Note

Electronic Commerce Joint Statement: Issues in the Negotiations Phase

By Katya Garcia-Israel and Julien Grollier

Summary

Electronic commerce has been a topic of interest within the WTO since the second Ministerial Conference in 1998. At the 11th Ministerial Conference in Buenos Aires on 13 December 2017, 71 members signed a joint statement announcing their objective of "advancing electronic commerce work in the WTO" as a group. In a second joint statement this year, they expressed their intention to begin electronic commerce negotiations at the WTO, based on "existing WTO agreements and frameworks." After a previous note (http://bit.ly/2XJgsYk) focused on issues during the discussions phase, the present note provides an overview of the meetings and proposals tabled during the negotiations phase.

KEEPING PACE WITH TRADE DEVELOPMENTS
This publication is published under the project "Keeping Pace with Trade Developments", undertaken with funding support from the Ministry of Foreign Affairs, Sweden.

FUNDING SUPPORT | RAPID-RESPONSE NOTE

Introduction

Electronic commerce has been a topic of interest within the WTO since the second Ministerial Conference in 1998, when the Declaration on Global Electronic Commerce was announced and the Work Programme on Electronic Commerce was created.[1]

The first Joint Statement on Electronic Commerce was released at the 11th Ministerial Conference in Buenos Aires on 13 December 2017. The 71 signatory members to the first joint statement announced their objective of "advancing electronic commerce work in the WTO" as a group, and hosting an initial meeting in early 2018, open to all member countries.[2] The intention of the meetings held in 2018 was to "initiate exploratory work together toward future WTO negotiations on trade-related aspects of electronic commerce."[3]

The joint statement of 25 January 2019 expresses the participating members' intention to begin electronic commerce negotiations at the WTO, based on "existing WTO agreements and frameworks."[4] The document elaborates that the members hope to include "as many WTO Members as possible,"[5] while acknowledging that developing countries and LDCs face different challenges associated with electronic commerce.

After a previous note (http://bit.ly/2XJgsYk) focused on issues during the discussions phase of 2018, the present note provides an overview of the meetings and proposals tabled during the negotiations phase since early 2019, including proposed definitions of selected terms.

Group composition and structure

Number of members: 77 as of 29 March 2019

LDC members: Benin, Lao People's Democratic Republic, and Myanmar

Number of Meetings: 12

Table 1: Least-developed countries in the Joint Statement on Electronic Commerce

LDCs in the Joint Statement on Electronic Commerce
Benin[6], Cambodia (withdrew; only present in 2017 statement), Lao People's Democratic Republic, Myanmar

[1] https://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm
[2] Joint Statement on Electronic Commerce 2017
[3] Joint Statement on Electronic Commerce 2017
[4] Joint Statement on Electronic Commerce 2019
[5] Joint Statement on Electronic Commerce 2019
[6] Joined on 29 March 2019 (INF/ECOM/18)

Table 2: Developing Countries[7] and LDCs[8] in the E-commerce Joint Statement (by region)

Asia	Africa	Central America and Mexico	South America
Bahrain	Benin*	Costa Rica	Argentina
Brunei Darussalam	Nigeria	El Salvador	Brazil
China		Honduras	Chile
Hong Kong		Mexico	Colombia
United Arab Emirates		Nicaragua	Paraguay
Israel		Panama	Peru
Kuwait			Uruguay
Lao People's Democratic Republic*			
Malaysia			
Mongolia			
Myanmar*			
Qatar			
Republic of Korea			
Singapore			
Taiwan			
Thailand			
Turkey			

Table 3: Emerging Economies[9] in the E-commerce Joint-Statement

G20 Members
Argentina, Brazil, China, Mexico, Turkey

[7] Country classifications based on UN 2014 country tables: https://www.un.org/en/development/desa/policy/wesp/wesp_current/2014wesp_country_classification.pdf
[8] (*) indicates LDC status
[9] Proxy for "emerging economies" is the developing countries in the G20 (http://g20.org.tr/about-g20/g20-members/)

Table 4. Economies in Transition Not Present in the E-commerce Joint Statement

Economies in Transition Not Present in Joint Statement[10]
Armenia, Kyrgyzstan, Republic of Moldova, Tajikistan

Membership Patterns

Various changes in membership occurred between the issuing of the 2017 Joint Statement on E-commerce and the 2019 Joint Statement. By the time of release of the 25 January 2019 Joint Statement, Cambodia and Guatemala were no longer part of the joint statement group. China, El Salvador, Georgia, Honduras, Mongolia, Nicaragua, Thailand, and the United Arab Emirates joined the group, raising the number of participants to 76. After the 2019 Joint Statement was released, Benin also joined the group as its 77th member on 29 March 2019.[11]

There are 29 developing countries in the joint statement, and three least-developed countries: Benin, Lao PDR and Myanmar. The regions that are least represented in the joint statement are Africa, with only two members from the continent participating, Benin and Nigeria, and the Caribbean, with no participants. None of the developing Pacific Island countries are part of the joint statement. The region of Central America and Mexico has the highest rate of participation as Guatemala is the only member not listed in the 2019 joint statement. Overall, most of the developing country members of the joint statement are in Asia, followed by South America. All developed countries were present in the joint statement as well as all but four of the countries categorized as "economies in transition."[12]

Timeline and Themes of Meetings since January 2019[13]

25 January 2019: Meeting for the 2019 Joint Statement

6 March 2019: Meeting to begin negotiations: In this meeting, organized by Australia, members discussed the negotiation process, deciding to "table negotiating texts by the end of April" and start the next negotiations on 13-15 May.[14]

