

2023

## CONVERGENCE & DIVERGENCE IN DIGITAL TRADE REGULATION: A COMPARATIVE ANALYSIS OF CP-TPP, RCEP, AND EJSI

Andrew D. Mitchell  
*Monash University, Australia*

Vandana Gyanchandani  
*Monash University, Australia*

Follow this and additional works at: <https://scholarcommons.sc.edu/scjilb>



Part of the [Law Commons](#)

---

### Recommended Citation

Mitchell, Andrew D. and Gyanchandani, Vandana (2023) "CONVERGENCE & DIVERGENCE IN DIGITAL TRADE REGULATION: A COMPARATIVE ANALYSIS OF CP-TPP, RCEP, AND EJSI," *South Carolina Journal of International Law and Business*: Vol. 19: Iss. 2, Article 6.

Available at: <https://scholarcommons.sc.edu/scjilb/vol19/iss2/6>

This Article is brought to you by the Law Reviews and Journals at Scholar Commons. It has been accepted for inclusion in South Carolina Journal of International Law and Business by an authorized editor of Scholar Commons. For more information, please contact [digres@mailbox.sc.edu](mailto:digres@mailbox.sc.edu).

# CONVERGENCE & DIVERGENCE IN DIGITAL TRADE REGULATION: A COMPARATIVE ANALYSIS OF CP-TPP, RCEP, AND EJSI

*Andrew D. Mitchell\* and Vandana Gyanchandani\*\**

## ABSTRACT

The article provides an in-depth comparative legal analysis of the fundamental digital trade provisions in three modern trade agreements: the Comprehensive and Progressive Trans-Pacific Partnership Agreement (CP-TPP), Regional Comprehensive Economic Partnership Agreement (RCEP), and Joint Statement Initiative on electronic commerce (eJSI) draft text. It features new, diverse regulatory priorities and approaches to govern digital trade. The comparative analysis will enable policymakers and civil society to appreciate the underlying regulatory concerns in negotiating digital trade agreements. The analysis aims to support an advancement of such digital trade provisions and make these deliberations more inclusive in future.

## INTRODUCTION

Digital trade, as enabled by cross-border data flows, is the main catalyst of an exponential form of economic globalization which is led by rapid digitalization and emerging new digital technologies. The COVID-19 global pandemic, since March 2020, has led to an exponential shift towards the economic digitalization which has accentuated physical distancing along with the swift proliferation of digital communications to support the global economy and society. The global or regional digital trade regulation is coordinated by specific international trade institutions and agreements, e.g., the WTO Joint Initiative on e-commerce (eJSI).

The article provides a comparative legal analysis of the three significant digital trade agreements: the Comprehensive and Progressive Trans-Pacific Partnership (CP-TPP) Agreement, Regional Comprehensive Economic Partnership (RCEP) Agreement, and the Joint Statement Initiative on e-commerce (eJSI) to rationalize the current regulatory environment. The legal analysis will help the stakeholders understand key opportunities and challenges to regulate digital trade in future.

This article is a significant addition to the existing scholarship on digital trade law<sup>1</sup> because it is a novel attempt to comparatively assess digital trade provisions in three prominent

---

\*Professor, Associate Dean, (Research), Faculty of Law, Monash University, Australia, e-mail address: andrew.mitchell@monash.edu; ORCID ID: <https://orcid.org/0000-0001-8399-8563>.

\*\* PhD Candidate, Faculty of Law, Monash University, Australia, e-mail address: vanadana.gyanchandani@monash.edu; ORCID ID: <https://orcid.org/0000-0002-2969-8516>.

