Briefing on US TISA Proposal on E-Commerce, Technology Transfer, Cross-border Data Flows and Net Neutrality

Professor Jane Kelsey

Faculty of Law, University of Auckland, New Zealand

and

Dr Burcu Kilic

Public Citizen, Washington D.C., USA

17 December 2014

Briefing on US TISA Proposal on E-Commerce, Technology Transfer, Cross-border Data Flows and Net Neutrality

CONTENTS

US Objectives in the Proposal ***3***

Secrecy **5**

Relationship to other negotiations **5**

Content **6**

Article 1: Local Presence 6

Article X.2: Local Content 9

Article X.3: Local Technology 12

Article X.4: Movement of Information 15

Article X.5: Open Networks, Network Access and Use 17

Article X.6: Electronic Authentication and Electronic Signatures 18

Article X.7: Exceptions 19

Briefing on US TISA Proposal on E-Commerce, Technology Transfer, Cross-border Data Flows and Net Neutrality[#]

A proposal by the US Trade Representative (USTR) dated 25 April 2014 to the Trade in Services Agreement (TISA) negotiations has been leaked. It focuses on e-commerce, technology transfer, cross-border data flows and net neutrality.

The TISA is a mega-agreement currently being negotiated between 23 parties (counting the EU as one), who call themselves, ironically, the Really Good Friends of Services. The TISA talks began formally in March 2013.

Their aim is to extend the scope and rules of the General Agreement on Trade in Services (GATS) at the World Trade Organization (WTO). Attempts to achieve that goal through the Doha round have been stalled for some years. 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.

TISA is one of three mega-negotiations currently underway. The other two are the Trans-Pacific Partnership Agreement (TPPA) and the Transatlantic Trade and Investment Partnership (TTIP). The US and its industry are dominant players in all three negotiations. One US advocate described them as '*creating alternative "play-by-the-rules" clubs of like-minded countries*'.[1]

US Objectives in the Proposal

The US proposal is driven by three imperatives, to:

1. advance the commercial interests of its services industry that supplies services across the border, mainly through e-commerce, and foreign direct investment in manufacturing and services. The proposal would provide particular gains to the information telecommunications and technology sector, but has broader based goals to protect US competitive advantage and monopoly rights over intellectual property and technology.
2. consolidate data repositories to the benefit of the US government, transnational companies (TNCs) and third party commercial interests. This serves a range of 'national security' and commercial purposes.
3. prevent or restrict government regulation that impedes the activities and profits of the major global services industries, and guarantees unrestricted cross-border data flows, which impacts on consumer protections, privacy laws, regulatory constraints and competition policy.

While this is a US proposal, much of its content mirrors the key principles of the 2011 EU-US Trade Principles for Information and Communication Technology

---

[#] Professor Jane Kelsey, Faculty of Law, The University of Auckland, New Zealand and Dr Burcu Kilic, Public Citizen, Washington DC.

[1] Robert D. Atkinson, Information Technology and Innovation Foundation, Hearing on 'The Impact of Information Technology Transfer on American Research and Development' before the House Science Committee, Subcommittee on Investigations and Oversight of the US House of Representatives, 5 December 2012, http://www2.itif.org/2012-international-tech-transfer-testimony.pdf

Services: promote the ability of consumers to access and distribute the information, applications, and services of their choice; not restrict the cross-border provision of services; not prevent cross-border transfers of and access to information; and not require service suppliers to use local infrastructure or establish a local presence.[2] These principles are not enforceable, whereas TISA presumably will be.

Equally, these demands are not limited to the US industry and advocates. The industry is global. In November 2014 the European technology industry lobby DigitalEurope, which includes Google Inc and Intel Corp, urged the new European Union Trade Commissioner to use TTIP and TISA to '*knock down protectionist rules, including mandatory data localization*'. The group reportedly *'attacked forced technology transfer requirements and forced local ownership of foreign firms' intellectual property, along with restrictions on moving data across borders and rules requiring domestic data centers or data hosting'*.[3]

The Information Technology Industry Council is an industry coalition against 'forced localization' to boost manufacturing, high-tech and R&D capabilities. Among the practices they highlight are '*mandatory technology transfer requirements, local sourcing requirements in government and private sector procurements, the escrow of source code and other sensitive design elements, import restrictions, and restrictions on the flow of data'*.[4]

However there are also tensions between the US and EU, let alone other TPPA countries, potential signatories and GATS parties. *The Wall Street Journal* wrote on 9 December 2014 on a 'pitched battle' between the US technology companies and Europe's sovereign states, which

> pits governments against the new tech titans, established industries *against upstart challengers, and freewheeling American business culture against a more regulated European framework. … Europe's policymakers, accustomed to controlling key sectors of their economies, are struggling to get a handle on the fast-moving newcomers from across the ocean. Growth is weak and government revenues soft, and they see profits that once accrued to European industries from retail to media to taxicabs, being diverted – often lightly taxed – to Silicon Valley. They worry that critical industries, such as autos may fall next.*[5]

