TWN
Third World Network
Website: www.twn.my

Briefing for 13th WTO Ministerial Conference

Abu Dhabi, 26-29 February 2024

Analysis of e-commerce JSI chairs' text of 20 February 2024, INF/ECOM/85 Rev.1

Jane Kelsey

23 February 2024

Days out from the World Trade Organization (WTO) 13th Ministerial Conference, the co-convenors from Australia, Japan and Singapore have issued a chairs' text (INF/ECOM/85 Rev.1) for their unmandated Joint Statement Initiative (JSI) on electronic commerce. This updates their text of 15 January 2024 by proposing outcomes for several outstanding issues. The text is presented as a first tranche that centres on the more transactional provisions of a proposed plurilateral e-commerce agreement, plus making the moratorium on customs duties on electronic transmissions permanent. It is not an agreed text and some participating governments are likely to be unhappy with the chairs' proposed compromises.

The February and January 2024 texts draw on a broader consolidated text of 15 November 2023 (INF/ECOM/62/Rev.5), which was produced after the US notified the withdrawal of its support for several core provisions relating to data and software. The cover note to the latest text reiterates, in bold, that these remaining provisions have not been dropped and the Rev.5 text remains "a comprehensive record of proposals, attributions and drafting notes". The new text needs to be analysed with that in mind. In particular, the inclusion of broad data-related exceptions in this latest text indicates that some countries, at least, still plan to pursue a comprehensive agreement and believe it would be difficult to add new exceptions in that future text so have inserted them here. If so, the limited development flexibilities in this text and the lack of special and differential treatment must ring alarm bells for developing countries.

Beyond issues with the text itself, the fundamental illegitimacy of these unmandated JSIs and how their proponents intend to secure their adoption needs to be addressed. In this case, the JSI runs in parallel to the WTO's mandated Work Programme on Electronic Commerce.

Published by Third World Network Berhad (198701004592 (163262-P))
Address: 131 Jalan Macalister, 10400 Penang, MALAYSIA **Tel**: 60-4-2266728/2266159 **Fax**: 60-4-2264505
Email: twn@twnetwork.org **Website**: www.twn.my

Content (new or amended provisions in this text are underlined)

38. Secretariat
39. Deposit
40. Registration

Scope of the agreement

The scope of the rules, commitments and obligations is extremely broad. The rules apply to "***measures***" adopted or maintained by a Party "***affecting***" ***trade by electronic means***, whether or not the measures were directed at the digital sphere.

"Trade by electronic means" is not defined, and potentially involves any digital activity that involves a foreign supplier, including advertising, search engines and social media.

"Measures" to which the provisions apply has an extensive and open-ended definition that includes decisions and administrative actions and "any other form".

Many provisions require parties to "***endeavour***" to achieve certain actions or outcomes. This is still an obligation that requires evidence of positive action.

Parties cannot enter ***reservations*** without the consent of all the other Parties. So developing countries must rely on flexibilities in the language and any carveouts or exceptions.

There are limited exclusions for ***government procurement*** (covering the *process* of procuring goods or services for purely internal use) and services supplied in the exercise of ***governmental authority*** (limited, in effect, to non-commercial monopolies).

The exceptions are critically important

The very limited exceptions proposed by the chairs are deeply problematic, given the policy context and geopolitics of these negotiations, including the US' withdrawal of support for binding rules on data flows and software. These exceptions are likely to be carried over into any more comprehensive agreement. The inclusion of privacy protections for data transfers, even though the text has limited data rules, suggests some parties expect it will be difficult to add new exceptions in any future text.

The ***general exceptions*** are imported from the General Agreement on Tariffs and Trade (GATT) and General Agreement on Trade in Services (GATS). These exceptions have almost always failed when invoked in a dispute.

The exception for ***prudential measures*** retains the circular requirement that measures are not used as a means of avoiding obligations in the agreement.

There is no exception for ***taxation measures***.

The ***security exception*** imports the limited and largely irrelevant GATT and GATS security articles that apply to fissionable material, provisioning of the military, war and an emergency in international relations, and UN obligations on peace and security. This choice of wording will continue the controversy and uncertainty over the provisions, given the US' insistence that actions taken under these exceptions are totally self-judging and not justiciable in the WTO. The chairs rejected proposals in Rev.5 for an explicitly self-judging, unlimited security exception that would not "prevent any party from taking any action which it considers necessary for the protection of its essential security interest".

