APPENDIX 4
THE E-COMMERCE ANNEX

Chapter 3 explained the context of the push in TiSA and other mega-agreements to secure globally binding rules on electronic commerce. That is a theme that runs throughout the TiSA text, from the core rules to the countries' schedules of commitments and the annexes, in particular the Annex on Electronic Commerce.

What is e-commerce?

Electronic commerce is not defined in TiSA. The WTO defined it simplistically as 'the production, distribution, marketing, sale or delivery of goods and services by electronic means', although that was solely for the purpose of discussions within the WTO working group on electronic commerce (established in 1998).[1] The OECD uses a more detailed definition:

> *An e-commerce transaction is the sale or purchase of goods or services, conducted over computer networks by methods specifically designed for the purpose of receiving or placing of orders. The goods or services are ordered by those methods, but the payment and the ultimate delivery of the goods or services do not have to be conducted online. An e-commerce transaction can be between enterprises, households, individuals, governments, and other public or private organisations.*

Whether a transaction is e-commerce would be defined by the method of placing the order. Orders made over the web, extranet or electronic data interchange are included; those made by telephone calls, facsimile or manually typed e-mail are not.[2]

E-commerce transactions are usually classified by four kinds of relationships, and are increasingly conducted across the border:[3]

- **Business-to-business (B2B),** which covers sales from producers to retailers, and transactions along supply chains, warehousing and logistics operations (the top 20 B2Bin 2016 included Huawei, IBM, Microsoft, Wells Fargo, Exxon Mobile, HSBC, Citi and Fedex);[4]
- **Business-to-consumer (B2C),** sales of goods and services online through direct purchase (eg. online insurance, Amazon, AliBaba), electronic marketplaces (eg. Expedia, Uber) and multi-channel retailing options (eg. Walmart, Tesco);
- **Consumer-to-consumer (C2C)** that connects people online, including through auctions, advertising and social media (Airbnb, eBay,[5] Facebook);
- **Business-to-government (B2G)** where governments purchase goods and services online, including significant government procurement contracts.

The actual product being bought and sold may be tangible goods, services that are organised online but delivered in person, or digital goods and services. Payment is generally on-line through separate

1 WTO General Council, 'Work Programme on Global Electronic Commerce', adopted on 20 May 1998, WT/L(274), 30 September 1998, para 1.3

2 OECD Glossary of Statistics Terms, https://stats.oecd.org/glossary/detail.asp?ID=4721

3 UNCTAD, *In Search of Cross-Border E-Commerce Trade Data,* Technical Note no.6, TN/UNCTAD/ICT4D/06, April 2016, p.1, Box 1.1

4 'Top 20 most valuable B2B brands revealed', B2B Marketing, 8 June 2016, https://www.b2bmarketing.net/en-gb/resources/news/top-20-most-valuable-b2b-brands-revealed

5 As with others, eBay also does B2C

payment systems, such as credit cards or PayPal, but can be at point of delivery. Sales and follow-up support for intangible services, such as insurance, ISPs or online courses, can be produced purely online. Many online services dealing with goods still require physical delivery, which engages postal, courier, logistics, and multi-modal transport.

Regulating telecoms, not the Internet

Telecommunications and the Internet operate as an integrated service. However, US free trade agreements have distinct annexes on telecommunications and e-commerce. That is because the US will not agree to anything in such agreements that requires it to change its laws,[6] and the US maintains two distinct regimes.

Historically, AT&T operated as a private monopoly. It was broken into regional operating monopolies in 1984. The Telecommunications Act of 1996 required the regional Baby Bells to open their networks to competitors. The statutory goal was to '***promote competition and reduce regulation in order to secure lower prices and higher quality services for American telecommunications consumers and encourage the rapid deployment of telecommunications technologies***'. Despite that, ownership of the traditional telecommunications networks has remained highly concentrated.

Meanwhile, the Internet was evolving. Even though computer users connected through the telephone network, first using the copper loop and then fibre-optic cables, the regime for regulating the Internet reflected the defence and security context in which it was developed. Under the Telecommunications Act it became US policy to '***preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation***'.[7] The US has ensured that the Internet and other interactive computer services have been effectively quarantined from the International Telecommunications Union (ITU) as the international standard setting body. Hence, TiSA has separate annexes on electronic commerce and telecommunications.

The e-commerce annex

An annex dedicated to e-commerce is a must-have for Team TiSA, on top of the core rules and schedules that guarantee access to countries' markets and non-discrimination.[8] Although the annex is notionally about services, it is really making binding and enforceable rules to facilitate the networked economy. Successive versions of the annex have been leaked. While there are strong similarities to the US-led e-commerce chapter in the TPP, there are differences and disagreements that reflect the sensitivities of other TiSA parties.