The principal targets of the US proposal are not the EU or other current negotiating parties. Certain countries are explicit targets. China was described by one advocate of the US' proposed rules as 'by far the most egregious actor when it comes to forced

---

[2] European Union-United States Trade Principles for Information and Communication Technology Services, 4 April 2011, http://www.ustr.gov/webfm_send/2780, as summarized in Centre for Democracy and Technology, 'Comments on Proposed Transatlantic Trade and Investment Agreement (TTIP)', 10 May 2013, 3

[3] Michael Lipkin, 'EU Tech Industry Wants Data Localization Out Of TTIP', Law360, 21 November 2014. http://www.law360.com/articles/598519/eu-tech-industry-wants-data-localization-out-of-ttip

[4] Information technology Industry Council, 'Forced Localization', http://www.itic.org/public-policy/forced-localization

[5] Tom Fairless, 'Europe vs. U.S. Tech Giants. Discontent on Continent Highlights Battle Over Economics, Culture, Internet Control', *The Wall Street Journal,* 9 December 2014

technology transfer'.[6] This means the US proposal will be especially controversial if the US drops its opposition to China joining the TISA negotiations. Other countries, including Malaysia, Brazil, Portugal, Argentina, Russia, India, Indonesia and Nigeria have also been identified as engaging in 'forced technology transfer'[7] or forced localisation to promote their domestic industry.[8]

Secrecy

The cover sheet of the leaked document confirms that TISA negotiations are intended to be more secretive than the controversial 12-country Trans-Pacific Partnership Agreement (TPPA).

The working documents for the TPPA, including draft texts and position papers, cannot be declassified until four years from entry into force of the agreement or four years after the negotiations are closed (ie. fail).

The equivalent period for the TISA documents is **five years**. That additional year presumably reflects the term of some governments (including the European Commission) and means those who are responsible for the documents no longer hold the same positions and cannot be held to account.

However, the recent criticism by the European Union Ombudsman Emily O'Reilly over TTIP secrecy,[9] and the EU Commission's decision to release its text proposals for TTIP,[10] as well as the EU's release of its draft TISA offer of commitments and some tabled documents, shows that secrecy is not inevitable in contemporary trade negotiations.

That approach has yet to spread to TISA as a whole, and informed debate continues to rely on leaks, such as this one, and the draft financial services chapter of 14 April 2014 that was leaked in August 2014.[11]

Relationship to other negotiations

Aspects of the US proposals are almost identical to the Korea-US Free Trade Agreement (KORUS), which is the most recent US free trade agreement (FTA). Some provisions go much further than KORUS or are new altogether.

There is some crossover between the US proposals for e-commerce, technology and data and the TISA financial services chapter, which has provisions for the supply of cross-border financial services (Art X.8), and for data processing and transfers of

---

[6] Atkinson, 'The Impact of Information Technology Transfer on American Research and Development', 3

[7] Atkinson, 'The Impact of Information Technology Transfer on American Research and Development', 8

[8] The Information Technology Industry Council is an industry coalition against 'forced localization': http://www.itic.org/public-policy/forced-localization

[9] 'EU Ombudsman Demands more TTIP Transparency', 31 July 2014, *EurActive,* http://www.euractiv.com/sections/trade-industry/eu-ombudsman-demands-more-ttip-transparency-303831

[10] 'Commission to further boost TTIP Transparency', 19 November 2014, http://trade.ec.europa.eu/doclib/press/index.cfm?id=1201

[11] The text of the financial services chapter and a preliminary analysis can be accessed at https://wikileaks.org/tisa-financial/

information (Art X.11).[12] A final note on the leaked US document says the applicability of the core rules to financial services is still under consideration.

In the absence of other information, the text should also be viewed as an indication of the likely US position in the TPPA and TTIP. The US dropped a proposal on e-commerce in the World Trade Organization in December 2014, which was presumably similar to this leaked proposal.[13]

Content

The US paper proposes 7 articles:
X.1 Local Presence
X.2 Local Content
X.3 Local Technology
X.4 Movement of Information
X.5 Open Networks, Network Access and Use
X.6 Electronic Authentication and Electronic Signatures
X.7 Exceptions

Articles X.1-4 and X.7 impose the most onerous constraints on governments.

Art X.4 is the most potent, with no provision for any reservations or exceptions. Articles X.5-6 provide much more flexibility, but are entry points for controversial ideas that can be made into more rigorous obligations once they become established as precedents.

The individual provisions are now discussed in terms of their goal, the rule itself, practical implications, legal points, any permitted limitations and exceptions, and possible scenarios.