<sup>1</sup> See, e.g., Andrew D. Mitchell & Neha Mishra, *Data at the Docks: Modernising International Trade Law for the Digital Economy*, 20 VAND. J. OF ENT. & TECH. L. 18 (2018); Andrew D. Mitchell, *Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute*, 22 J. OF INT. ECON. L. 3 (2019); Neha Mishra, *International Trade, Internet Governance and the Shaping of the Digital Economy*, UNESCAP ARTNET WORKING PAPER SERIES No. 168 (2017); Neha Mishra, *Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation*, 19 WORLD TRADE REV. 3 (2019); Neha Mishra, *Building Bridges: International Trade Law, Internet Governance, and the Regulation of Data Flows*, 52 VAND. J. TRANSNAT'L L. 2 (2021); Andrew D. Mitchell & Neha Mishra, *A New Digital Economy Collaboration in the Indo-Pacific: Negotiating Digital Trade in the Australia-India CECA*, 57 J. OF WORLD TRADE 1 (2023); Andrew D. Mitchell & Jarrod Hepburn, *Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer*, 19 YALE J. OF L. AND TECH. 192 (2017); Andrew D. Mitchell & Neha Mishra, *WTO Law and*

trade agreements. It discusses the impact of Joint Statement Initiative on e-commerce (eJSI) draft text in relation to the most relevant regional digital trade agreements. The article systematically tracks and examines these new regulatory approaches to regulate digital trade. It aims to make these deliberations intelligible and inclusive for all policymakers and civil society members.

The article consists of five sections. This introduction is the first section. The second section provides a general background to the three covered digital trade agreements. The third section provides a uniform general classification of all digital trade provisions to streamline the discussions among stakeholders. The fourth section provides a substantive comparative legal analysis on the most pertinent digital trade provisions. The fifth section concludes this article.

## I. GENERAL BACKGROUND

A complex political process to reach agreements on “digital trade” in the multilateral context has been the main catalyst for the rise in cross-regional FTA networks as the principal alternative to steer the global regulatory deliberations.<sup>2</sup> It has motivated the policymakers to value strategic and efficacious “minilateral approaches” as compared to the traditionally-established but detrimentally protracted “multilateral approach.”<sup>3</sup>

The RTAs have become the most effective forum to promote digital trade liberalization.<sup>4</sup> The RTAs act as “regional trade regulatory incubators” to experiment with the distinct regulatory approaches and cooperation models as prompted by diverse policy considerations of member states.<sup>5</sup> International deliberations and negotiations in the sphere of digital trade have been mainly led by such RTAs, especially, the Comprehensive and Progressive Trans-Pacific Partnership (CP-TPP) Agreement and the Regional Comprehensive Economic Partnership (RCEP) Agreement as followed by the new WTO Joint Statement Initiative on electronic commerce (eJSI). These RTAs with varied membership cover the most pertinent legal, political, and economic considerations in the governance of digital trade.

---

*Cross-Border Data Flows: An Unfinished Agenda* in Mira Burri (ed.) *Big Data and Global Trade Law*, CAMBRIDGE UNIV. PRESS 83-112 (2021);

Andrew D. Mitchell, *Towards Compatibility: The Future of Electronic Commerce within the Global Trading System*, 4 J. OF INT. ECON. L. 683-723 (2001); Neha Mishra, *Digital Trade in the Australia-EU FTA: A Future-Forward Perspective*, EUROPEAN YEARBOOK OF INT'L ECON. L. (2021); Henry Gao & Gregory C. Shaffer, *The RCEP: Great Power Competition and Cooperation over Trade*, UC IRVINE SCH. OF L. RSCH. PAPER No. 2021-09 (2021); Henry Gao, *Digital or Trade? The Contrasting Approaches of China and US to Digital Trade*, 21 J. OF INT'L ECON. L. 2 (2018); Henry Gao, *Data Regulation with Chinese Characteristics in Mira Burri (ed.) Big Data and Global Trade Law* (2021); Henry Gao, *Across the Great Wall: E-commerce Joint Statement Initiative Negotiation and China* (2020); Henry Gao, *Data Sovereignty and Trade Agreements: Three Digital Kingdoms*, HINRICH FOUND. (2022); Henry Gao, *Regulation of Digital Trade in US Free Trade Agreements: From Trade Regulation to Digital Regulation*, 45 LEGAL ISSUES OF ECON. INTEGRATION 1 (2017).

<sup>2</sup> What is at stake for developing countries in trade negotiations on e-commerce? *The case of the Joint Statement Initiative*, UNCTAD (Feb. 19, 2021), [https://unctad.org/system/files/official-document/ditctncd2020d5\\_en.pdf](https://unctad.org/system/files/official-document/ditctncd2020d5_en.pdf).

