft obligation couched in language of 'recognition' that consumers should be able 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.

The provision addresses net neutrality in a minimalistic, yet nonetheless problematic manner. Article 8 sub-clause 1 (a) imposes a prohibition on blocking access to content. Sub-clause 1(a) allows providers to block access to content for 'reasonable network management' purposes. Reasonable network management' is a more permissive standard than that adopted by other jurisdictions, and may require changes to existing net neutrality frameworks. It is unclear how TISA's 'reasonable network management' exception will ultimately be interpreted by whatever oversight body is ultimately adopted to enforce its obligations. Interestingly, the term 'reasonable network management' is not used in the equivalent provision in KORUS Article 15.7. Sub-clause 1(b), which prohibits blocking of non-harmful devices from accessing networks, but does not exempt 'reasonable network management'.

Article 8 sub-clauses 1(a) and (b) of TISA 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[2].

[2] FCC, In the Matter of Protecting and Promoting the Open Internet, FCC 15-24, 26

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, TISA 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 8 sub-clause 1 (a) of TISA is also problematic because it only applies to situations where access to applications or services is blocked. It does not include situations where traffic is unjustifiably degraded or discriminated against in an economic sense. Yet the majority of net neutrality concerns relate to economic or technical discrimination against downstream traffic.

Article 8 sub-clause 2 of TISA recognizes that Parties should "endeavor" to avoid "unreasonable discrimination" by ISPs in the transmission of lawful network traffic. However, not only is 'reasonable discrimination' permitted (replicating the 'reasonableness' standard adopted by the FCC which, as stated above, is more permissive than those adopted by other jurisdictions such as Brazil and Canada) but TISA imposes no requirement for regulatory action with respect to such discrimination. 'Endeavour' does not implicate the state's law enforcement apparatus and may well preclude its use. Due to these shortcomings, TISA'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.

If it becomes the international standard for addressing open access or net neutrality harms, it will do so in a manner that is woefully deficient.

Article 9: Local Infrastructure / Local Presence

Article 9: [JP/CH/US propose: Local Infrastructure] [JP propose: and Local Presence] [KR propose:1]
1 **[KR propose:** Article 9 does not apply with respect to suppliers of public telecommunication networks or services.**]**
1. **[CO/US propose:** No Party may require a service supplier, as a condition for supplying a service or investing in its territory, to:

(a) use computing facilities located in the Party's territory;

February 2015 ["FCC, Open Internet Rules"], paras. 15-19.

(b) use computer processing or storage services supplied from within the Party's territory; or

(c) otherwise store or process data in its territory.]

[CO propose: However, nothing in paragraph 1 should prevent a Party from conditioning the receipt or continue receipt of an advantage on compliance with the requirement to use, establish, or expand computing facilities in its territory, including those needed for the processing or storage of data.**]**
[KR: Regarding paragraph 1(local infrastructure), Korea has reservations in accepting the current language, taking into account our telecommunications regulatory framework. Korea is open to discussion on limiting or defining the scope of application of this provision.**]**
2. **[US propose; KR/CO oppose:** This article shall only apply to cross-border financial service suppliers to the extent cross-border financial services are covered by a Party's specific commitments.**]**

[JP would like to clarify the meaning of paragraph 2.**] [KR:** Regarding paragraph 2, Korea believes that this can be addressed in the Annex on Financial Services. Korea suggests the deletion of this paragraph, and at the same time supports the Swiss/Japanese proposal to carve out financial services from this Annex, as in the General Provisions Article III.X.**]**
3. **[KR oppose: [JP propose:** No Party shall**] [CH propose:** Parties should not**] [JP/CH propose:** require**] [JP propose:** ICT service suppliers**] [CH propose:** suppliers of electronic commerce**] [JP/CH propose:** to use**] [CH propose:** or establish any**] [JP/CH propose:** local infrastructure as a condition for**] [JP propose:** supplying**] [CH propose:** the supply of**] [JP/CH propose:** services.**]]**