Article 1: Local Presence

Goal

One aspect of 'localisation' is the requirement that a person or company that supplies a service from offshore has a local commercial presence (such as an agency, branch or subsidiary) or is resident in the country. This is considered an onerous and unnecessary obligation. It also is seen as one way of requiring US companies to bring their technology and knowledge into the country, for example by requiring them to enter into a joint venture with a local firm that then gains access to the technology and skills.

Rule

This rule is the same as in KORUS (Arts 12.5 and 12.6). It says that having a local presence cannot be made 'a condition' for the cross-border supply of the service.

[12] The text of the financial services chapter and a preliminary analysis can be accessed at https://wikileaks.org/tisa-financial/
[13] 'The US Paper on E-Commerce', *Washington Trade Daily*, 1 December 2014 (paywall)

Legal points

Several legal points arise:

- ***'as a condition for the cross-border supply of a service'*** implies that this rule would only affect services that require some form of approval.

  Many e-services, such as retail, entertainment, some forms of education or even health advice, are provided without prior approval and already pose some of the above problems.

  If an e-service that currently does not require authorisation, and was later made subject to approval, this rule would then apply.

  This rule would certainly apply to services that can only be supplied within the country by authorised or registered providers or licensed operators, such as accounting, law, medicine, engineering, financial service advice and banking and insurance services.

- ***'a service supplier … to be resident'*** is likely to extend to all elements of the supplier, including governance. That would prevent a requirement that there be one or more director resident within the country.

- ***'commercial presence'*** is defined in the GATS as any type of business or professional establishment, including through a legal person (a company etc), a branch or representative office.[14]

Limitations and exceptions

The provision would allow each country that was party to TISA to limit or qualify the application of this rule.

But a government cannot simply list the kind of service suppliers and services it is willing to make subject to the rule. Instead, they must list any limitations or conditions or qualifications they want to apply to services suppliers and their services in the future (a negative list). It is not clear whether the general rules on TISA will provide additional restrictions on governments' annexes.[15]

A negative list of limitations would restrict a country to those that they nominated at the time the agreement was concluded (or they joined it). The final lists will have been subject to negotiation with other countries that try to prune them back. It will presumably be very hard to add anything to the list later, and concessions would usually need to be made in other services areas if new restrictions on e-commerce were approved.

Yet the kind of restrictions that a country believes are necessary for a particular service supplier or service will change over time, especially in e-commerce where new services and new risks are constantly arising.

No government has a crystal ball that allows them to foresee the need to list them now – and other governments would probably reject them as unnecessary.

---

[14] GATS Art 28(d)

[15] The same approach is taken in the TPPA.

Practical implications

These days services are supplied across the border mostly by the Internet, although telephones and traditional mail delivery are still used. People also travel to another country to use a service.

Governments have many reasons why they may want to insist that a foreign supplier of a service has a local presence, which are not simply about forced technology transfer. These include:

- Application of quality assurance standards to the provider and/or its activities
- Application of consumer protection laws/codes to the provider and/or its activities
- Inspection and monitoring of compliance with those obligations
- Civil legal action by consumers for breach of those obligations
- Civil or criminal enforcement action by state agencies for noncompliance
- Enforcement of orders for compliance, compensation, or penalties
- Fiscal loss due to exemption from consumption and income tax
- Competition effects on local firms of exemption from consumption and income tax, and added costs of maintaining local facilities
- Depletion of local face-to-face facilities
- Loss of local employment and training opportunities
- Capital outflows and lack of reinvestment in local economies.

It can already be difficult for governments to achieve these outcomes, especially where foreign firms can minimise their local legal presence and capital backing. Consumers already face problems when they buy products through cross-border e-commerce and have few, if any, practical and legal protections. Governments can and do seek to make regulation more effective when there is a local presence.

Imagine …

- A government is unable to stem the loss of tax revenue from consumption tax and income tax by requiring Amazon and Google to have a local presence, which is a requirement for levying such taxes in some countries.
- An offshore financial services provider gives negligent or fraudulent advice to a local council, which loses a large investment. If the supplier is subject to home country regulation, that does not provide any guaranteed protection as some countries have weak risk-tolerant regulation – as the Icesave investors in the UK and Netherlands discovered when Iceland's poorly regulated banks failed.
- A mining company outsources its computerised operations to an offshore IT company. The software fails or the company is negligent, resulting in an explosion that causes illness and property damage. The local mining company may be held liable domestically for the harm, but the offshore company cannot be held to account.
- Reading of x-rays is outsourced to radiographers in another country. The reading is incorrect and the patient suffers serious harm. The radiographer may have been negligent or misrepresented their qualifications to their offshore employer. The patient has no means of taking action against the offshore radiographer or their employer because the law is weak, it is too costly or difficult, the radiographer does not have the requisite insurance, or the

insurance company will not pay where the patient is located offshore. Whether the local health provider who relied on the service is liable would depend on the domestic law and the rules of their insurers, and the resources of the patient to pursue a claim.