As of November 2016, there were three documents setting out text on e-commerce: the full Annex on Electronic Commerce,[9] a 'Small Group Non Paper' on a number of provisions,[10] and a 'Non-Paper TiSA Landing Zone' from the US on Article 2: Movement of Information. The documents indicate a significant level of disagreement on basic rules. The annex is not limited to *cross-border* electronic commerce. Indeed, very little of it is about commerce *per se*. The main purpose is to restrict government regulation of the digital domain and the operations of the major tech companies and other transnationals. This analysis evaluates four substantive elements of the annex, the first of which is the most important:

i. ***Prohibiting national regulations*** that require local storage and processing of information, transfer of or access to source code, use of local computer facilities, local content in electronic transmissions, no ISP liability for uploaded content;

6 United States, *Cyber Security Strategy and Programs Handbook, Vol 1: Strategic Information and Developments*, International Business Publications, 2017, 153-55

7 Code 47 U.S.C.¶230(b)

8 AT&T, BSA Software Solutions, Cisco Systems Computer and Communications Industry Association, Consumers Electronic Association, Computer & Communications Industry Association, ebay, Express Association of America, Google, IBM, Information Technology Industry Council, Intel, Microsoft, Oracle Corporation, Software and Information Industry Association, TechAmerica, Verizon, Western Digital

9 TiSA, Annex on Electronic Commerce, undated (November 2016) http://www.bilaterals.org/IMG/pdf/annex_on_electronic_commerce.pdf

10 http://www.bilaterals.org/IMG/pdf/ecommercenonpapersmallgroup.pdf

ii. ***Weak privacy and consumer rights*** involving online consumer protection, personal information protection, unsolicited commercial electronic messages, and conditional access to and use of the Internet and open networks;

iii. ***Strong state security powers*** that allow deviations from the provisions on a self-judging basis, including from already weak protections; and

iv. ***Streamlining actual cross-border commerce*** through electronic authentication and e-signatures, no customs duties, and international cooperation.

Scope of coverage

The annex needs to be read alongside each party's commitments to the market access and non-discrimination (national treatment) rules in their annexes, and the restrictions on regulating licensing requirements and procedures and technical standards in the domestic regulation annex. Commitments to remove restrictions in cross-border services (mode 1) are especially important, whether they are for computer-related or substantive services like health, financial or audio-visual services. If the principle of technological neutrality is accepted (see Chapter 5), the restrictions in this annex would apply to digital delivery of services in ways that were never foreseen by governments when they drafted their schedules.

It had not been agreed, as of November 2016, whether the annex would apply to financial services. Switzerland wanted them excluded; other powerful countries wanted them covered, although the US had a complicated proposal that is discussed in Appendix 6: Annex on Financial Services.[11]

There was no agreement in the leaked text from November 2016 on the status of **government data**. A large number of countries want to exclude information held or processed by or for the government, or measures related to such information, including its collection.[12] If accepted, that would apply to all levels of government. The US is considering whether to support this and the EU has not taken a position.

Proposals to exclude other key public policies of subsidies and grants,[13] and government procurement,[14] were also still being debated. However, government procurement would have a very limited meaning; at most it would protect purchasing for the internal purposes of government agencies. The procurement of e-commerce activities provided by the government that people might have to pay for, such as on-line services and facilities, would still be covered by the text.

There was also no agreement by November 2016 on whether countries would be allowed to schedule restrictions on the application of the most significant obligations dealing with movement of information, location of computing facilities, source codes and local content.[15] The US was 'considering' the possibility and the EU was silent on it. The Small Group Non Paper proposed allowing some limitations, but only on a negative list basis: governments would have to list any measures, limitations and conditions they want to keep with no realistic chance of adding to it in the future. These limitations might be added to a country's main schedule or in a separate schedule. As the Internet Digital Economy Alliance remarked: 'A negative list approach is much more future proof, but also means that countries must be comfortable with the idea that over time the commitments to liberalization they are making will expand automatically'.[16]

Protecting digital providers from national regulation

The five most important provisions of the annex reflect the industry wish-list.

11 TiSA, Article 1.6, Annex on Electronic Commerce, undated (November 2016). The EU, US, Australia, Canada, Chile, Iceland, Norway, Peru.

12 TiSA, Article 1.5(c) Annex on Electronic Commerce, undated (November 2016). Supporters are Australia, Canada, Chile, Colombia, Costa Rica, Iceland, Japan, Mauritius, New Zealand, Pakistan, Peru, South Korea, Taiwan, Turkey.

13 TiSA, Article 1.5(b), Annex on Electronic Commerce, undated (November 2016)

14 TiSA, Article 1.5(a), Annex on Electronic Commerce, undated (November 2016)

15 TiSA, Article 1.4, Annex on Electronic Commerce, undated (November 2016)

16 International Digital Economy Alliance, 'The Trillion Dollar Question: How trade agreements can maximize the economic potential of data in the networked economy and support the Internet as the world's trading platform', 2013, Fn 12, p.3

Unrestricted movement of data (Article 2)

The primary goal of the Team TiSA lobby is to prohibit a government from requiring that data is held inside its territory, which they argue prevents them taking advantage of economies of scale, state of the art technology, and in-house expertise. The description of such policies as 'forced localisation of data' or 'data protectionism' is a crude attempt to transfer the negative connotations of trade protectionism from goods to the totally different issue of control over data.