13-15 May 2019: Discussion of negotiation text proposals

Key issues

In the country proposal documents submitted to the group, the most common issues raised included open trade environments/trade facilitation, customs duties, privacy protection and online security, infrastructure for digital

[10] Country classifications based on UN 2014 country tables: https://www.un.org/en/development/desa/policy/wesp/wesp_current/2014wesp_country_classification.pdf
[11] INF/ECOM/18
[12] Country classifications based on UN 2014 country tables: https://www.un.org/en/development/desa/policy/wesp/wesp_current/2014wesp_country_classification.pdf
[13] http://www.meti.go.jp/english/press/2018/0315_002.html Japanese Ministry for Economy, Trade, and Industry
[14] https://borderlex.eu/beyond-brussels-wto-e-commerce-talks-get-off-to-uneasy-start/

trade, electronic payments and paperless trading, intellectual property, data localization, domestic regulations, developing countries and LDCs' interests, and inclusion of women and MSMEs. The need for discussion of jurisdiction and cooperation between countries was emphasized throughout the various documents. Concerning past agreements, members stated the intention to clarify them in future discussions but keep the agreements separate from new negotiations to avoid disagreement.

Infrastructure for digital trade, electronic payments and paperless trading were all considered to be essential to trade facilitation and allowing for inclusive access to markets. The legality and security of electronic contracts and signatures was also emphasized, as well as electronic payments being crucial to e-commerce growth in developing countries. Within the broader category of 'trade facilitation,' fall the concerns countries have regarding transparent trade regulations, free and open internet, and improved access to information for traders. Regarding customs duties, nearly all the countries that circulated proposals or communications stated that the current customs duties moratorium should be extended permanently.

Domestic regulations were mentioned various times, with the consensus being that members should be free to implement internal fees on goods or services but keep their frameworks transparent. Many proposals also stated that domestic regulations that were contrary to the elements proposed in the electronic commerce framework could be implemented if they were aimed towards a "legitimate policy objective."[15]

Privacy and online security concerns include measures against SPAM, cybersecurity, disinformation issues, consumer confidentiality, and fraudulent business activities. The issues of intellectual property and data ownership were discussed in several documents, with emphasis on source code, copyright, trade secrets, and proprietary algorithms. Countries that mentioned source code emphasized that access to source code should not be a requirement for doing business in any given territory.[16]

The countries that mentioned data localization[17] in their negotiating text proposals wanted no imposition of mandatory requirements for server locations, computer facilities, or national technologies, with the exception of China, which stated that issues of data storage should not be included at the current negotiation stage, due to differences of opinion between members and need for further exploration and discussion.[18]

Countries from varying levels of development included points about including challenges that developing countries face in the agenda for negotiations. Aid for trade and technical assistance were mentioned as possible measures to help "bridge the digital divide."[19] In a recent country document from China, an Electronic Commerce for Development Program was proposed for assisting LDCs and developing

[15] INF/ECOM/20, 23, 24, 25, 27, 28, 31 (Japan, United States, Chinese Taipei, Singapore, Brazil, Ukraine, Republic of Korea)
[16] European Union, United States, Japan, Ukraine, Korea, and Singapore all mentioned source code in their negotiating text proposals
[17] European Union, United States, Japan, Ukraine, Korea, Singapore
[18] INF/ECOM/19
[19] JOB/GC/174

members.[20]

The participation of MSMEs and women was also a point that a few members[21] brought forward to include in future negotiations.

During the meeting in March 2019, the issue of country differentiation was a topic on which countries had differing views. The United States Ambassador to the WTO stated that the negotiation agreements should have "the same obligations for all participants," while the most recent joint statement acknowledges "challenges faced by Members, including developing countries and LDCs."[22]

Steps taken towards commencing negotiations

The Joint Statement released on the 25 of January 2019 declared the joint statement members' intention to begin negotiations regarding electronic commerce. The meeting held on 6 March 2019 , was the first meeting for negotiations. In April and the beginning of May, additional negotiating text proposals were tabled. A recent text proposal submitted by Japan included the establishment of a Committee on Trade-Related Aspects of Electronic Commerce, which would report annually to the General Council and oversee the electronic commerce agreement. Twelve countries have submitted text proposals thus far: Ukraine, Singapore, Hong Kong, Republic of Korea, Brazil, Chinese Taipei, Japan, Canada, New Zealand, European Union, United States, and China. Seven of these countries included definitions of relevant electronic commerce terms in their text proposals.

[20] INF/ECOM/19

[21] Brazil, Ukraine, and the United States explicitly mentioned electronic commerce and MSMEs

[22] WT/L/1056

Annex: Tables of Proposals from the Negotiations Phase

The tables are organized by country and by issue, to facilitate the identification of a country's position on a certain topic. For purposes of comparison within development category, there are two tables: Table 1. Proposals from Developing Countries and Table 2. Proposals from Developed Countries and Economies in Transition. The information displayed in the tables is a mix of summaries and quotations from the country text proposal documents available on the WTO documentation website.[23]

Table 1. Proposals from Developing Countries

	Brazil[24]	China[25]	Chinese Taipei[26]	Hong Kong[27]	Republic of Korea[28]	Singapore[29]
Infrastructure for Electronic Trade	Free and open internet for "all legitimate commercial and development purposes"		"the internet should remain free and open for all legitimate commercial and development purposes"			
Open trading environment/trade facilitation	Avoid "barriers that constitute a disguised restriction on digital trade" Competition should not be prevented by online platforms	Emphasis on transparency in e-commerce laws and regulations Members should undertake "joint study and cooperative		Members should "open up government data and facilitate public access", using machine-readable formats and updating	Parties should ensure consistency, transparency, and efficiency in their customs procedures and be open about providing information	"members shall allow the cross-border transfer of information by electronic means" for business purposes[31] Measures that do not allow cross-border electronic information