Article X.2: Local Content

Goal

Local content requirements are another form of 'localisation' that the US industry objects to. The US wants to ensure that governments do not require firms that supply a service (from media to retail to IT) to buy or use a proportion of locally produced goods and services. That reflects a long-standing opposition to local content requirements as barriers to trade in goods and services. With the increasing use of Internet as the delivery mechanism, an exemption for digital platforms from traditional local content requirements means their impact can be eroded without having to remove them.

The rule

A government cannot require a service supplier (foreign or local) to buy, use or give a preference to

- locally produced goods or locals who supply goods;
- e-content that was created, produced, published, contracted for or commissioned in a particular country (that could be any country)
- e-content on the basis of the nationality of the author, performer, producer, developer or owner (again, they could be from any country)
- computing facilities located within its country
- computer processing or storage services supplied from within its country.

A government also cannot require a service supplier engaged in marketing or distributing goods or e-content to buy, use or give a preference to

- goods that were produced locally;
- e-content that was created, produced, published, contracted for or commissioned in a particular country (that could be any country)
- e-content on the basis of the nationality of the author, performer, producer, developer or owner (again, they could be from any country).

The government cannot impose or enforce such a requirement on a service supplier, or enforce a commitment or undertaking the service supplier has made to that effect, or make it a condition of receiving an advantage (such as a subsidy or other benefit).

Legal points

This provision is a variation and expansion of the rules that prevent governments from imposing performance requirements on foreign investors, in KORUS Art 11.8 and the leaked TPPA investment chapter (Art 12.7). Importantly, those provisions only apply to foreign investors.

This are supplying the service or purchasing the good for distribution is far more sweeping.

The obligation applies to ***all service suppliers***, ***including domestic private firms and state-owned enterprises***.

The rules would apply to ***existing and future suppliers*** of services from the time TISA comes into force.

The restrictions apply to '***in connection with the supply of a service'.*** That is wide reaching as it applies to all direct and indirect elements in the supply chain of a service.

The e-content rules (Art X.2.1(a)(ii)) ***prevent a government from specifying which country the content or its creator must come from***. That applies to any country (for example, with which there is a co-production agreement for films, or is part of an economic integration arrangement).

Art X.2.1(a)(ii) applies only to ***electronically transmitted content***. That allows a government to continue to impose local content obligations for non-digital transmission, but prevents the governments from imposing the same requirement on any supplier of electronically transmitted content or online platforms.

Art X.2.1(b)(ii) extends the ***same rule to marketers or distributors*** of electronically transmitted content, such as Amazon and Kindle.

The e-content rule applies to content that is ***digitally encoded*** (fn1). The US has long argued that electronic delivery of tangible goods and non-IT services should be governed by rules on e-commerce, computer and telecom services. That proposal has been especially fraught where governments have sought to protect ***cultural content*** by special rules in goods and services chapters, and protect them in their schedules of commitments.

Art X.2.1(a)(iii) would prevent a government from ***requiring computer facilities, including servers, to be located within its territory*** and the process of data to take place within the country.[16] Annex 13B of KORUS and Article X.11 of the leaked TISA financial services text contain prohibitions on localisation, but only for financial services.

The inclusion of a ban on requirements to ***hold and process data locally*** (Art X.2.1(a)(iii) in a provision that purports to be about local content reduces the visibility of this ban.

It might be argued that Art X.2.1(b)(i) is an indirect restriction on ***geographical indicators***, as a marketer or distributor cannot be required to buy, use or make available goods of domestic content.

[16] This ban is consistent with the statement from US E-Commerce negotiator Christine Bliss at an event hosted by the Brookings Institution on 25 September 2014 that they were negotiating in the TPPA 'a rule prohibiting the requirement that countries require servers to be located within their own territory' and 'we are also pursuing similar requirements in TISA' (see Article X.4 below) http://www.brookings.edu/~/media/events/2014/09/25%20internet%20fracture/092514_internet%20fracture_transcript.pdf

Limitations and exceptions

As with Article X.1, governments can limit the application of these obligations, but must use a ***negative list*** approach. The same problems apply as identified above.

There is an additional problem that a negative list assumes that the subject of the exemption is known. ***Future digital platforms*** are by definition unknown and unknowable, and may therefore not be protected.

That will depend on what form the annexes take. Some negative list approaches allow two annexes: one for existing non-conforming measures, and one for exemptions from the rules. However, the leaked financial services chapter of TISA proposed a draconian 'standstill' rule that would make it impossible for governments to retain the right to adopt new more restrictive regulations in the future. A similar approach might apply to TISA as a whole.

If governments do not, or cannot include reservations that require the holding of data within their territories they will lose the right to do that in the future, even if they do not have that requirement now.