The basic rule says no TiSA party can require a service supplier from another TiSA party to hold data inside its country where the supplier is transferring the data *in connection with* its business. The information transferred offshore can include personal information. For example, the EU could not require an Australian transport company operating in Germany to hold data regarding its loads and drivers' hours within Germany or Europe; likewise, the Canadian government could not require an American health insurance provider to hold data on its clients within the country. There is no suggestion that a government could even specify a list of acceptable countries where its data could be held and processed. The restriction is very broad, as it does not say the transfer is necessary for the business, just done in connection with it.

There are several variations. The US proposed 'landing zone' would apply to the transfer and processing of information within or outside the territory.[17] A number of mainly TPP countries[18] want to retain the right to require information to be *processed* inside the country, presumably so local rules apply, and to restrict the movement of information *within* the country (the reason for that is not clear).

The leaked text showed broad agreement to the rule, but strong disagreement about whether and how it might be limited. There were three options:

1. As discussed above, a number of countries want to limit their exposure to this rule in their schedules, but on a negative list basis that identifies the measure, activity or sector that is not subject to the rule.[19] It is unclear whether this would allow a full policy space reservation or just maintain the country's current regulation with a ratchet that locks in further liberalisation.

2. A lot of countries favour a rhetorical recognition that each can have its own regulatory requirements on the transfer of data by electronic means.[20] What is not spelt out is that those requirements would still be subject to the annex. The US did not commit even to include this.

3. Switzerland wanted a positive assertion that a country has the right to apply its own regulatory requirements concerning information transfer. It may be concerned to protect citizens' rights, but it would also want to protect the strict privacy rights of rich clients of Switzerland's legal and banking industry.

4. Hong Kong, Mauritius and Iceland had an intermediate position that would make the obligation subject to domestic laws; but those laws could not involve arbitrary or unjustified discrimination or disguised barriers to e-commerce, which would create serious uncertainty for regulators.

5. A number of countries propose a defence that would allow a government to keep or adopt a measure that restricts the movement of information to achieve a 'legitimate public policy objective', so long as it was not applied in a way that amounts to 'arbitrary or unjustified discrimination' or a backdoor way of restricting 'trade' as broadly defined in TiSA.[21] Because this is a defence, it would have to be argued during a dispute and accepted by the adjudicating panel of trade experts. Again, that could create uncertainty and potentially have a chilling effect on policy makers and regulators.

17 US, Non-Paper, TiSA Landing Zone, Article 2: Movement of Information, undated (November 2016)

18 Australia, Canada, Chile, South Korea and New Zealand

19 TiSA, Article 1.4, Annex on Electronic Commerce, undated (November 2016)

20 TiSA, Article 2.1, Annex on Electronic Commerce, undated (November 2016). Supporters are Australia, Canada, Chile, Colombia, Costa Rica, Iceland, Japan, Mauritius, Mexico, New Zealand, Pakistan, Panama, Peru, South Korea, Taiwan.

21 TiSA, Article 2.3, Annex on Electronic Commerce, undated. Supported by Australia, Canada, Chile, Colombia, Japan, Mauritius, Mexico, New Zealand, Panama, Taiwan.

This proposal is a variation on the general exception in the core TiSA text, which applies similar wording to public morals, public order, health and the environment, but is further limited by a 'necessity' test that means a government must adopt the approach that can achieve its policy goal while imposing the least burden on commercial interests.[22] The inclusion of this option in the e-commerce annex suggests the TiSA parties don't think their policy objectives relating to data would fall within those categories and/or that the protection in the general exception is too weak. The consumer protection and privacy part of the general exception is even weaker, as discussed below.

The US has not supported this defence. It is considering a narrower exception that would allow conditions on transfers of *personal* (not commercial) information, if the measure was *necessary* (the least burdensome option) to protect *personal privacy* only *and* is not applied in a way that amounts to arbitrary or unjustified discrimination or a backdoor way of restricting 'trade'.[23]

Location of computer facilities (Article 8)

Team TiSA argues that the benefits to companies of free movement of data are undercut if a country can insist that service suppliers use or locate computer facilities within its territory, another example of what it labels 'forced localisation'. Hence, the annex would prevent a government from requiring the use or location of computing facilities inside the country as a condition of supplying a service in that country. 'Computing facilities' is defined as 'computer servers and storage devices for the processing or storage of information for commercial use'.[24]

Fewer protections are being proposed than for the data localisation rule, but they are similar. The same group proposes a rhetorical recognition that each may have its own regulatory requirements on the use of computing facilities, including requirements that 'seek to' ensure the security and confidentiality of communications.[25] Again, those requirements would be subject to the TiSA rules, including this annex. A number of countries also want a similar defence for 'legitimate public policy objectives' provided the requirement does not amount to arbitrary or unjustifiable discrimination or a disguised restriction on trade.[26] The wording is very like the TPP, although that imposed an additional restriction that the restrictions were no greater than needed to achieve the public policy objective (a necessity test).[27] Neither the US nor the EU has stated a position on this protection.

Colombia and Mauritius have proposed that a country could still make a subsidy or other advantage conditional on the use, expansion or establishment of computing facilities inside the country.[28] The Small Group Non Paper notes the inconsistency of this article with the flexibility on 'performance requirements' in the 'localisation' text;[29] it is unclear which text would prevail so the group suggests consulting on the matter.