A provision on ***non-application between particular Parties*** would allow one Party to cherry-pick which other Parties the agreement applies to. That appears to be geopolitical, given that China and Anglo-American countries are both Parties. It would be very difficult for most developing countries to use in practice, in contrast to a broader self-judging national security exception.

There are no ***development*** exceptions. In Rev.5 Nigeria proposed a carveout relating to the data rules, a variation on which would be as relevant for this text as the new data privacy exception is. Cote d'Ivoire proposed that developing countries would not be required to implement the agreement until they have acquired the capacity to do so, and least developed countries (LDCs) must only implement the rules to the extent consistent with their needs and capabilities. The chairs have rejected both.

New Zealand's partly self-judging carveout for measures relating to the rights of ***Indigenous Peoples*** has been substantially narrowed in ways that would make it very difficult to apply.

Data privacy provisions

The new text has two provisions on ***privacy of data***. Even though the main data transfer and location provisions have been omitted from this text, data remains at the core of everything digital. Data privacy provisions would have some relevance to this "first tranche" text, for example rules on "enabling" e-commerce, open government data, access to and use of the Internet, and spam, among others. As noted, the inclusion of two expansive data privacy rules in this text also anticipates a broader agreement and that it would be difficult to reopen these exceptions in future negotiations.

The overriding privacy provision in Section A was not in any previous text. The ***Personal Data Protection exception*** originates from the EU-Japan protocol on data flows. The EU previously provided Parties with the right to maintain personal data transfer rules that the Party "deems appropriate". That could limit challenges to measures that interfere with trade but which a Party declares are to advance data protection. The protocol introduced a specific condition that a Party's laws must include mechanisms facilitating data transfers under conditions of general application. Only a few countries will currently have privacy laws with mechanisms that enable such transfers.

The second, more flexible, provision is an obligation to adopt a ***legal framework for the protection of personal data*** of those who use e-commerce. There is no minimum threshold. The obligation only applies to identified or identifiable persons, and it is unclear whether that includes de-anonymised data. Governments must "endeavour" to ensure the legal framework is non-discriminatory (across countries). The footnote, drawn from the US-driven Trans-Pacific Partnership (TPP), allows compliance through sector-specific laws or "other laws that address privacy violations". Compliance with even this low threshold may be challenging for some developing countries.

No special and differential treatment

Following the pattern of other JSIs, there is no special and differential treatment, just longer periods for developing countries and LDCs to comply with obligations that most developed country Parties already satisfy. This time-limited flexibility only applies where obligations "require public policy, institutional or legislative changes" or increased technical capacity, for implementation. There is also a seven-year peace clause on bringing disputes, but only for LDCs.

The phase-in process is much more limited than in the Trade Facilitation Agreement or even the JSI on investment facilitation. At the time the agreement enters into force, a developing country or LDC must designate any provision it considers would require up to five years to implement. It must submit this at the time of entry into force. The five years might be extended for another two years, with advance notice, and on detailing the reasons and actions required to complete implementation. Donors are "encouraged" to provide support for developing countries and LDCs to conduct or update needs assessments to identify gaps in their capacity to implement, and those assessments should inform designations at the time of

entry into force. So needs assessments would have to be conducted before the agreement enters into force, not before ratification by the developing country or LDC.

There is no guarantee of resourcing. A developing country or LDC could designate any provision regarding which they would benefit most from capacity building and technical assistance (it is unclear if this means only one). Developing countries agree to "facilitate" such assistance and support on mutually agreed terms and taking account of countries' specific priorities. There is a list of principles for providing such "assistance and support" for capacity building, which include regional options, role of private sector, and non-duplication of support. The only obligation on developed countries (and developing countries declaring themselves in a position to provide support) is to provide information on new and existing capacity-building programmes. There would be close monitoring of developing countries' compliance at least annually.