[23] https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S001.aspx
[24] INF/ECOM/27
[25] INF/ECOM/19, INF/ECOM/32
[26] INF/ECOM/24
[27] INF/ECOM/26
[28] INF/ECOM/31
[29] INF/ECOM/25
[31] INF/ECOM/25, p. 3

	Brazil[24]	China[25]	Chinese Taipei[26]	Hong Kong[27]	Republic of Korea[28]	Singapore[29]
	Online platforms should not give "arbitrary or unjustifiable" advantages to their own products International cooperation for measuring digital trade flows	training" to promote information exchange		information in a timely manner[30]	regarding its procedures	transfer may be enacted if they are for a "legitimate policy objective"[32]
Electronic Payments, Contracts, and Paperless trading	Electronic contracts, signatures, and authentications should not be denied legality Parties involved in an electronic contract should be allowed to "mutually determine the appropriate electronic methods for their transaction" Members can enact specific "objective, transparent, and non-discriminatory" standards for authentication Administrative documents should be available electronically to the public	Electronic payments, trade administration documents, invoices, contracts and signatures should be legally treated in the same way as their paper counterparts Trade administration documents should be made publicly available in electronic form		Electronic signatures should be given legal validity Encourage electronic authentication Parties shall be able to "mutually determine the appropriate authentication methods" for their transaction and be allowed to defend it before judicial authorities Members may require their own specific authentication standards Electronic trade administration documents should be legally accepted	Electronic signatures should not be denied legal validity Parties should not be prevented from negotiating the best authentication methods for their transaction or from defending their transaction before the relevant authorities Members may require their own specific authentication standards for certain types of transactions Trade administration documents should be made electronically available and legally equivalent to the paper versions	Trade administration documents should be legally accepted in electronic form except in cases with a "legal requirement to the contrary"[33] International cooperation "to enhance acceptance of electronic versions" is needed[34] Electronic signatures should be legally accepted Parties may decide the best authentication methods for their transactions; however members may call for specific authentication standards for certain transaction types Members should allow parties to bring the case

[30] INF/ECOM/26, p.3
[32] INF/ECOM/25, p. 3
[33] INF/ECOM/25, p.1
[34] INF/ECOM/25, p.1

	Brazil[24]	China[25]	Chinese Taipei[26]	Hong Kong[27]	Republic of Korea[28]	Singapore[29]
	No prior authorization principle International cooperation to promote paperless trading					of their transaction and authentication "before judicial or administrative authorities"[35] E-invoicing systems and electronic transferable records should be recognized and encouraged
Customs Duties	Members should not have customs duties for electronic transmissions Members should not be prevented from having taxes or fees if they are "imposed in a manner consistent with this Agreement and on a non-discriminatory basis"	The customs duties moratorium for electronic transmissions should continue		No customs duties shall be imposed on electronic transmissions; however, countries are free to impose their own internal fees if those are "consistent with the rules of the WTO"	No customs duties should be placed on electronic transmissions "including content transmitted electronically"[36] Customs administration should be "predictable, consistent, transparent, and efficient"[37]	No customs duties shall be placed on electronic transmissions between members Members can place internal fees or charges on electronic content if such measures are "consistent with WTO agreements"[38]
Domestic Regulations	Clear frameworks to facilitate e-commerce development Members may adopt exceptions to allowing cross-border electronic information transfer provided that such exceptions "achieve a	Agreement should take "full consideration of Members' right to regulate"[39] Differing "industry development conditions, historical and cultural traditions, legal systems," and e-	Members may establish exceptions to the agreement of not restricting cross-border electronic information transfer if it is not "arbitrary or unjustified discrimination" or if it is "necessary to achieve	Members should establish a legal framework for electronic transactions	Parties may enact measures that impede the cross-border transfer of information if they are implemented to "achieve a legitimate	Regulatory measures should not be burdensome Members should "facilitate input by interested persons in the development of its legal framework"[42]

[35] INF/ECOM/25, p.2
[36] INF/ECOM/31
[37] INF/ECOM/31 Article 6
[38] INF/ECOM/25, p.2
[39] INF/ECOM/19 p.1
[42] INF/ECOM/25, p.2

	Brazil[24]	China[25]	Chinese Taipei[26]	Hong Kong[27]	Republic of Korea[28]	Singapore[29]
	legitimate public policy objective" and are not "arbitrary or unjustifiable" Members will not be prevented from enacting measures for "protect(ing) public morals or public order", safety, security, privacy, war or emergency purposes	commerce development paths must be understood and respected[40]	a legitimate public policy objective" "a party may maintain a measure inconsistent with this agreement provided that such a measure is listed in its Schedule in the Annex of this Agreement"		public policy objective"[41] Parties may implement any measure deemed necessary for its security interests	
Intellectual Property and Source Code					Parties should not require access to or transfer of source code or software as a condition of selling the software in its territory Parties should allow users of other parties "access to and use of interactive computer services on fair terms"[43]	Access to source code should not be required "as a condition for the import, distribution, sale or use of such software"; however, this does not apply to "software used for critical infrastructure"[44] Members may call for modification of source code "to comply with laws or regulations that are not inconsistent with this Agreement"[45]
Privacy and Consumer Protection	Consumers should not be sent marketing communications without consent	Personal information of e-commerce users should be protected by members using the		Members should establish consumer protection laws to protect against "fraudulent and	Parties should create measures for consumer protection that are "equivalent to those provided for	Measures should be adopted to ensure that consumers can opt out of receiving spam messages and that their