Keeping source codes secret (Article 6)

A source code is the formula for a computer programme that humans can read, which is then converted into an object code or machine code that can be read by the computer. Open source means it is accessible to everyone to use, copy, check, alter or correct. The scope of the TiSA rule proposed by the US, Canada, Switzerland and several others is very broad: no TiSA government can require a person (firm or individual) of another TiSA country that owns software to transfer or provide access to source code for that software '*in connection with* the supply of a service'.[30] The non-paper suggests 'as a condition for the supply of a service' as an alternative. Although it is not stated, the ban presumably includes requirements to transfer source code to another TiSA government.

22 TiSA, Article 1.9, Core text, dated 14 July 2016.

23 TiSA, Article 2.3*alt,* Annex on Electronic Commerce, undated (November 2016)

24 TiSA, Article 14, Annex on Electronic Commerce, undated (November 2016)

25 TiSA, Article 8.1, Annex on Electronic Commerce, undated (November 2016)

26 TiSA, Article 8.4, Annex on Electronic Commerce, undated (November 2016)

27 TPP, Article 14.13.3(b), Annex on Electronic Commerce (November 2016)

28 TiSA, Article 8.3, Annex on Electronic Commerce, undated (November 2016)

29 Article X.3.4 Performance Requirements of the TiSA Localisation text, dated November 2016, allows countries to condition such benefits on locating production or supply services inside the country.

30 TiSA, Article 6.1, Annex on Electronic Commerce, undated (November 2016)

Keeping source codes secret gives monopoly rights to the creator. The argument that this is not a problem because other digital products and individual apps compete for customers ignores the reality that the digital domain is not a level playing field. Secrecy of source codes perpetuates the power of the handful of corporations that control the major search engines and digital platforms, and of mega-corporations with massive research budgets that dominate the tech sector and smart products. Various kinds of risks could go unchecked and unchallenged:[31]

Corporate non-compliance: Computer programmes are now embedded in smart products, from household appliances to motor vehicles to smart phones. Non-disclosure makes it impossible to monitor compliance with product standards. The scandal over Volkswagen's fraudulent emissions software for monitoring emissions shows the importance of disclosure for consumer protection, enforcing environmental standards, and prosecuting criminal acts.[32]

Security and safety: Software operates artificial intelligence, such as robots, drones, and driverless vehicles. Aside from risks of error and design faults, there are serious concerns about potential for hacking and installing malware, including by routing attacks indirectly through less secure software.

Personal information: Algorithms are used for:

- profiling that can lead to bans from activities (such as no-fly lists), differential charges for services (so-called dynamic pricing), selective exposure to information;
- employment decisions, performance monitoring, and assessing and rating applicants and employees; and
- risk assessments for credit ratings or health insurance, based on assumptions about gender, race, income and other factors.

Economic development: Manufacturers of generic components and servicers of smart products are unable to provide local inputs, and technology transfer to developing countries is meaningless without the source code.

Financial risk and fraud: Complex algorithms are used to engineer financial products, calculate the LIBOR[33], conduct automated trading in currency, shares and derivatives, allocate ratings to financial products, assess risk for insurance, and many other activities that have been associated with fraud, and financial instability and crises. (It is not yet decided whether the e-commerce annex will apply to financial services.)

Several countries – but not the US or EU- propose a 'legitimate public policy' defence similar to that for localisation of data and computer facilities. The public policy objective for requiring the transfer of or access to source code must be 'legitimate', the measure must not involve 'arbitrary' or 'unjustified discrimination' against the owner of source code, and the requirement must not be a disguised restriction on trade. A requirement to disclose a source code could be challenged on any of those grounds. The November 2016 text explicitly questions whether the (limited) general exception in the Core text would apply here and, if it does not, why the Article 6 protection is needed – in other words, ***why any exception is needed***.

The US and Australia would ensure that terms and conditions on providing source code could still be written into commercial contracts. A party could also require the source code software to be modified where *necessary* for the software to comply with laws or regulations, ***provided those laws and regulations are already permitted under TiSA*** (eg. not discriminatory). Again, 'necessary' means the government must choose the least restrictive option to achieve compliance with those laws.

31 Based on research by Sanya Reid Smith, Third World Network, Malaysia, 2017

32 Russell Hotten, 'Volkswagen: the scandal explained', 10 December 2015, http://www.bbc.com/news/business-34324772

33 The London Interbank Offer Rate that provides the benchmark for interest rates from the City of London, which was subject to fraudulent manipulation by bankers from 2012-2014. 'Libor Scandal: the bankers who fixed the world's most important number', *The Guardian,* 18 January 2017, https://www.theguardian.com/business/2017/jan/18/libor-scandal-the-bankers-who-fixed-the-worlds-most-important-number

No local content requirements (Article 10)

The US wants to prohibit a TiSA country from giving preferential treatment to local electronic content on the grounds that it was created, produced, published, contracted for, commissioned or first made available on commercial terms locally, or where the creator, producer, developer or owner is local.[34] This restriction would not apply to subsidies or grants, government-supported loans, guarantees and insurance.[35]

While the US proposal could apply to many services, it is most sensitive for the culture sector. For example, the EU proposed a requirement in 2016 that video-on-demand providers, such as Netflix, Amazon.com and Apple's iTunes, would have to dedicate at least one-fifth of their catalogues to European content.[36]

Although the US is not a party to the UNESCO Convention on Cultural Diversity, many TiSA countries are.[37] Principle 2 of the Convention adopts the

> *principle of sovereignty: States have, in accordance with the Charter of the United Nations and the principles of international law, the sovereign right to adopt measures and policies to protect and promote the diversity of cultural expressions within their territory.*[38]

Article 20 of the Convention requires the parties to foster mutual supportiveness with the other treaties to which they are parties. The US proposal does the opposite. This is not the only place where cultural content is under attack in TiSA; making commitments on market access, adopting a standstill on discriminatory measures, and applying domestic regulation disciplines could have a similar effect. TiSA is silent on cultural rights, even in the flawed general exception.