4. **[KR oppose: [JP propose:** No Party shall require ICT service suppliers to establish a local presence as a condition for the cross-border supply of services.**]]**
[JP would like to delete paragraph 4 of this article if local presence is to be set out in TiSA's core text.**] [KR** has reservations on the article of Local Presence (paragraph 4 of Article 9, which is proposed by Japan).**]**

5. **[KR oppose: [JP propose:** No Party shall,**] [CH propose:** In addition, Parties should not**] [JP/CH propose:** give priority or preferential treatment to**] [JP propose:** its own suppliers of services**] [CH propose:** national suppliers of electronic commerce**] [JP/CH propose:** in the use of local infrastructure,**] [JP propose:** national**] [CH propose:** terrestrial**] [JP/CH propose:** spectrum**] [JP propose:**,**] [JP/CH propose:** or orbital resources.**]]**

[CO would like to exclude matters related to government procurement from this provision.**]**

The US and Colombia proposal on data localization states that "no party may require a service supplier to use territorially localized computer facilities for processing and storage of data as a condition of supplying or investing to that country." This obligation applies to all service suppliers (existing and future), including domestic private firms and state-owned enterprises. The restrictions apply to "supplying a service or investing in its territory," which is wide reaching as it applies to all direct and indirect elements in the supply chain of a service.

The USTR has long considered any requirements to use local network infrastructure or local servers as a non-tariff barrier as well as discriminatory restrictions on trading rights, claiming that localization requirements are trade protectionist strategies that disadvantage foreign goods, services, or IP compared to domestic goods. The US also feels that localization requirements would undermine the advantage of US cloud-based services, since

most, if not all, corporations that utilize cloud-based services are currently located in the US.

Blanket local server requirements, without any exemptions, are disproportionate and may have a detrimental effect on the digital economy. Nevertheless, cloud computing is rapidly gaining popularity among service providers, which raises important questions regarding accountability of service providers. It is important to highlight the resulting risks for domestic laws on privacy and protection of health information, non-trading in personal information and consumer protection. The current privacy legislative framework is far from ideal. Divergent privacy laws and regulations exist. The location of data often determines the applicable laws on how data is stored and processed. Most of the American ICT companies store the data in the US, which makes US rules applicable to the data storage, process and transfer. The inadequate level of data protection in the US might be considered a trade barrier for the non-US negotiating parties with strong privacy and data storage laws.

The US wants to limit the application of this article to cross-border financial service suppliers to the extent cross-border financial services are covered by a Party's specific commitments. Switzerland and Japan want to carve out financial services from the Annex, and Korea supports this proposal. Article X.11 of the Leaked TISA financial services chapter provides for cross-border transfer of information.[3] It is also worth noting that the draft "Digital Trade Act," introduced in the US Senate in December 2013, would give the United States Trade Representative a binding mandate for international negotiations in the area of e-commerce. Regulations for "localization" would have to be banned, and "interoperability" of data processing rules would be enshrined as a fundamental principle. This Act would of course also apply to negotiations over the corresponding chapter in the TTIP agreement.

Japan and Switzerland propose that a government cannot require a service supplier (e-commerce or ICT) to use or establish any local infrastructure as a condition for the supply of a service (applying to all direct and indirect element in the supply chain of a service). This provision prevents a government from requiring computer facilities, including servers, to be located within its territory.

According to Japan's proposed paragraph 4, a local presence cannot be made 'a condition' for the cross-border supply of a service. Japan wants to be able to supply ICT services without being required to have a physical office in TISA countries. The rule will only affect services that require some form of approval and apply to services that can only be supplied within the country by authorized or registered providers or licensed operators, such as firms providing services in accounting, law, medicine, engineering etc.

[3] https://wikileaks.org/tisa-financial/

Japan, however, wants to delete the paragraph if local presence is addressed in TISA's core text.

Article 10: Electronic Authentication and Electronic Signatures

Article 10: Electronic Authentication and Electronic Signatures

1. [AU/CA/TW/CO/EU/IS/KR/MX/NO/PA/PE/TR/US propose: Except where otherwise provided for in its law, a Party shall not deny the legal validity of a signature solely on the basis that the signature is in electronic form.]

[JP would like to clarify the meaning of "except where otherwise provided for in its laws" in paragraph 1.]