Threats to policy space

The Rev.5 text had three options on the ***moratorium on customs duties on e-transmissions***: a permanent ban, including fees and other charges; continuing current practice, with e-transmissions interpreted to exclude content; and maintaining WTO practice, allowing for future changes. This chairs' text would make the moratorium permanent. Governments could still apply internal taxes, fees and charges provided they are consistent with WTO rules.

The text has a broad carveout for information collected by or for the government. However, that does not apply to the ***open government data*** provision, which restricts how governments can regulate the use of central government data whose dislosure is not limited under domestic law, and which they have put online for public access and use. This would include, for example, census data, climate risk or hazards data, and Indigenous Peoples data published without their consent. The aim is to allow users to search, retrieve, analyse and manipulate the data for commercial and non-commercial purposes (why in an e-commerce agreement?). This would prevent governments from imposing restrictions on data when they publish it, unless they do so formally through domestic law.

Governments must endeavour, as far as practicable, to make sure the data is machine-readable, searchable, retrievable, up to date, and accompanied by meta data that is based on commonly used formats so the user can understand and use the data, and do so for no or a reasonable cost. Governments must also endeavour to avoid imposing conditions that "unduly prevent or restrict the user of such data" from using it in various ways, including "regrouping" it (presumably by algorithms) and using it for commercial and non-commercial purposes without consent. The obligation applies to "measures" (which have an open-ended definition) "with respect to" such data, whose scope is broad and unclear.

The major beneficiaries of this will be big tech companies that use free public data to improve the capabilities of their artificial intelligence (AI) models. Making government data available openly, especially at no or reasonable cost as the text stipulates, means disadvantaging the public sector and smaller firms in favour of larger firms.

A Party must "endeavour to ***facilitate input by interested persons in the development of its legal framework*** for electronic transactions". The scope of "electronic transactions" is not defined. The legal framework is linked to the UNCITRAL (UN Commission on International Trade Law) Model Law on Electronic Commerce from 1996, but the article additionally refers to avoidance of "undue regulatory burden". As with "transparency" rules proposed or adopted in other agreements, this gives foreign corporate interests, including Big Tech, the opportunity to support or oppose an overall framework and specific digital regulation. Governments must also make public all "measures" (broadly defined) "affecting" (not just directed at) e-commerce on the date the measures come into force, at the latest, except in emergencies.

It is unclear how this agreement would ***interface with the GATS***, where commitments on cross-border services (mode 1) and the sectoral classifications CPC84 Computer and Related Services and CPC752 Telecommunications overlap with the JSI. The GATS positive-list approach allows WTO Members to limit their commitments on those modes and services sectors. This agreement would significantly expand those obligations without formally amending the GATS through the Marrakesh Agreement or schedules through the specified procedures.

The single ***telecommunications article is GATS-plus***. All Parties must adopt the GATS Reference Paper on Basic Telecommunications, which is currently voluntary to adopt in whole or part. Fewer than half the WTO Members have done so. The Reference Paper constrains how universal service obligations are structured and offered, and contains rules on ensuring competitors have access to "essential facilities" that are often run by public telcos. The main additional JSI rules require a telecom regulatory authority that is independent of a supplier of public telecom networks and services, with the power and ability to carry out its functions and to impose sanctions. Facilities considered "essential" must be made available by major suppliers (often state-owned enterprises (SOEs)) to other public telecom suppliers on "reasonable", non-discriminatory and public terms, and access to them supplied on an unbundled basis so they do not need to support the entire network. Developing countries' public telcos that provide unprofitable public services may struggle to survive.

Other obligations on Parties

Provisions on ***e-authentication, e-signatures and e-contracts*** are designed to enable digitalised transactions. Most provisions are hard obligations, not "endeavour". Governments retain some control "in circumstances otherwise provided under its laws or regulations", e.g., on specific uses of e-signatures in legal proceedings or the validity and enforceability of e-contracts. To take advantage of this, Parties need to have such laws in place; most developed countries do, but many developing countries would not. Allowing parties to a transaction to "mutually determine" the means for e-authentication would in practice allow Big Tech to dictate the means used for authenticating identity, given the power differential in its relationship with users.