This is a familiar battle-ground in the GATS. The US, on behalf of Hollywood, has a long-standing opposition to local content quotas or other preferences for the cultural sector. The EU is committed internally to maintain a 'cultural exception' in trade agreements. That is basically limited to audio-visual services, but is enough to create a major conflict with the US.[39] The US says the e-commerce provision is without prejudice to whether electronic transmissions are treated as goods or services,[40] but its approach would make that distinction redundant for local content.

No ISP liability for uploaded content (Article 11)

The Internet industry wants to maximise its freedom while avoiding any liability. The US wants to help it by including rules that protect providers and users of 'interactive computer services', described as 'a system or service that provides or enables electronic access by multiple users to a computer server'.[41] Australia, Canada, Colombia and South Korea oppose the entire provision and the EU opposes all the substantive parts of it.

The US proposal says: where *information* provided through a platform (like Google or Facebook) has been created or developed by another person or entity, and there is potential liability for the harm that *information* has caused (such as breach of libel, privacy or hate laws that are not criminal laws[42]), a TiSA government must not treat *the supplier* or *the user* of the computer service as a supplier of the information content, unless they were actively involved in creating the information.[43]

Predictably for a US proposal, this protection from liability would not apply to measures relating to intellectual property (IP), including infringements of IP. Nor would it prevent enforcement of the

34 TiSA, Article 10.3, Annex on Electronic Commerce, undated (November 2016)

35 TiSA, Article 10.5, Annex on Electronic Commerce, undated (November 2016)

36 http://www.bloomberg.com/news/articles/2016-05-25/netflix-amazon-face-minimum-eu-quota-for-european-films-shows

37 Australia, Belgium, Canada, Chile, Colombia, Costa Rica, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Mexico, Netherlands, New Zealand, Panama, Peru, Portugal, South Korea, Slovakia, Slovenia, Spain, Sweden, Switzerland, UK and EU

38 http://en.unesco.org/creativity/sites/creativity/files/passeport-convention2005-web2.pdf

39 This argument underpins their dispute on whether digitised products are a good (the GATT has an exception for audio-visual content) or a service (the GATS has no such exception) - a question that is explicitly left open in footnote 7 to Article 10: Customs Duties, Annex on Electronic Commerce, undated (November 2016)

40 TiSA, Article 11, Annex on Electronic Commerce, undated (November 2016)

41 TiSA, Article 14, Annex on Electronic Commerce, undated (November 2016)

42 TiSA, Article 11.(c)(i), Annex on Electronic Commerce, undated (November 2016)

43 TiSA, Article 11.2, Annex on Electronic Commerce, undated (November 2016)

criminal law, or requirements that an ISP complies with an order of a law enforcement authority that is 'not inconsistent with the provisions of this article'. In other words, the US proposes that ***this obligation could overrule a lawful order of a law enforcement authority where it would conflict with a provision of TiSA!***

Internet self-governance

Champions of global e-commerce promise a future of inclusion and empowerment. Appeals to 'Internet freedom', 'unfettered information highways' and 'open access' convey the impression of a neutral force. But the technology is controlled by commercial interests who have accumulated enormous power. Very few rules currently govern the Internet, and they are made in forums which the tech giants like Google, Apple, Amazon, and Facebook dominate. Even civil society voices tend to split on the basis of who is funded by Google.

As discussed below, the provision to enable choice of networks and apps is subject to 'reasonable network management',[44] which is undefined in the text. In a global system of Internet self-governance, those who run the networks will decide what is reasonable network management. The European Consumer Organisation (BEUC) observes that a secretive and non-participatory trade agreement is not the place to determine Internet governance.[45]

Sham consumer and citizen protections

The first article of the e-commerce annex recognises that e-commerce provides 'opportunities for inclusive economic growth' and the 'importance of avoiding *unnecessary barriers'* to the use and development of e-commerce.[46] Again, 'necessary' means that rules which could negatively affect the big tech companies and the network or gig economy must be the least restrictive or burdensome of the available options that can achieve the policy goal.

Article 1.2 also talks of the need to promote 'consumer confidence' in e-commerce. But the proposals for consumer and privacy protections, and for Internet freedom, which might build that confidence are weak and contested. The US is even resisting the most ineffective powers to regulate the e-commerce industry to protect people's rights. Moreover, there are no development flexibilities or obligations to close the digital divide. Instead, the annex empowers those states and corporations that already dominate the digital domain.