Article X.7 suggests the US would reject the application of a ***cultural exception*** to these provisions (see below)

Paragraphs 2 and 3 provide tailored exceptions to address the US's sensitivities:

- content levels that are necessary for goods or services to qualify for export promotion and foreign aid programmes; and
- content requirements (rules of origin) that goods must meet to take advantage of preferential tariffs or quotas.

Practical implications

Many countries require a service supplier, such as movie theatre chains or broadcast media (radio and TV), to include a proportion of local services content. That serves cultural and social purposes, such as promotion of culture, language and identity, especially indigenous or minority cultures, as well as supporting the local cultural sector. Internet is now becoming the main delivery medium for content, overtaking terrestrial broadcasting.

A government would not be allowed to extend the local content quotas it has for traditional terrestrial broadcasting to transmission of content and information over the internet[17] to ensure those benefits are not eroded, even for public broadcasting via the Internet - for example, Italian regulators decided in late 2010 to impose broadcast regulations on video-hosting websites that included content requirements.[18]

---

[17] This restriction was advocated by Centre for Democracy and Technology, Comments on Proposed Transatlantic Trade and Investment Agreement (TTIP), May 2013, p.4 https://www.cdt.org/files/pdfs/CDT-TTIP-Comments-5-10-13.pdf

[18] It is not clear from available reports whether these include local content as well as viewing times for certain content, but such a measure could cover both. See Wendy Zeldin, "Italy: Video-Sharing Sites to Be Viewed by the Law as Television Broadcasters", Library of Congress Global Legal Monitor, Jan. 13, 2011 http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205402469_text, quoted in Centre for Democracy and Technology, Comments on Proposed Transatlantic Trade and Investment Agreement (TTIP), May 2013 https://www.cdt.org/files/pdfs/CDT-TTIP-Comments-5-10-13.pdf

Public broadcasters are especially vulnerable. Many are required to give preferential treatment to local content, and are subsidised (receive an advantage) to do so.

A number of TISA negotiating parties (not the US) are parties to the UNESCO Convention on Cultural Diversity. The Convention espouses the principle of complementarity between economic and cultural aspects of development, noting 'the cultural aspects of development are as important as its economic aspects, which individuals and peoples have the fundamental right to participate in and enjoy'.[19] This proposed article violates that balance.

An internet retailer like Amazon could not be required to make available national cultural products as a condition of selling into the country.

Other forms of commerce are also affected. Distributors may be required to include a proportion of local products, such as supermarkets selling a mix of locally grown and foreign grown fruit and vegetables, or hotels using some local food and cosmetic products.

Governments will not be able to require servers to be situated within the country. That poses serious concerns about the ability to ensure that domestic laws on privacy and protection of health information, non-trading in personal information and consumer protection apply to personal or commercial data.

A government can still require a service supplier to do certain things within the country as a condition of receiving an advantage, such as a subsidy or other special treatment. But this is a closed list of five possible conditions, which means no other conditions can be imposed. The five are:

- Locating production in a certain place
- Supplying a specific service
- Training or employing workers
- Constructing or expanding certain facilities
- Carrying out research and development.

Article X.3: Local Technology

Goal

The US wants to ensure that governments cannot impose obligations on firms that disadvantage its control and commercial gains from intellectual property and technology and undermine its competitive advantage. Industry claims that 'innovation mercantilism' in areas like ICT, renewable energies and biotech is anticompetitive and constitutes theft.[20] 'Forced technology transfer' is a major focus

[19] Formally called the Convention on the Protection and Promotion of the Diversity of Cultural Expressions 2005. http://portal.unesco.org/en/ev.php-URL_ID=31038&URL_DO=DO_TOPIC&URL_SECTION=201.html

[20] http://www.itif.org/publications/localization-barriers-trade-threat-global-innovation-economy

of electronic and IT industries across the US, EU and Japan.[21] Industry has made it clear that China is a prime target, but not the only one.[22]

The rule

A government cannot require the following, if the aim is to protect or privilege its local services, service suppliers or technology:

- the transfer of a particular technology or proprietary knowledge to a local person or firm;
- purchase, use or given preference to technology produced by the state or its locals, or
- preventing a particular technology being bought or used in the country.

A government cannot enforce an existing requirement, commitment or undertaking of those kinds, if it has that purpose.

Legal points

This provision complements ***Article X.1.*** If a government cannot require a service supplier to have a local presence (eg joint venture with local firm) it cannot impose requirements for technology transfer.

The scope is broad. As with Article X.2 it covers a requirement '***in connection with'*** the supply of a service, not just the supply of the service itself. That would involve inputs to the activity, underlying R&D, technology specifications and knowhow.

There is no reference to the nature of the entity to which the rule applies. It therefore ***applies to any entity, local or foreign, state or private***.