<sup>3</sup> Lior Herman, *Multilateralising Regionalism: The Case of E-Commerce*, OECD TRADE POL'Y WORKING PAPER No. 99 (2010), <https://www.oecd-ilibrary.org/docserver/5kmbjx6gw69x-en.pdf?expires=1648094649&id=id&accname=guest&checksum=3440E6A3DB4704075CAD1B421D7EB517>.

<sup>4</sup> JEAN-BAPTISTE VELUT ET AL. EDS., *UNDERSTANDING MEGA FREE TRADE AGREEMENTS* (Routledge Taylor & Francis Group, 1st ed. 2018).

<sup>5</sup> *Id.*

The CP-TPP and RCEP mainly center on the Asia-Pacific region. The TPP prior to CP-TPP was an endeavour by the US to increase its market presence in the Asia-Pacific region vis-à-vis China.<sup>6</sup> However, with the US's withdrawal from TPP and China's active engagement in RCEP, the economic presence of China has increased, as compared to the US, who is not a party to any of the two RTAs.<sup>7</sup> We should appreciate that any regulatory coherence achieved with or within the Asia-Pacific region will be definitive for multilateral consensus on digital trade.<sup>8</sup> Lastly, the co-conveners of WTO eJSI negotiations are from the Asia-Pacific region: Australia, Japan, and Singapore.<sup>9</sup> The Asia-Pacific region plays a leading role in regional and global digital trade negotiations.

The CP-TPP is a mega-regional agreement which was concluded on January 23, 2018, and signed on March 8, 2018, by Australia, Brunei Darussalam, Canada, Chile, Japan, Malaysia, Mexico, Peru, New Zealand, Singapore, and Vietnam, constituting a population of 500 million and 13% of the global economy.<sup>10</sup> The US, Colombia, South Korea, Taiwan, Thailand, Philippines, and China indicated their interest to join the same.<sup>11</sup> Of the list of countries, UK, China, and Taiwan have already applied to join the CP-TPP.<sup>12</sup> The USTR Katherine Tai, in response<sup>13</sup> to a question whether the US aims to join the CP-TPP, said:

I will review CP-TPP to evaluate its consistency with the Build Back Better agenda and whether it would advance the interests of all American workers. I commit to consulting closely with Congress on any trade agreement negotiations.

The basic formulation of working closely with like-minded countries in the Asia-Pacific with shared strategic and economic interests is a sound one, but much has changed in the world since the TPP was signed in 2016. If confirmed, I commit to working closely with like-minded countries in the Asia-Pacific region to deepen our trade relationship in ways that benefits America broadly, including our workers, manufacturers, service providers, farmers, ranchers, and innovators.

Cutler outlines four ways to re-engage the US with the CP-TPP parties: “(1) returning to the original TPP agreement; (2) acceding to the CP-TPP; (3) seeking a broader renegotiation;

---

<sup>6</sup> Henry Gao & Gregory Shaffer, *The RCEP: Great Power Competition and Cooperation over Trade*, LEGAL STUDIES RSCH. PAPER SERIES No. 2021-09 (2021), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3777604](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3777604).

<sup>7</sup> *Id.*

<sup>8</sup> See *Embracing the E-Commerce Revolution in Asia and the Pacific*, U.N. ESCAP & ADB (2018), [https://www.unescap.org/sites/default/files/Embracing%20E-commerce\\_0.pdf](https://www.unescap.org/sites/default/files/Embracing%20E-commerce_0.pdf).

<sup>9</sup> *E-commerce co-convenors release update on the negotiations, welcome encouraging progress*, WTO (Dec. 14, 2020), [https://www.wto.org/english/news\\_e/news20\\_e/ecom\\_14dec20\\_e.htm](https://www.wto.org/english/news_e/news20_e/ecom_14dec20_e.htm).

<sup>10</sup> Hiroshi Matsuura, *Why joining the CP-TPP is a smart move for the UK?*, CHATHAM HOUSE (Mar. 19 2021), <https://www.chathamhouse.org/2021/03/why-joining-cptpp-smart-move-uk>.