Consumer protection (Article 3)

It has been agreed that TiSA parties must have consumer protection laws, but ***there are no minimum standards for those laws***. They could be absolutely minimal. The scope of the required laws is also restricted to those that 'proscribe fraudulent and deceptive commercial practices that cause harm or potential harm to consumers engaged in online commercial activities'. Other anti-consumer practices such as re-routing, geo-blocking and price discrimination are not mentioned. For cross-border e-commerce transactions, consumers have no clarity on whose law applies or guaranteed access to dispute mechanisms and enforcement of remedies. They may not even know where the provider is located or where the relevant data they would need to access is held.

Privacy protection (Article 4)

The article on privacy is entitled 'Personal Information Protection'. Personal information is defined as information, including data, relating to an identified or identifiable natural person – Switzerland wants to include legal persons (such as companies).[47] None of the article is agreed.

Positions span a broad spectrum. On one hand, the US and Hong Kong are still considering whether they will even support a statement that recognises the economic and social benefits of protecting

44 TiSA, Article 7(a), Annex on Electronic Commerce, undated (November 2016)

45 BEUC, 'Analysis of the TiSA E-Commerce Annex and Recommendations to the Negotiators', September 2016

46 TiSA, Article 1.2, Annex on Electronic Commerce, undated (November 2016)

47 TiSA, Article 14, Annex on Electronic Commerce, undated (November 2016)

personal information of users of electronic commerce – wording the US agreed to in the TPP[48]. The US also wants parties to *endeavour* to provide flexibility for firms engaged in transactions between countries with different privacy regimes. This would allow them to protect personal information in ways that are 'substantially similar' to the requirements of parties' laws, effectively re-writing a sovereign country's laws.[49] It could be costly and burdensome for a country to challenge the company's interpretation of its privacy law and the equivalence of another.

By contrast, Switzerland wants a total carve out from the annex for all national laws and policies that aim to protect intellectual property, privacy, confidentiality of personal and confidential information, consumer protection, and protection of cultural diversity.[50] In the November 2016 text only Pakistan was considering whether to support Switzerland. Sixteen negotiating parties opposed the carveout: Australia, Canada, Chile, Taiwan, Colombia, the EU, Iceland, Japan, South Korea, Mauritius, Mexico, New Zealand, Norway, Peru, Turkey and the US. Switzerland also wants to reserve its right to take 'all measures necessary' to protect the data of natural and legal persons – clearly, on behalf of its banking system – and for countries to enhance their enforcement capacity to ensure their privacy and data protection laws are complied with.[51]

The wording supported by most countries is exceptionally weak: governments are required to have a domestic legal framework to provide protection for personal information, which *should* (but does not have to) *take into account* (rather than apply) principles and guidelines of relevant international bodies (which may be less ambitious than countries' domestic laws).[52] The relevant international bodies are not necessarily inter-governmental. They might be principles developed by TiSA parties in the OECD or Asia Pacific Economic Cooperation (APEC) forum, or rules agreed by stakeholders in the private forums that the Internet industry dominates. The US seeks to weaken this provision further by a footnote that says it would be enough to have a law to enforce voluntary undertakings by companies relating to privacy.[53] A number of countries propose that governments *shall endeavour* to ensure their domestic framework is *applied* in a non-discriminatory way.[54]

The European Union has been unable so far to develop an internally agreed position on privacy, which is a constitutional right. The European Commission has apparently drafted a compromise that it believes satisfies the EU Charter of Fundamental Rights and the EU General Data Protection Regulation. However, political sensitivity means a decision is unlikely until after the German elections in September 2017. European consumer organisation BEUC has made it clear that TiSA is not the place to decide countries' data protection and privacy rules.[55]

Because there is no mandatory standard, a country's domestic law could therefore fall below the weakest international standards. Where a country is more ambitious, it could be challenged for going beyond what is *necessary* to achieve the policy objective under the general exception.

The flawed general exception

In the absence of specific protections for privacy and consumers in the annex, governments would have to rely on the general exception that was imported from the GATS[56] into the TiSA core text.[57] That exception is especially problematic for consumer protection and privacy for several reasons:

- It is not a carve out or exclusion that protects privacy or consumer protection measures from the rules, but a defence that the government must establish during a dispute to the satisfaction of a panel of trade law authorities;

48 TPP, Article 14.8.1.

49 TiSA, Article 4.3, Annex on Electronic Commerce, undated (November 2016)

50 TiSA, Article 1.5bis, Annex on Electronic Commerce, undated (November 2016)

51 TiSA, Footnote 2 to Article 4.1, Annex on Electronic Commerce, undated (November 2016)

52 TiSA, Article 4.2, Annex on Electronic Commerce, undated (November 2016)

53 TiSA, Footnote 3 to Article 4.2, Annex on Electronic Commerce, undated (November 2016)

54 Article 4.4, proposed by Canada, Chile, Colombia, Mauritius, Pakistan; Taiwan, Colombia, South Korea, Mexico considering

55 BEUC, 'Analysis of the TiSA E-Commerce Annex and Recommendations to the Negotiators', September 2016

56 GATS 1994, Article XIV.

57 TiSA, Article I-9, Core text, dated 14 July 2016

- It does not actually refer to consumer protection, but only to the prevention of deceptive or fraudulent practices or to deal with the effects of a default on a services contract (which carries a further burden of proof);
- The privacy protection relates only to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts, not to improper use by those who collect the data.
- Rather than giving governments relief, the exception imposes an *additional* restraint on what governments are otherwise allowed to do under TiSA to protect consumer protection and privacy. The consumer or privacy measure must be
    - adopted to secure compliance with a law or regulation that is consistent with TiSA, which means the law could not require data localisation or the location or use of computers within the country, or treat foreign providers differently from nationals; plus
    - *necessary* to achieve that compliance, meaning it is the least burdensome option reasonably available to ensure compliance with the law or regulation.