The rule on purchase, use and preferences for local technology only applies where the government's motivation for imposing or enforcing such requirements is '***to afford protection on the basis of nationality'*** to its own services, service suppliers and technology.[23] That means the government must be taking those actions with the aim of achieving that outcome. That means another Party that complains would have to show that protectionism is the aim of the requirement.

Limitations and exceptions

As with Article X.1, governments can limit the application of these obligations, but must use a negative list approach. The same problems apply, as above.

Compulsory licenses have been seen as a tactic to transfer know-how and technology and an indirect form of forced localisation.[24] Article X.3 provisions do not apply where a government has permitted use of a patent without authorisation of the right holder (compulsory license or government use), on the terms of Article

[21] Jimmy Goodrich, 'Global IC industry agree to enhance joint efforts to tackle Forced Localization Measures', 17 October 2014, http://blog.itic.org/blog/global-ict-industry-agree-to-enhance-joint-efforts-to-tackle-forced-localization-measures

[22] Atkinson, 'The Impact of Information Technology Transfer on American Research and Development, p.10 http://www2.itif.org/2012-international-tech-transfer-testimony.pdf

[23] This provision is basically copied from the leaked TPPA investment chapter (Art 12.7.1h) http://www.citizenstrade.org/ctc/wp-content/uploads/2012/06/tppinvestment.pdf and the US Model Bilateral Investment Treaty (Art 8.1h) http://www.ustr.gov/sites/default/files/BIT%20text%20for%20ACIEP%20Meeting.pdf

[24] http://www.itif.org/publications/localization-barriers-trade-threat-global-innovation-economy

31 of the WTO Agreement on Trade-Related Aspects of Intellectual Property (TRIPS). However, that provision is restrictive and the government needs to negotiate with the rights-holder for a voluntary licence, unless there is a public health crise or public non-commercial use. If the negotiations are not successful, the government can issue a compulsory license, subject to adequate compensation.

TRIPS Article 39 provides protection for 'undisclosed information' against unfair commercial practices. Article 39.3 deals with a specific type of undisclosed information required by governments – certain test and other data. Under Article 39.3 the public is the ultimate beneficiary of the information that is submitted to regulatory authorities; those authorities can disclose the information to protect the public interest, including public health.

The provision does not provide enough shelter to countries. For all the TRIPS safeguards to apply the provision would need to state "except as provided for in TRIPS". If not, it would at least need to enumerate more articles, for example TRIPS Article 30 (exceptions to rights conferred), Article 44 (injunctions) and Article 66 (technology transfer to least-developed country members).

There is a further exception (Art X.3.2(b)) where the country's courts or competition authority has imposed these requirements to remedy what it considers an anticompetitive practice under domestic law. However, this only applies to the technology transfer issues in this Article. Complaints that entities like Google are too big and need to be split is not relevant to these rules. There may be some other rules in TISA on domestic competition, but that is not known.

Practical implications

Access to technology is important for general economic and social development. Developed countries object to achieving this through compulsory licensing provisions on the basis that developing countries should rely on technology transfer. But this provision would restrict their ability to require technology transfer.

Technology transfer is especially in areas like climate change mitigation and adaptation where countries need to build own technologies, as recognised in the Framework Convention on Climate Change.

The industry lobby and its supporters argue that countries should not take shortcuts using 'forced technology transfer' to achieve the same level of R&D and technological development as other countries have now achieved.

China is accused of such practices in areas like IT, air transportation, power generation, high-speed rail, agricultural sciences, and electric vehicles.[25] On one hand, China is accused of dirty technologies, on the other it is not allowed to expedite the development of alternatives.

Other examples include:

- Portugal requiring wind companies wanting to access its market to partner with a local university to conduct clean technology research;

[25] Atkinson, 'The Impact of Information Technology Transfer on American Research and Development', p. 6

- Malaysia's official policy 'to use government procurement to try to force the transfer of technology from foreign to domestic industries'; and
- Indonesia's requirement that foreign pharmaceutical companies manufacture locally or entrust a company registered as a manufacturer into Indonesia with obtaining drug approvals for them. [26]

Article X.4: Movement of Information

Goal

The US wants to ensure that any firm can move its data in and out of other countries, process and store it within or outside that country's territory. That means a government cannot require that data is held or processed within its territory.

The rule

A government cannot stop a service supplier from another TISA country from transferring, accessing, processing or storing information in its country or any country in the world, when those activities are connected to the service supplier's business.

Legal issues

This proposal is far more extensive than KORUS (Art 15.8), which requires parties to ***endeavour*** to refrain from imposing or maintaining ***unnecessary*** barriers to electronic information flows across borders'. The TPPA reportedly goes further, and says parties ***shall*** refrain from imposing or maintaining ***unnecessary*** barriers to electronic information flows across borders to be a direct obligation in TPPA.[27] This provision goes even further, by imposing a strict prohibition.