2. [AU/CA/TW/CO/EU/IS/JP/KR/MX/PE/TR/US propose: No Party may adopt or maintain measures for electronic authentication that would:

(a) prohibit parties to an electronic transaction from mutually determining the appropriate authentication methods for that transaction; or

(b) prevent parties from having the opportunity to establish before judicial or administrative authorities that their electronic transaction complies with any legal requirements with respect to authentication.]

3. [AU/CA/TW/CO/EU/IS/JP/KR/MX/PE/TR/US propose: Notwithstanding paragraph 2, a Party may require that, for a particular category of transactions, the method of authentication meet certain performance standards or be certified by an authority accredited in accordance with the Party's law.]

This provision aims to minimize the restrictions on use of electronic signatures. It is based on the US proposal dated 25 April 2014. Accordingly, a government cannot deny the legal validity of a signature just because it is electronic. Even though the rule sounds strong, it is still subject to domestic law. Domestic law can prevent or limit legal recognition of electronic signatures as valid.

According to this well supported provision, a government cannot introduce or keep existing requirements for authentication that stop parties to an electronic transaction from deciding for themselves what is the best way to authenticate the transaction. A government cannot either prevent parties to an electronic transaction from proving to judicial or administrative bodies that their transaction complies with the law in relation to authentication.

Paragraph 3 allows for performance standards to be set for authentication and requirement for certification by an accredited authority, but only where a measure is substantially related to achieving a 'legitimate governmental objective'. A government can still require a

'particular category of transaction' to meet certain performance standards or be certified by an authority accredited under the domestic law. There is no indication of what these categories might be, and therefore no limitation to their scope or their number.

Article 11: Custom Duties on Electronic Deliveries

> **Article 11: [AU/CO/EU/IS/NO/PE/CH/TW propose: Customs Duties on Electronic Deliveries**
>
> [EU/NO propose: The Parties agree that a delivery transmitted by electronic means shall not be subject to customs duties, [TW oppose: fees or charges].] [CO/CR/JP/PE propose: No Party may impose customs duties, [TW oppose: fees or charges] on electronic transmissions.]
>
> 2. For greater clarity, paragraph 1 does not prevent a Party from imposing internal taxes or other internal charges on [EU/NO propose: a delivery transmitted by electronic means] [CO/MX/PE propose: electronic transmissions], provided that such taxes or charges are imposed in a manner consistent with this Agreement.]

While the provision provides that services delivered by electronic transmission are not subject to customs duties, fees or charges, the provision 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 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. Countries, especially developing countries where tariff revenues play a significant role in national budgets should carefully consider the difficulty of replacing lost revenue before locking themselves into permanent duty free status for delivery by electronic means.

Article 12: International Cooperation

> **Article 12: [JP/CH propose: International Cooperation]**
>
> 1. [CO/JP/NO propose: Each Party shall endeavour to cooperate with the other Parties to increase the level of digital literacy globally and reduce the "digital divide."]
> 2. [CO/CH propose: Parties will [CO propose: to the extent possible] exchange information in the area of electronic commerce and telecommunications Services. That may include information on, inter alia:
>
> (a) technological developments and research in the area of electronic commerce and telecommunications services;
>
> (b) commercial and technical aspects of the supply of electronic commerce and telecommunications Services through all modes of supply;
>
> (c) available possibilities for the exchange of electronic commerce and telecom related

technology; and
(d) applicable laws and regulations, legislative processes and recent legislative developments; applicable technical standards.]

3. [CO/NO/CH propose: Parties will exchange views on developments related to electronic commerce and telecommunications Services at the international level.]
4. [CH propose: Promotion
Parties affirm their intention to:
(a) promote these provisions in order to contribute to the expansion and spread of electronic commerce and telecommunications services;
(b) work together and cooperate in international fora to increase the level of digital literacy and to reduce the global digital divide;
(c) cooperate with third countries with a view to enhancing national regulatory capacity and to contribute to the spread of electronic commerce and telecommunications Services, which are powerful tools for promoting economic development.]