    By making those laws subject to a necessity test, the 'exception' actually restricts what TiSA would allow governments to do.
- Because the exception makes explicit reference to consumer protection and privacy, it would be hard to invoke the public order or public morals categories in the general exception to provide protection.

Spam (Article 5)

An 'unsolicited commercial electronic message' (spam) is defined as one sent without consent of the recipient or against their explicit wishes.[58] The main proposal says TiSA parties must have measures that require suppliers of spam to either *facilitate* opting out of receiving unsolicited messages or *require consent* as set out in a country's laws. Government have to provide some kind of legal recourse, presumably to the recipient, when the supplier does not comply, but it does not require that the recourse is effective. The US and Latin American countries want a third option, whereby a government measure merely 'provides for the minimisation' of spam. Canada has suggested an alternative approach that requires states to adopt a *legal framework* for regulation of spam that requires either opting in by recipients or facilitates their ability to opt out.

The US has also proposed an exclusion for messages between parties to an existing transaction (for example, until an e-purchase with Amazon is completed) or between parties with an existing relationship, which could cover any website or ISP provider with whom someone has registered, such as Netflix, Agoda or Google. That would render the spam protection useless for a large amount of traffic. The EU is considering the US proposal.

Conditional network access, use of Internet and open networks (Article 7)

As noted above, Internet freedom is a loaded term, especially in agreements like TiSA that are designed to advance the commercial interests of powerful countries and tech corporations. At first glance, Article 7 appears to recognise that end-users should be able to choose which services, apps and devices they want to connect to. However, there is no obligation in relation to open networks and network access, just a statement that the parties recognise the benefits of consumers being able to have access to and use services and apps of their choice on the Internet. There are several illusions in the article's wording:

- it recognises the benefits of freedom of choice, but imposes no obligations to guarantee it;
- it refers to choice of services and apps, but not to choice of networks or platforms;
- freedom to choose services and apps is still subject to the applicable laws and regulations of the TiSA country; and

58 TiSA, Article 5 and Article 14, Annex on Electronic Commerce, undated (November 2016)

- choice of services and apps is subject to 'reasonable network management', but in a global system of internet self-governance, those who run the networks will determine what is reasonable network management.

The article also recognises the benefits of consumers having access their ISP's network management practices. But again, there is no obligation.

National Security (Article 13)

Several countries, including the US and Australia,[59] have proposed a security exception specific to this annex that gives even stronger rights to governments than the security exception in the TiSA core text.[60] A government could define what are its 'essential security interests' and what action it considers is necessary to protect them. Japan wants more clarity on what 'essential security interests' means. There is nothing that would require a state to disclose to the other TiSA countries, let alone to users or ISPs, when it was breaching any rule in the annex (including the weak consumer and privacy provisions). Past practice shows the US would interpret this wording to prevent a dispute body from reviewing a party's actions altogether. The International Digital Economic Alliance, an industry think tank, observed that this kind of overreach generates distrust and unwillingness to locate data in countries that are likely to invoke this kind of exception.[61] However, many Internet users would not know where the server hosting their data was based.

Facilitating cross-border electronic transactions

Only three provisions are really directed towards facilitating commercial transactions conducted through digital trade.

Electronic authentication and e-signatures (Article 9)

The expansion of cross-border trade requires changes to rules and practices that assume the physical presence of the participants. One of the few agreed provisions in the annex says that a signature cannot be rejected just because it is in electronic form, but would allow governments to say the contrary in their domestic law. They have also agreed not to adopt any measures for authentication[62] that would prohibit the parties to an e-transaction from deciding the appropriate methods for authentication, or from being able to establish before a judicial tribunal that they have complied with any legal requirements on authentication. It is still possible for a country to make the electronic authentication of a specific category of transactions meet certain performance standards or be certified by an authority accredited under its domestic law.

The term 'electronic signature' is only used in the heading of the provision, which avoids the thorny question of its scope and the distinction between electronic and digital signatures.[63]

No customs duties (Article 10)

WTO members have maintained a temporary moratorium on customs duties for electronic transmissions that has been rolled over at successive ministerial meetings.[64] This annex would make that permanent. 'Electronic transmissions' is not defined. Where the term is used in the WTO it does not extend to physical products bought through offshore electronic transactions.