[40] INF/ECOM/19 p.3
[41] INF/ECOM/31 p.5
[43] INF/ECOM/31
[44] INF/ECOM/25, p. 4
[45] INF/ECOM/25, p. 4

	Brazil[24]	China[25]	Chinese Taipei[26]	Hong Kong[27]	Republic of Korea[28]	Singapore[29]
	Social media platforms and digital apps should "inform consumers of the use of their personal information" Measures should be taken to prevent fraudulent commercial activities and give redress to consumers Data privacy requires international cooperation Members should form frameworks for personal data protection and publish information about them	measures they deem necessary No unsolicited electronic commercial messages to nonconsenting consumers Members should "publish information on the personal information protections they provide"[46] including how individuals may pursue redress and businesses can comply with requirements Online consumers should be protected similarly to other consumers Judicial procedures should be maintained to solve disputes between consumers and e-commerce providers Members should increase cooperation between national consumer protection agencies		deceptive commercial practices"[47] National consumer protection agencies should cooperate at the international level Members should create legal frameworks to protect users' personal information Redress and compliance information for individuals and businesses should be published Regarding unsolicited commercial electronic messages: consumers should be given the option of opting out of messages, or consumer consent must be required before sending messages	consumers engaged in other forms of transaction"[48] An Online Dispute Resolution (ODF) scheme should be established by each party National consumer protection agencies should cooperate at the international level Parties "should publish information on the personal information protections it provides"[49] including how individuals can get redress and business compliance guidelines Parties should establish regulations on unsolicited commercial electronic messages	consent must be obtained "Members shall provide recourse" against non-complying suppliers[50] Members should provide legal frameworks for protecting personal information of e-commerce users Information regarding redress and compliance for individuals and businesses shall be published Members should recognize the differing legal frameworks of other members regarding personal information protection

[46] INF/ECOM/32 p.3
[47] INF/ECOM/26, p. 2
[48] INF/ECOM/31
[49] INF/ECOM/31
[50] INF/ECOM/25, p. 5

	Brazil[24]	China[25]	Chinese Taipei[26]	Hong Kong[27]	Republic of Korea[28]	Singapore[29]
Online Security	International cooperation needed on matters of cybersecurity Members should build cybersecurity response capacities	Consumers using electronic commerce should be given protection like that of other consumers Members should increase cooperation and share best practices regarding cybersecurity			Parties should increase capabilities of bodies in charge of computer security Parties should collaborate to identify the "dissemination of malicious code that affects the electronic networks"[51]	Members should provide consumer protection through laws against "fraudulent and deceptive commercial activities"[52] International cooperation between national consumer protection agencies is crucial
Data Localization		The negotiations should not include the issues of data flow or data storage or treatment of digital products at this time, due to differing views of Members[53]			Parties shall not "require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory" unless such measures are needed for "legitimate public policy objectives"[54]	"Members shall not require the use or location of computing facilities in its territory as a condition for conducting business in that territory" except in the case of meeting "a legitimate public policy objective"[55]
Developing Countries and LDCs' interests		Negotiation objectives to assist developing and LDC members to "integrate into global value chains, bridge the digital divide" and help make trade more inclusive				

[51] INF/ECOM/31 p. 7
[52] INF/ECOM/25, p.6
[53] INF/ECOM/19
[54] INF/ECOM/31 p.6
[55] INF/ECOM/25, p.3

	Brazil[24]	China[25]	Chinese Taipei[26]	Hong Kong[27]	Republic of Korea[28]	Singapore[29]
		An Electronic Commerce for Development program should be created under the WTO framework to assist LDCs and developing members				
Inclusion (MSMEs and women)	It is important for MSMEs to increase their digital trade participation					
Digital Products		The negotiations should not include the issues of data flow or data storage or treatment of digital products at this time, due to differing views of Members[56]				
Past Agreements/Frameworks		"this negotiation should be complementary to the electronic commerce discussion in relevant subsidiary bodies of the WTO" and these bodies "should be informed of negotiation progress" The connection between current and past agreements should be clarified		Members' legal frameworks should be "consistent with the principles of the UNCITRAL Model Law on Electronic Commerce 1996 or the United Nations Convention on the Use of Electronic Communications in International Contracts"		Members' legal frameworks should be "consistent with the principles of the UNCITRAL Model Law on Electronic Commerce 1996 or the United Nations Convention of the Use of Electronic Communications in International Contracts, 2005"[57]

[56] INF/ECOM/19
[57] INF/ECOM/25, p. 2

Table 2. Proposals from Developed Countries and Economies in Transition

	Canada[58]	European Union[59]	Japan[60]	New Zealand[61]	United States[62]	Ukraine[63]
Infrastructure for Electronic Trade	Consumers should be able to "access and use services and applications" of their choice, "subject to reasonable network management"[64]	Open internet access should be maintained in Members' territories	Consumers should have the ability to access information and services on the internet "subject to reasonable network management"[65]			Customers should have the ability to access information and services on the internet "subject to reasonable network management"[66]
Open trading environment/ trade facilitation			Open cross-border electronic transfer of information when it is for business purposes between members (Exception: members may apply restrictions when needed for "a legitimate public policy objective"[67] Members should increase public access of government data		Cross-border electronic information transfer should not be restricted if it is for business purposes (unless the restrictions are for "legitimate public policy objective(s)" and are not a "disguised restriction on trade"[68] Government data, when publicly available, should be	Government data that is publicly available should be searchable and usable