The transfer, processing etc of the data has to be carried out '***in connection with the conduct of the service suppliers business'***. As noted above, this can be an input or incidental to the business. 'Service suppliers business' means anything connected to the business, including its operation as a business, not simply the 'service' or the 'supplying of the service'. Very few dealings with data would not be caught within that broad wording.

The data explicitly includes '***personal information'***. The exception provision X.7 contains no protections for privacy. If this were adopted in TISA in relation to the e-commerce chapter it would presumably preclude the application of any privacy provision in the general exception. In any case, the privacy protection in the general exception of GATS is weak and self-cancelling.

The government cannot ***prevent the data being held or processed*** in another country. There are two possible interpretations. One is that a government cannot prevent a service supplier from transferring, processing and storing data in their country of choice, even if it does not comply with any conditions that source country might impose on acceptable protections for information. That is probably the meaning the US intends.

---

[26] Atkinson, 'The Impact of Information Technology Transfer on American Research and Development', p. 8

[27] Bliss http://www.brookings.edu/~/media/events/2014/09/25%20internet%20fracture/092514_internet%20fracture_transcript.pdf

A more tenuous interpretation would treat '***prevent'*** as a conclusive action. Specifying a list of countries to which data can be sent is not 'preventing' its movement offshore, merely setting conditions on which offshore locations are acceptable. This approach that would allow a government to restrict the countries in which data can be located, or require that ***minimum legal protections*** exist in such a country, such as the EU Data Protection Directive. However, that interpretation is probably not what the US intended.

The list of activities does not include ***commercial use or sale***. The nearest term is 'processing',[28] and the definition in the EU Data Protection Directive would not include commercial use or sale.

As noted above, Articles X.2 and X.4 cross-fertilise. Art X.2 says a government cannot require local servers, and Article X.4 says the government cannot prevent the movement of data or its local processing or storage.

The provision is silent on the matters of ***privacy and data protection***.

Exceptions

This provision is not subject to the exceptions in Article X.7, or to any scheduled conditions, limitations or qualifications. Nor is there any ability to designate a certain kind of data, such as health information, as an exception. ***There appear to be no exceptions permitted at all.***

As noted below, there is no equivalent reference to privacy in Article X.7 to that contained in the GATS Article XIV. However, that is irrelevant, as Article X.7 does not apply to Article X.4.

A government would have to rely on ***whatever general exceptions might exist*** in TISA relating to consumer protection, privacy, fraud or national security. All except for national security exception are weak and subject to conditions that are extremely difficult to satisfy.

Practical implications

There can be no requirement that data is held locally.

Assuming the first legal interpretation of 'prevent data being held', the EU privacy directive would be overridden. The second interpretation would mean the EU could require personal information is only held in safe countries or in accordance with the safe harbour rules could still apply.

If the second interpretation is incorrect, then a government would have no ability to impose any restrictions to stop the transmission or storage of data in countries that have weak or no privacy or data protection, or that have extensive national security laws that enable ready access to data held within its territory.

A government could also prevent a service supplier from selling data, including personal information, to advertisers and other third users.

---

[28] EU Directive 95/46/EC - The Data Protection Directive, Article 2 - definitions (b) "processing of personal data" ("processing") shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

Article X.5: Open Networks, Network Access and Use

Goal

The US proposes open Internet rules, but it wants to give the ISPs legal room to manage the Internet according to the ISP's preferences and commercial interests.

The rule

Local 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, provides that doesn't harm the network; and
- access information on network management practices of those who supply their access to the Internet.

Legal observations

This is a soft obligation, couched in language of '***recognizes'*** that consumers '***should'*** be able to do those things. But what begins as a soft obligation is an entry point that over time creates a precedent, which can progressively become more onerous.

'Reasonable network management' is code for an exception to ***'net neutrality'***, whereby everything on the Internet is treated the same. There is no guidance on the meaning of 'reasonable network management'. The concept has been highly controversial when the US Federal Communications Commission (FCC) proposed it in the US. The FCC says it 'consists of practices which are reasonable', which is a vague and circular meaning that could be a rubber stamp for anything the network operator wants to do. [29] The term 'reasonable network management' is not used in the equivalent provision in KORUS

'***Connect their choice of devices to the Internet that do not harm the network'*** is part of the set of Open Internet principles issued by the FCC in 2005.[30]

KORUS Art 15.7(d) says consumers should have ***access to competition*** among providers. That is not in the US's TISA proposal. However, competition is likely to be covered in another part of TISA. Instead Article X.5(c) says consumers are entitled to ***information about the network management practices*** of their Internet providers.

---

[29] Clear Standards for Reasonable Network Management, available at http://www.savetheinternet.com/blog/10/01/20/clear-standards-reasonable-network-management

[30] See, FCC Adopts Policy Statement New Principles Preserve and Promote the Open and Interconnected Nature of Public Internet, 2005 available at https://apps.fcc.gov/edocs_public/attachmatch/DOC-260435A1.pdf

Exceptions and limitations

Article X.7 does not apply to this provision. However, the obligation is soft, and is explicitly subject to applicable domestic laws and regulations.