The goal of ***paperless trading*** is to eliminate paper forms and documents for import, export and transit of goods. Customs authorities are required to provide border documents in digital form and governments must endeavour to have other government agencies do the same. Digital forms and supporting documentation must be accepted as equivalent to paper forms, unless overridden by domestic or international legal requirements, but a list of non-compliant documents would have to be provided within two years of the JSI entering into force. That obligation could also be overridden if it would reduce the effectiveness of customs or other trade procedures; however, the criteria for this are not specified and "effectiveness" would seem to be an objective factor that could be put to the test. These obligations assume a level of digitisation, capacity and compliance that is currently unrealistic for many developing countries.

Parties must "limit" unsolicited commercial messaging or ***spam***, such as targeted advertising, but one of the three options is minimal.

Parties must also adopt ***consumer protection*** measures that proscribe activities that cause harm to actual or potential consumers engaging in e-commerce. This applies only to misleading, fraudulent and deceptive commercial activities. There is no minimum level of protection required and its aims are basic (e.g., endeavour to ensure that suppliers deal fairly and honestly with consumers). Even achieving this, however, may be difficult for a number of developing countries.

When governments design responses to ***cybersecurity*** threats, they must "endeavour" to employ "risk-based" approaches and minimise "trade barriers" to tech providers. Risk-based assessment seems contradictory in an article that recognises cybersecurity threats are evolving – by definition, risks are not yet known or well understood, which would logically require a precautionary approach. Standards

are to be developed in an open, transparent, "consensus-based" manner, which reinforces the pressure to minimise constraints.

Finally, the latest text proposes a provision on the outstanding question of ***ICT products that contain cryptography***, used to prevent unauthorised access or use; a "key" unlocks that access. There are strong human rights reasons for protecting communications from monitoring and interference by governments and third parties, and public policy justifications for and against. This text does not address that balance; instead, it approaches cryptography from the position of the manufacturer and the government regulator.

The wording is similar, but not identical, to the cryptography Annex 8-B to the TPP/CPTPP chapter on Technical Barriers to Trade. A Party cannot require a legal person of another Party to transfer or provide access to proprietary information as a condition of manufacture, sale, distribution, import or use of such an ICT product, e.g., disclosing the key, even if they are in a joint venture or cooperating with a local counterpart. Nor can they be required to use a particular cryptographic algorithm.

There are several complex exceptions. A government or non-government body with power to investigate, inspect, examine or conduct a legal proceeding can require disclosure to ensure compliance with national laws, but only where that is consistent with WTO agreements, including on intellectual property rights. A competition authority can require disclosure to prevent or remedy an anti-competitive practice. There are broad exclusions for financial regulators, for ICT products for government use, and for access to networks, including devices that are owned or controlled by the government and used for government purposes.

Where information relating to cryptography is revealed for these purposes, it has to be protected from unauthorised disclosure. There is an overarching protection for law enforcement and national security authorities to require access to encrypted and unencrypted communications, pursuant to legal procedures. This gives these agencies far more extensive power than under the security exception.

The illegitimacy of the JSI

The WTO has a longstanding Work Programme on Electronic Ccommerce to be conducted through its standing Councils. The JSI negotiations have no such mandate. The text assumes it will become a WTO agreement, for example providing that only the WTO's Dispute Settlement Understanding would apply, as provided in the GATT and GATS.

The article on Relation to Other Agreements says only the Parties would have rights and obligations under the agreement. That suggests a plurilateral agreement, whose adoption under Annex 4 of the Marrakesh Agreement requires the consensus of all WTO Members, similar to attempts being made to adopt the JSI on investment facilitation under Annex 4. Currently there are only 90 of the soon-to-be 166 WTO Members participating in the plurilateral initiative on e-commerce.

Alternatively, the participants might argue that this is predominantly a trade in services agreement and attempt to introduce the agreement through Members' GATS schedules. That would significantly expand participating Members' GATS obligations and add new rules to the GATS for those Members without formally amending the GATS through the Marrakesh Agreement procedures. A similar approach was pursued for the JSI on services domestic regulation, which South Africa and India challenged as an abuse of GATS schedules and creating a precedent for amending agreements through the backdoor. A review of this abuse of schedules, provided for under the relevant WTO documents (S/L/84 and S/L/80), is currently being proposed.

Jane Kelsey *<j.kelsey@auckland.ac.nz> is Professor Emeritus at the University of Auckland.*