<sup>11</sup> Christopher F. Corr et al., *The CPTPP Enters into Force: What Does it Mean for Global Trade?*, WHITE & CASE (Jan. 21 2019), <https://www.whitecase.com/publications/alert/cptpp-enters-force-what-does-it-mean-global-trade>.

<sup>12</sup> Matsuura, *supra* note 10; Shannon Tiezzi, *Wendy Cutler on China, Taiwan and the CP-TPP*, THE DIPLOMAT (Oct. 5, 2021), <https://thediplomat.com/2021/10/wendy-cutler-on-china-taiwan-and-the-cptpp/>.

<sup>13</sup> *Hearing to Consider the Nomination of Katherine C. Tai, of the District of Columbia, to be United States Trade Representative, with the rank of Ambassador Extraordinary and Plenipotentiary*, SENATE FINANCE COMM. (2021), <https://www.finance.senate.gov/imo/media/doc/Katherine%20Tai%20Senate%20Finance%20Committee%20QFRs%202.28.2021.pdf>.

or (4) pursuing a narrow sectoral agreement as a first step.”<sup>14</sup> She provides that the 3<sup>rd</sup> and 4<sup>th</sup> options are better aligned to re-establish the US’s leadership in setting the trade policy agenda for the trans-Pacific region.<sup>15</sup> The third option’s approach to re-negotiate the CP-TPP will restore the US’s role in trade negotiations and allow it to leverage its market size as well as to push for more extensive revisions than accession would permit.<sup>16</sup> The fourth option provides that the US needs to engage bilaterally on an issue specific agreement, e.g., the US-Japan Digital Trade Agreement, as effective from January 1, 2020.<sup>17</sup>

In recent times, the US trade diplomacy has been inclined towards specific sectoral or bilateral issues, e.g., the US-EU large aircrafts dispute resolution,<sup>18</sup> the US-EU Trade and Technology Council,<sup>19</sup> or the recent review of the US-China phase I deal.<sup>20</sup> President Biden stated that the US intends to pursue the “Indo-Pacific Economic Framework (IPEF)”<sup>21</sup> as a novel means to strengthen ties with the Asia-Pacific region on key strategic issues individually, i.e., through defined modular economic pacts rather than an integrated FTA framework.<sup>22</sup> The new IPEF initiative is a response by the USTR to meet the current economic and geopolitical pressures by re-engaging and cooperating with the Asia-Pacific region on strategic areas.<sup>23</sup> One of the strategic areas of negotiations is “digital and emerging technologies-related issues.”<sup>24</sup> The US will host APEC 2023, and it will likely announce IPEF-related agreements during the final APEC ministerial conference.<sup>25</sup> While the IPEF is different from an all-encompassing and integrated FTA, it offers opportunities for both the US and Asia-Pacific region, especially in the field of digital trade. The study undertaken in this article will be informative for future deliberations on achieving regional and international regulatory cooperation on digital trade, especially in the context of a plausible US – Indo-Pacific Digital Economy Agreement (USIP DEA).

Alternatively, the RCEP, as concluded and signed on November 15, 2020, is a regional trade agreement between Australia, Brunei Darussalam, Cambodia, China, Indonesia, Japan, Korea, Lao PDR, Malaysia, Myanmar, New Zealand, Philippines, Singapore, Thailand,

---

<sup>14</sup> Wendy Cutler, *Reengaging the Asia-Pacific on Trade: A TPP Roadmap for the Next US Administration*, ASIA SOC’Y POL’Y INST. (2020), <https://asiasociety.org/sites/default/files/2020-09/A%20TPP%20Roadmap%20for%20the%20Next%20U.S.%20Administration.pdf>.

<sup>15</sup> *Id.*

<sup>16</sup> *Id.*

<sup>17</sup> *Id.*

<sup>18</sup> *EU and US take decisive step to end aircraft dispute*, EUR. COMM’N (June 15, 2021), [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_3001](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3001).

<sup>19</sup> *US-EU Trade and Technology Council (TTC)*, OFF. OF THE U.S. TRADE REP., <https://ustr.gov/useuttc>.

<sup>20</sup> Chad P. Bown, *Why Biden will try to enforce Trump’s phase one trade deal with China*, PIIE (Dec. 15, 2021), <https://www.piie.com/blogs/trade-and-investment-policy-watch/why-biden-will-try-enforce-trumps-phase-one-trade-deal-china>.