[58] INF/ECOM/29, INF/ECOM/30
[59] INF/ECOM/22
[60] INF/ECOM/20
[61] INF/ECOM/21
[62] INF/ECOM/23
[63] INF/ECOM/28
[64] INF/ECOM/30, Article 2
[65] INF/ECOM/20, p. 6
[66] INF/ECOM/28 p.4
[67] INF/ECOM/20 p. 6
[68] INF/ECOM/23 p.5

	Canada[58]	European Union[59]	Japan[60]	New Zealand[61]	United States[62]	Ukraine[63]
			Any government data that is made public should be available in a usable form		presented in a usable form	
Electronic Payments, Contracts, and Paperless Trading	Electronic signatures should not be denied legal validity Parties should not be prevented from negotiating the best authentication methods for their transaction and should not be prevented from defending the legality of their transaction before the relevant authorities Parties may require specific certification or performance standards for certain types of transactions	Electronic contracts should not be denied legality solely because they are in electronic form[69] Parties may negotiate the best authentication methods for their transaction and should not be prevented from proving the legality of their authentication to the relevant authorities Members may require specific certification standards for different types of transactions, provided standards are "objective, transparent, and non-discriminatory"[70]	Electronic signatures should be legally accepted unless domestic regulations specify otherwise Parties should be allowed to negotiate the best authentication methods for their transaction and should not be prevented from proving the legality of their authentication methods to relevant authorities Electronic trade administration documents should be made publicly available and legally acceptable		Electronic signatures should be legally accepted Parties should be allowed to negotiate the best authentication methods for their transaction and should not be prevented from defending the legality of their transaction before the relevant authorities Members may require certain authentication standards for specific types of transactions	Electronic signatures should not be denied legal validity Parties should not be prevented from determining the best authentication methods for their contract or from defending the legality of their transaction before the relevant authorities Members may require certain authentication standards for specific types of transactions Electronic trade administration documents should be made publicly available and legally accepted
Customs Duties	No imposition on custom duties for electronically transmitted digital products Members may have internal fees on digital products		No customs duties should be imposed on electronic transmissions between members		No customs duties should be imposed on electronic transmissions	No customs duties should be imposed on electronic transmissions (yet members may impose internal fees)

[69] Note: This statement "does not apply to broadcasting services, gambling services, legal representation services", notaries or equivalent professions, real estate, "contracts requiring by law the involvement of courts, public authorities of professions exercising public authority, contracts of suretyship granted and or collateral securities furnished by persons acting for purposes outside their trade, business or profession and contracts governed by family law or by the law of succession" INF/ECOM/22 p.1

[70] INF/ECOM/22 p.2

	Canada[58]	European Union[59]	Japan[60]	New Zealand[61]	United States[62]	Ukraine[63]
Domestic Regulations			Members' regulations should be "transparent, objective, reasonable" and designed "to meet legitimate public policy objectives"[71] Measures should be made publicly available in a timely fashion		Parties should "avoid unnecessary regulatory burden" and "facilitate input by interested persons in the development of its legal framework"[72]	Members should "avoid unnecessary regulatory burden on electronic transactions" and "facilitate input by interested persons in the development of its legal framework"[73]
Intellectual Property and Source Code		"Members shall not require the transfer of, or access to, the source code of software owned by a natural or juridical person of other Members" The above is "without prejudice to" cases of violation of competition law, intellectual property rights protection, and national security interests [74]	"No member shall require the transfer of, or access to source code of software owned by a person of another Member" Members can require source code modification for compliance "with laws and regulations which are not inconsistent with this Agreement"[75] exceptions to no disclosure of source code: patent or court requirements Members should not require manufacturers or suppliers to disclose information or access to any technology or		"No party shall require the transfer of, or access to, source code of software owned by a person of another Party"[76] except in cases of legal investigations or enforcement action	No requirements for access to source code as a condition for trade (except in the cases of achieving "a legitimate public policy objective," enforcement of intellectual property rights, security concerns, or court requirements[77]

[71] INF/ECOM/20 p.5
[72] INF/ECOM/23 p.4
[73] INF/ECOM/28 p.1
[74] INF/ECOM/22 p.3
[75] INF/ECOM/20 p.8
[76] INF/ECOM/23 p.6 Article 12
[77] INF/ECOM/28 p.4

	Canada[58]	European Union[59]	Japan[60]	New Zealand[61]	United States[62]	Ukraine[63]
			cryptography used in a product (except in cases of government-controlled networks and law enforcement matters)			
Privacy and Consumer Protection		Measures should be taken to ensure that consumers have opportunity for redress and traders are providing true information Consumers should be protected against unsolicited commercial electronic messages by requiring consent of the recipient and the opportunity to opt out Suppliers should be obligated to disclose "on whose behalf [unsolicited electronic messages] are sent"[78] "Members recognize the protection of personal data and privacy is a fundamental right" and relevant safeguards should be applied[79]	Members should take consumer protection measures against "fraudulent and deceptive commercial activities"[80] Members should create their own frameworks specifying privacy protection measures Information regarding how to seek redress and how to comply with legal regulations should be published Members should cooperate amongst themselves to ensure that privacy protection frameworks are compatible In the case of unsolicited commercial electronic messages, consumers must give consent to receive them	Members should enact consumer protection laws to avoid harm from "misleading and deceptive conduct" (including misrepresentations and false claims, false advertising, failure to or no intention to deliver products, unauthorized charging of consumers' financial or telephone accounts)[81] Members' national consumer protection agencies should increase cooperation	Members should enact regulations for protection of personal information Information regarding access to redress and how businesses comply with regulations should be publicly available "Any restrictions on cross-border flows of personal information [should be] necessary and proportionate to the risks presented"[82]	Members should enact consumer protection laws and increase international cooperation between relevant national authorities Members should create frameworks for personal data protection Members should develop compatible mechanisms that allow for increased cooperation between jurisdictions Measures should be taken to allow consumers to opt out or give prior concept before receiving unsolicited commercial electronic messages