Practical implications

Net neutrality is a hotly debated and controversial topic in the US, EU and elsewhere, and is currently the subject of domestic debate in this countries. Including the opaque term 'reasonable network management' into the TISA provision seeks to circumvent that debate. The Internet needs to remain open and neutral to keep its innovative character, enhance access to knowledge and freedom of speech.

Thus the principles of openness and neutrality require special protection. ISPs have economic incentives to promote their own products and services by degrading the experience of competing products and services, unless they are constrained by regulatory mechanisms. Subjecting consumers' access, use of services and applications to 'reasonable network management' can undermine the principles of openness and neutrality.

'Reasonable network management' is not a purely technical concept (and in any case technical is never neutral). Moreover, the conditions under which network management might be considered reasonable, and who determines that, is not specified, and implies that it may be left to the ISP to decide. There is no requirement that the public interest infrastructure and consumer interest are relevant factors in determining 'reasonable'.

Article X.6: Electronic Authentication and Electronic Signatures

Goal

The US wants to minimise the restrictions on use of electronic signatures and electronic transactions.

The rule

A government cannot deny the legal validity of a signature just because it is electronic.

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.

Nor can a government prevent parties to an electronic transaction from proving to judicial or administrative bodies that their transaction complies with the law in relation to authentication.

Legal observations

The rules on acceptance of e-signatures themselves are strong, but a government can deviate from them by provisions in its domestic law.

This proposal is a step back from KORUS Art 15.4, because the entire provision is subject to domestic law.

KORUS Art 15.4.3 also allows 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'.

Exceptions

Domestic laws can prevent or limit legal recognition of electronic signatures as valid.

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 a category might be, and therefore no limitation to its scope. It is unclear whether there can be more than one such category.

Even the weak and circular exception for fraud in the GATS Article XIV is not included in Article X.7.

Article X.7: Exceptions

Goal

The US has provided minimal scope and flexibility for governments to limit their obligations under these proposals by narrowing the scope of the normal exceptions.

The rules

Three 'exceptions' apply to the provisions on Local Content (Art X.2) and Local Technology (Art X.3).

- The proposed rules only apply to the specific obligations, commitments, undertakings and requirements mentioned in them.
- An obligation, commitment, undertaking or requirement between private parties can still be enforced so long as the government did not impose or require it.
- A government can still adopt or keep an existing measure that relates to the conservation of living or non-living exhaustible natural resources, but only if it is not a 'disguised' way of restricting international services transactions, or is applied in an 'arbitrary or unjustifiable manner'.

A fourth exception protects the right of a government to take any action it deems necessary to protect its essential security interests.

Legal points

By specifying an exception that applies to these rules, the US clearly aims to ***exclude the application of any general exception*** to these rules. That is inconsistent even with previous US FTAs, where the e-commerce chapter imposed weaker obligations on countries. For example, the e-commerce chapter in KORUS is subject to the general exception used in the GATS.

The EU has also proposed the adoption of the GATS general exception in TISA. However, that standard general exception is subject to requirements of 'necessity', not involving 'arbitrary or unjustifiable discrimination' and not a 'disguised restriction on trade in services', which sets a threshold that has almost never been met.[31]

[31]Public Citizen. 'Only One of 40 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', https://www.citizen.org/documents/general-exception.pdf

The ***scope of Article X.7 is much narrower*** than the general exception in the GATS or US FTAs. GATS Article XIV allows limited government flexibility for measures:

- Necessary to protect ***public morals*** or to maintain ***public order;***
- Necessary to protect ***human, animal or plant life or health***;
- Necessary to secure compliance with laws or regulations *which are not inconsistent with the agreement* (a phrase which makes this paragraph effectively self-cancelling) relating to
    - deceptive and ***fraudulent*** practices or default on services contracts,
    - the protection of ***privacy of individuals in relation to processing and dissemination of personal data and protection of confidentiality of individual records and accounts***,
    - and safety;
- Tax equity and avoidance of double taxation.[32]

The exception in Article X.7 applies ***only to conservation of living and non-living exhaustible natural resources***. The burden of proof is on the government invoking it. It is subject to further requirements that it is not used in an arbitrary or unjustifiable manner or is a disguised restriction on trade in services.

Article X.7 only applies to Articles X.2 Local Content and X.3 Local Technology. That means this minimal degree of flexibility is provided for those provisions, but ***no equivalent flexibility for the rules on local presence and movement of information.*** Governments would need to rely on their annexes or the national security exception.

The rules on ***open networks and electronic authentication are both subject to domestic laws***.

Article X.4 makes no provision for limitations or reservations. ***The only exception for movement of information is for national security.***

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.

[32] The limitations of this exception are not discussed here.