The US wants to extend this provision to make electronically transmitted *content* duty free, or at least to make it explicit that the rule covers content transmitted electronically. That would exempt from customs duties a wide range of digitised products, such as e-books, music, movies, and other

59 Australia, Mauritius, Pakistan and US

60 TiSA, Article I-10, Core text, 14 July 2016.

61 International Digital Economy Alliance, 'The Trillion Dollar Question: How trade agreements can maximize the economic potential of data in the networked economy and support the Internet as the world's trading platform', 2013, p.6

62 Electronic authentication is defined in Article 14 as the process or act of verifying the identity of a party to an electronic communication or transaction or ensuring the integrity of an electronic communication.

63 'The difference between digital signatures and electronic signatures', 1 June 2016, https://www.globalsign.com/en/blog/electronic-signatures-vs-digital-signatures/

64 https://www.wto.org/english/thewto_e/minist_e/mc10_e/briefing_notes_e/brief_ecommerce_e.htm

commercial content transmitted electronically, such as architectural or engineering drawings, IT programmes, back office transcriptions, etc. Technological innovations would introduce new uncertainties: for example, would electronic transmission cover an instruction conveyed to a 3-D printer across the border by the Internet?

A government could still impose an internal tax, such as a consumption tax, provided it is consistent with the rest of the agreement, for example that it does not impose a higher rate on cross-border transactions.[65] Other leaked TiSA texts say that tax matters have not yet been resolved in TiSA. A proposed footnote says this provision is without prejudice to whether electronic transmissions are a good or a service, which could prove important for tax purposes.[66] However, market power may prove a bigger obstacle to tax. The major electronic marketplaces are threatening to geo-block Australian users from buying goods from overseas if the federal government proceeds with plans to impose the goods and services tax on transactions conducted through their platforms and make them collect it.[67]

The fiscal consequences of this provision could be significant if cross-border transactions displace local services that benefit the economy through employment, payment of business taxes and secondary economic benefits. Global e-commerce firms are notorious for transfer pricing and tax avoidance. Governments give away the right to restrict international transfers and payments for current transactions[68] and movements of capital where they have taken market access commitments on cross-border supply of the service.[69] An outflow of foreign exchange could also cause balance of payments issues; yet the core text provides very limited room for interventions even in an emergency.[70]

International cooperation (Article 12)

The annex contains a weak commitment for the TiSA parties to exchange information and share experiences. The cooperation provision merely 'recognise(s) the importance' of various activities: exchanges of information and experiences on technology and research, commercial practices and applicable laws, regulations, policies and standards. Some countries would extend this to online consumer protection and spam,[71] and consumer access to online products and services.[72]

There is a nod to the digital divide, possibly motivated by the goal of inserting TiSA back into the WTO. The parties appear to have largely agreed to cooperate to reduce disparities in access to and use of ICT and enhance national regulatory capacity,[73] and recognise the importance of positively assisting access for SMEs and participation in e-commerce. But these are unenforceable promises. A large number of countries want to preface this with a specific purpose: 'with a view to promoting the development of innovative and sustainable electronic commerce'.

Less benign proposals from the US, Switzerland and others[74] would encourage the private sector to adopt methods of self-regulation that foster e-commerce.[75] That foreshadows likely arguments from the US and from the tech industry that self-regulation is an appropriate form of regulation, and should be preferred when the right to regulate e-commerce is subject to a 'necessity' or least-trade restrictive test.

The US and a different group of countries[76] propose 'recognising the importance' of TiSA parties 'actively participating in regional and multilateral fora', presumably to push a TiSA-style text. The November 2016 draft deleted an explicit reference to the WTO as one such forum.[77] The proposal

65 TiSA, Article 10.2 and Article 14, Annex on Electronic Commerce, undated (November 2016). It also excludes antidumping or countervailing duties or fees charged commensurate with a service provided.

66 TiSA, footnote 7 to Article 10, Annex on Electronic Commerce, undated (November 2016)

67 'Amazon, Alibaba, eBay and Etsy may block Australian users if GST changes go ahead', *NZ Herald,* 22 April 2017, http://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=11843234

68 TiSA, Article I-7, Core text, dated 14 July 2016.

69 TiSA, Footnote 2 to Article I-3, Core text, dated 14 July 2016.

70 TiSA, Article I-8, Core text, dated 14 July 2016.

71 Australia, Colombia, Costa Rica, Turkey and the US; Chile, Taiwan, EU, Korea, Lichtenstein, Mexico and New Zealand 'considering'

72 Australia's proposal; Chile, Taiwan, Costa Rica, EU. South Korea, Lichtenstein, New Zealand, Turkey 'considering'

73 TiSA, Article 12(e), Annex on Electronic Commerce, undated (November 2016)

74 Proposed by US, Switzerland, Mauritius with Canada, Chile, Colombia and South Korea 'considering'

75 TiSA, Article 12(c), Annex on Electronic Commerce, undated (November 2016)

76 Canada, Costa Rica, South Korea, US, NZ 'considering'

77 TiSA, Article 12(d), Annex on Electronic Commerce, undated (November 2016)

to include the WTO was clearly linked to the push by many TiSA countries to secure a mandate to negotiate e-commerce at the WTO ministerial meeting in Argentina in December 2017.[78] It may have been removed to avoid inflaming concerns from non-TiSA developing countries who oppose such negotiations in the WTO.

78 https://www.wto.org/english/news_e/news17_e/serv_14mar17_e.htm