[78] INF/ECOM/22 p. 3
[79] INF/ECOM/22 p. 4
[80] INF/ECOM/22 p.7
[81] INF/ECOM/21 p. 1
[82] INF/ECOM/23 p.4

	Canada[58]	European Union[59]	Japan[60]	New Zealand[61]	United States[62]	Ukraine[63]
			or be given a way to opt out			
Online Security			Members should build their capacity to respond to cybersecurity threats and collaborate with other Members		Members should build their capacity to respond to cybersecurity threats and "strengthen existing collaboration mechanisms"[83] "Risk-based approaches" should be implemented for cybersecurity threat responses[84]	Members should build their capacity to respond to cybersecurity threats and increase existing international cooperation
Data Localization		Members should not require data to be processed at computing facilities in their territories No requirement of data localization No prohibition on storing or processing data in other Members' territories	"No member shall require a person of Members to use or locate computing facilities in that Member's territory as a condition for conducting business in that territory" except in cases where "legitimate public policy objective(s)" are being met[85]		"No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory"[86] No requirements regarding the locations of financial services computing facilities	No requirements for the location of computing facilities in a Member's territory (unless they are undertaken "to achieve a legitimate public policy objective"[87])
Developing Countries and LDCs' interests						Future texts should include "appropriate and effective special and differential treatment for developing country

[83] INF/ECOM/23 p.5 Article 11
[84] INF/ECOM/23 p.5 Article 11
[85] INF/ECOM/20 p.7
[86] INF/ECOM/23 p. 5 Article 9
[87] INF/ECOM/28 p.4

	Canada[58]	European Union[59]	Japan[60]	New Zealand[61]	United States[62]	Ukraine[63]
						Members and least developed country Members"[88]
Inclusion (MSMEs and women)					Interactive computer services should be promoted for e-commerce growth, and are important for small and medium-sized enterprises (SMEs) Open government data is especially important for SMEs	Increasing public availability to government data is important for SMEs
Digital Products			No discrimination in treatment of digital products (not applicable in cases of broadcasting)		Digital products shall not be given less favorable treatment (not applicable in cases of subsidies such as government-supported loans or insurance)	No discrimination in treatment of digital products
Past Agreements/Frameworks			Articles XXII and XXIII of GATT 1994 should apply to dispute settlement			WCO cross-border E-commerce Framework of Standards should serve as a basis

[88] INF/ECOM/28 p.5

Table 3: Tables of Definitions from Country Proposals[89]

Developing Countries		
	Hong Kong[90]	**Korea[91]**
Algorithm		
Cipher		
Computing facility		"computer servers and storage devices for processing or storing information for commercial use"
Covered financial service supplier		
Covered person		"with respect to a Party, an investment in its territory of an investor of another Party in existence as of the date of entry into force of this Agreement for those Parties or established, acquired, or expanded thereafter; (b) a Party, or a national or an enterprise of a Party, that attempts to make, is making, or has made an investment in the territory of another Party, with an exception of an investor in a financial institution; or (c) a person of a Party that seeks to supply of supplies a services,"
Cryptography		
Customs duty		Customs procedure: "the treatment applied by each customs authorities to goods and means of transport that are subject to customs law"
Digital product		
Electronic authentication	"the process of establishing and subsequently verifying the identity of a party to an electronic communication or transaction or ensuring the integrity of an electronic communication"	"the process or act of establishing the identity of a party to an electronic communication or transaction or ensuring the integrity of an electronic communication"
Electronic signature		"data in electronic form that is in, affixed to, or logically associated with, an electronic document, and that may be used to identify the signatory in relation to the INF/ECOM/31 - 2 - electronic document and indicate the

[89] Singapore's statement on definitions: "We have excluded Definitions, Scope and General Provisions relating to the proposed disciplines below as these would be dependent on the legal architecture and will be determined in the course of the negotiations." (INF/ECOM/25)
[90] INF/ECOM/26
[91] INF/ECOM/31

Developing Countries		
	Hong Kong[90]	**Korea[91]**
		signatory's approval of the information contained in the electronic document”
Electronic transmission		“a transmission made using any electromagnetic means, including by photonic means”
Encryption		
Enterprise		“any entity constituted or organized under applicable law, whether or not for profit, and whether privately or governmentally owned or controlled, including any branch, corporation, trust, partnership, sole proprietorship, joint venture, association or similar organization”
Essential facilities		
Financial institution, financial institution of another party		
Financial market infrastructure		
Financial service		
Financial service computing facility		
Financial service supplier of another party		
Fraudulent or deceptive commercial activities		
Government data	“non-proprietary data held by the government, except personal data”	
Government procurement		“process by which a government obtains the use of or acquires goods or services, or any combination thereof, for governmental purposes and not with a view to commercial sale or resale or use in the production or supply of goods or services”
Information content provider		
Interactive computer service		“the process by which a government obtains the use of or acquires goods or services, or any combination thereof, for governmental