Digital literacy can be defined as the ability to use digital technology, communication tools or networks to locate, evaluate, use and create information. Digital literacy relies on digital modes of communication and facilitates the collaboration and sharing of knowledge. On the other hand, the digital divide is a complex and dynamic concept and describes the differences in access to ICTs. However, there is not a single divide but multiple divides and therefore there are numerous ways to measure the digital divide.

Even though e-commerce opened up new global business opportunities, it is very likely that these developments may widen the digital divide and developing countries may lag behind and lose in the race. Thus international coordination and exchange of information becomes important. This provision promotes cooperation and information exchange among the governments but it does not impose any obligation.

Article 14

[US propose: Nothing in Section III (Electronic Commerce) shall be construed to prevent any Party from taking any action which it considers necessary for the protection of its own essential security interests.]

[CO/JP would like to clarify the meaning of “essential security interests” in paragraph 1 of this article.]
[KR: Korea would like to have greater discussion on what is meant by “essential security interests” in this this article.]

This US proposed exception protects the right of a government to take any action it deems necessary to protect its essential security interests. The provision makes no

provision for limitations or reservations. When applying these exceptions, governments should weigh the harm to the public interest.

The national security exception is self-judging. The US has refused to submit to any dispute that has challenged its use of a similar, but weaker provision under the GATT and in the WTO.

Article 15: Definitions

For purposes of this Annex:
[AU/CO propose: authentication means the process or act of establishing the identity of a party to an electronic communication or transaction or ensuring the integrity of an electronic communication;**]**
[CO propose: electronic commerce means any cross-border business or commercial transaction conducted by electronic means; including, among others, contracts for distribution services, construction works, consulting services, engineering services and business services.**]**
[EU/TR: electronic signature means data in electronic form which are attached to or logically associated with other electronic data and fulfils the following requirements:

(i) it is used by a person to agree on the electronic data to which it relates;

(ii) (ii) it is linked to the electronic data to which it relates in such a way that any subsequent alteration in the data is detectable.**]**

AU/CO/NZ propose: personal information means any information, including data, about an identified or identifiable natural person.**]**

[Proponents will consult on this definition of personal information.]

[AU propose: unsolicited commercial electronic message means an electronic message which is sent for commercial and marketing purposes to an electronic address without the consent of the recipient or against the explicit rejection of the recipient, using an Internet access service supplier and, to the extent provided for under the domestic laws and regulations of each Party, other telecommunications service.**]**

Authentication: Even though the notion of authentication fulfils different functions among legal systems, it is generally understood to refer to the genuineness of a document or record, which refers the originality of the document, support of the information it contains, in the form it was recorded and without any alteration. The different legal definition of authentication in various legal systems may cause confusion over particular procedures or form requirements. The Australia and Colombia proposed definition is the same definition as in the Australia- US Free Trade Agreement[4]

Electronic signature: The proposed definition mimics the definition of "advanced electronic signature" provided in the Directive. It should be noted that as new forms of technology develop, providing a technologically specific form of electronic signature in legislation is not desirable. A broad definition of electronic signature will help governments to determine their use for each form of signature, and coordinate authenticity with other partners.

[4] Article 16.8, Australia – US FTA (https://ustr.gov/sites/default/files/uploads/agreements/fta/australia/asset_upload_file508_5156.pdf)

Personal Data: How the term ‘‘personal data’’ is defined determines the applicability and scope of privacy laws. Australia, Colombia and New Zealand proposed definition mimics the European Data Protection Directive definition of personal data--‘‘information relating to an identified or identifiable natural person.’ Given the multiple competing definitions in US law, this provision may be expansionist for the US.

The cross border data transfers highly depend on the coordination between legal systems, divergence between the definitions of personal data is very likely to create problems for the protection of privacy.

New Provisions Applicable to All Services

[Inclusion in this working document of the following articles from the U.S. proposal for Part III of the core TiSA text is intended to facilitate discussion and is without prejudice to the final inclusion and arrangement of such articles in the core TISA text or an annex.]

The analysis of the previously leaked US proposal (Trade in Services Agreement TISA Proposal New Provisions Applicable to All Services April 25, 2014) is available here.