Developing Countries		
	Hong Kong[90]	**Korea**[91]
		purposes and not with a view to commercial sale or resale or use in the production or supply of goods or services”
Interconnection		
investment		“every asset that an investor owns or controls, directly or indirectly, that has the characteristics of an investment, including such characteristics as the commitment of capital or other resources, the expectation of gain or profit, or the assumption of risk”
Key		
Major supplier		
measure		
Network element		
Person		“a natural person or an enterprise”
Personal information	“any information, including data, relating to an identified or identifiable natural person”	“any information, including data, about an identified or identifiable natural person”
Service supplied in the exercise of governmental authority		
Telecommunications regulatory authority		
Trade administration documents	“forms issued or controlled by a Member that must be completed by or for an importer or exporter in connection with the importation or exportation of goods”	“forms issued or controlled by a Party that must be completed by or for an importer or exporter in connection with the import or export of goods”
Unsolicited commercial electronic message	“an electronic message which is sent for commercial purposes without the consent of the recipient or against the explicit rejection of the recipient, using an internet access service supplier or, to the extent provided for under the laws and regulations of each Member, other telecommunications service”	“an electronic message which is sent for commercial or marketing purposes to an electronic address, without the consent of the recipient or despite the explicit rejection of the recipient, through an Internet access service supplier or, to the extent provided for under the laws and regulations of each Party, other telecommunications service”
User		“a consumer and an enterprise”

Developed Countries					
	Canada[92]	EU[93]	Japan[94]	New Zealand [95]	United States[96]
Algorithm			"means a defined sequence of steps, taken to solve a problem or obtain a result"		"a defined sequence of steps taken to solve a problem or obtain a result"
Cipher or cryptographic algorithm			"a mathematical procedure or formula for combining a key with plaintext to create a ciphertext"		
Computing facility			"computer servers and storage devices for processing or storing information for commercial use"		"a computer server or storage device for processing or storing information for commercial use"
Covered financial service supplier					"(a) a financial institution of another Party; or (b) a financial service supplier of another Party, other than a financial institution of another Party, that is subject to regulation, supervision, and licensing, authorization, or registration by a financial regulatory authority of the Party"
Cryptography			"the principles, means or methods for the transformation of data in order to hide its information content, prevent its undetected modification or prevent its unauthorised use; and is limited to the transformation of information using one or more secret parameters, for example, crypto variables, or associated key management"		

[92] INF/ECOM/30
[93] INF/ECOM/22
[94] INF/ECOM/20
[95] INF/ECOM/21
[96] INF/ECOM/23

Developed Countries					
	Canada[92]	**EU[93]**	**Japan[94]**	**New Zealand [95]**	**United States[96]**
Customs duty			"any duty or charge of any kind subject to Articles I and II and other relevant provisions of the General Agreement on Tariffs and Trade 1994 in Annex 1A (hereinafter referred to in this Agreement as "GATT 1994") to the Agreement Establishing the World Trade Organization (hereinafter referred to in this Agreement as the "WTO Agreement"), but does not include any duty, fee or charge referred to in subparagraphs 2(a) to 2(c) in Article II of GATT 1994"		"a duty or charge of any kind imposed on or in connection with the importation of a good, and any surtax or surcharge imposed in connection with such importation, but does not include any: (a) charge equivalent to an internal tax imposed consistently with Article III:2 of GATT 1994; (b) fee or other charge in connection with the importation commensurate with the cost of services rendered; or (c) antidumping or countervailing duty"
Digital product	"a computer program, text, video, image, sound recording, or other product that is digitally encoded, produced for commercial sale or distribution, and that can be transmitted electronically"		"a computer programme, text, video, image, sound recording or other product that is digitally encoded, produced for commercial sale or distribution, and that can be transmitted electronically; (i), (ii) 5 (i) The definition of digital product should not be understood to reflect a Member's view on whether trade in digital products through electronic transmission should be categorised as trade in services or trade in goods. (ii) For greater certainty, digital product does not include a digitised representation of a financial instrument, including money."		"a computer program, text, video, image, sound recording, or other product that is digitally encoded, produced for commercial sale or distribution, and that can be transmitted electronically. A digital product does not include a digitized representation of a financial instrument, including money"
Electronic authentication	"the process or act of verifying the identity of a Party to an electronic communication or transaction and ensuring the integrity of an electronic communication"	"the process or act of verifying the identity of a party to an electronic communication or transaction, or ensuring the origin and integrity of data in electronic form"	"the process or act of verifying the identity of a party to an electronic communication or transaction and ensuring the integrity of an electronic communication"		"the process or act of verifying the identity of a party to an electronic communication or transaction and ensuring the integrity of an electronic communication"

Developed Countries					
	Canada[92]	**EU**[93]	**Japan**[94]	**New Zealand** [95]	**United States**[96]
Electronic signature	"data in electronic form that is in, affixed to, or logically associated with, an electronic document or message, and that may be used to identify the signatory in relation to the electronic document or message and indicate the signatory's approval of the information contained in the electronic document and message"	"data in electronic form, which is attached to or logically associated with other data in electronic form that: (a) is used by a natural person to agree on the data to which it relates; or (b) is used by a juridical person to ensure the origin and integrity of the data to which it relates; and (c) ensures that any subsequent change in the data to which it relates is detectable"			"data in electronic form that is in, affixed to, or logically associated with an electronic document or message and that may be used to identify the signatory in relation to the electronic document or message and indicate the signatory's approval of the information contained in the electronic document or message"
Electronic transmission			"a transmission made using any electromagnetic means, including by photonic means"		"a transmission made using any electromagnetic means"
Encryption			"the conversion of data (plaintext) into a form that cannot be easily understood without subsequent re-conversion (ciphertext) through the use of a cryptographic algorithm"		
Enterprise			"any entity constituted or organised under applicable law, whether or not for profit, and whether privately or governmentally owned or controlled, including any corporation, trust, partnership, sole proprietorship, joint venture, association or similar organisation"		
Essential facilities		"facilities of a public telecommunications transport network or service that (a) are exclusively or predominantly provided by a single or limited number of suppliers; and (b) cannot			

Developed Countries					
	Canada[92]	**EU**[93]	**Japan**[94]	**New Zealand** [95]	**United States**[96]
		feasibly be economically or technically substituted in order to provide a service"			
Financial institution					"a financial intermediary or other enterprise that is authorized to do business and is regulated or supervised as a financial institution under the law of the Party in whose territory it is located"
Financial market infrastructure					"a multi-participant system in which a covered financial service supplier participates with other financial service suppliers, including the operator of the system, used for the purposes of clearing, settling, or recording payments, securities, derivatives, or other financial transactions"
Financial service					"a service of a financial nature. Financial services include all insurance and insurance-related services and all banking and other financial services (excluding insurance), as well as services incidental or auxiliary to a service of a financial nature"
Financial service computing facility					"computer server or storage device for the processing or storage of information for the conduct of business within the scope of the license, authorization, or registration of a covered person"
Financial service supplier of another party					"a financial institution, including a branch, located in the territory of a Party that is controlled by a person of another Party"

Developed Countries					
	Canada[92]	**EU**[93]	**Japan**[94]	**New Zealand** [95]	**United States**[96]
Fraudulent or deceptive commercial activities			"those fraudulent and deceptive commercial practices that cause actual harm to consumers, or that pose an imminent threat of such harm if not prevented, for example: (a) a practice of making misrepresentations of material fact, including implied factual misrepresentations, that cause significant detriment to the economic interests of misled consumers; (b) a practice of failing to deliver products or provide services to consumers after the consumers are charged; or (c) a practice of charging or debiting consumers' financial, telephone or other accounts without authorization"	Misleading or deceptive conduct	
Government data					Government information: "non-proprietary information, including data, held by the central government"
Information content provider					"a person or entity that creates or develops, in whole or in part, information provided through the Internet or another interactive computer service"
Interactive computer service					"a system or service that provides or enables electronic access by multiple users to a computer server"
Interconnection		"linking with suppliers of public telecommunications transport networks or services in order to allow users of one supplier to communicate with users of the same or another supplier			

Developed Countries					
	Canada[92]	EU[93]	Japan[94]	New Zealand [95]	United States[96]
		or to access services provided by the suppliers involved or any other supplier who has access to the network"			
Key			"a parameter used in conjunction with a cryptographic algorithm that determines its operation in such a way that an entity with knowledge of the key can reproduce or reverse the operation, while an entity without knowledge of the key cannot"		
Major supplier		"a supplier of public telecommunications transport networks or services which has the ability to materially affect the terms of participation (having regard to price and supply) in a relevant market for public telecommunications services as a result of: (a) control over essential facilities; or (b) use of its position in the market"			
measure			"any measure by a Member, whether in the form of a law, regulation, rule, procedure, decision, administrative action, or any other form"		
Network element		"a facility or equipment used in supplying a telecommunications service, including features, functions and capabilities provided by means of that facility or equipment"			

Developed Countries					
	Canada[92]	**EU**[93]	**Japan**[94]	**New Zealand** [95]	**United States**[96]
Person			“a natural person or an enterprise”		Covered person: “a national of a Party or an enterprise of a Party”
Personal information			“any information, including data, about an identified or identifiable natural person”		“information, including data, about an identified or identifiable natural person”
Service supplied in the exercise of governmental authority					“any service that is supplied neither on a commercial basis nor in competition with one or more service suppliers”
Telecommunications regulatory authority		“the body or bodies charged by a Member with the regulation of public telecommunications transport networks and services covered by these principles”			
Trade administration documents			“forms issued or controlled by a Member that must be completed by or for an importer or exporter in connection with the import or export of goods”		
Unsolicited commercial electronic message		Commercial electronic message: “electronic message, which is sent for commercial purposes using telecommunications services, comprising at least electronic mail and, to the extent provided for in domestic law, other types of electronic messages”	“an electronic message which is sent for commercial or marketing purposes to an electronic address, without the consent of the recipient or despite the explicit rejection of the recipient, through an Internet access service supplier or, to the extent provided for under the laws and regulations of each Member, other telecommunications service”		
User		“any natural or juridical person using a public telecommunications transport service”			

CUTS International, Geneva

CUTS International, Geneva is a non-profit NGO that catalyses the pro-trade, pro-equity voices of the Global South in international trade and development debates in Geneva. We and our sister CUTS organizations in India, Kenya, Zambia, Vietnam, Ghana and Washington have made our footprints in the realm of economic governance across the developing world.

This note is authored by Katya Garcia-Israel and Julien Grollier. CUTS' notes are to inform, educate and provoke debate on specific issues. Readers are encouraged to quote or reproduce material from this paper for their own use, provided due acknowledgement of the source is made.

37-39, Rue de Vermont, 1202 Geneva, Switzerland
geneva@cuts.org ● www.cuts-geneva.org
Ph: +41 (0) 22 734 60 80 | Fax: +41 (0) 22 734 39 14 | Skype: cuts.grc
Also at: Jaipur, Lusaka, Nairobi, Accra, Hanoi, Delhi, Calcutta and Washington, D.C