<sup>21</sup> Joint Statement from United States, Australia, Brunei Darussalam, India, Indonesia, Japan, Republic of Korea, Malaysia, New Zealand, Philippines, Singapore, Thailand, and Vietnam, Launch of the Indo-Pacific Economic Framework for Prosperity (IPEF) (2022) ([www.dfat.gov.au/news/media-release/launch-indo-pacific-economic-framework-prosperity-ipef-joint-statement](http://www.dfat.gov.au/news/media-release/launch-indo-pacific-economic-framework-prosperity-ipef-joint-statement)). See also Hiroyuki Tanaka & Hiroshi Tajima, *First in-person IPEF talks to be held in LA next week*, THE NATION THAI. (Sept. 2, 2022), <https://www.nationthailand.com/international/ann/40019678>.

<sup>22</sup> Eric C. Emerson, *The Indo-Pacific Economic Framework: How the United States intends to re-engage with Asia on Trade*, LEXOLOGY (Mar. 14, 2022), <https://www.lexology.com/library/detail.aspx?g=a51bed8f-9c38-46e3-9b9e-f24be6986999>.

<sup>23</sup> *Indo-Pacific Strategy of the United States*, WHITE HOUSE (2022), <https://www.whitehouse.gov/wp-content/uploads/2022/02/U.S.-Indo-Pacific-Strategy.pdf>.

<sup>24</sup> *Id.*

<sup>25</sup> *Id.*

Vietnam.<sup>26</sup> India withdrew before the conclusion of negotiations, citing the adverse impact of RCEP on sensitive sectors, especially agriculture and MSMEs.<sup>27</sup> However, India can join later without waiting 18 months for a new accession as per the protocol.<sup>28</sup> The Indian officials have hinted that India will not join the agreement as it currently stands.<sup>29</sup>

The RCEP encompasses a population of around 2.3 billion people, making up 30% of the world's population with a total GDP of \$38,813 billion or 30% of the global GDP.<sup>30</sup> As we can note in figure 1, there is common membership among certain countries in both the CP-TPP and RCEP. Australia, Brunei Darussalam, Japan, Malaysia, New Zealand, Singapore, and Vietnam being parties to both of the RTAs. It doubles the benefit for them with access to both the North America and Asia-Pacific economic region.<sup>31</sup> In economic terms, the RCEP has a larger market share than CP-TPP given the membership base, so the trade liberalization impact of RCEP will be more widespread than CP-TPP.<sup>32</sup> However, in light of new applications to join CP-TPP by the UK, China, Taiwan, and South Korea, the economic impact of CP-TPP and RCEP is now relatively at par.

**Table 1: State parties to the CP-TPP vs. RCEP**

CP-TPP		RCEP	
1.	Australia	1.	Australia
2.	Brunei Darussalam	2.	Brunei Darussalam
3.	Japan	3.	Japan
4.	Malaysia	4.	Malaysia
5.	New Zealand	5.	New Zealand
6.	Singapore	6.	Singapore
7.	Vietnam	7.	Vietnam
8.	Canada	8.	Cambodia
9.	Chile	9.	China
10.	Mexico	10.	Indonesia <sup>33</sup>
11.	Peru	11.	Korea

<sup>26</sup> *Regional Comprehensive Economic Partnership (RCEP)*, AUSTL. GOV'T. DEP'T OF FOREIGN AFF. AND TRADE, <https://www.dfat.gov.au/trade/agreements/in-force/rcep>.

<sup>27</sup> *Regional Comprehensive Economic Partnership: Overview and Economic Impact*, ADB BRIEFS No. 164 (2020), <https://www.adb.org/sites/default/files/publication/664096/adb-brief-164-regional-comprehensive-economic-partnership.pdf>.

<sup>28</sup> *Id.*

<sup>29</sup> Suhasini Haidar, *India storms out of RCEP, says trade deal hurt Indian farmers*, THE HINDU (Dec. 3, 2021), <https://www.thehindu.com/news/national/india-decides-against-joining-rcep-trade-deal/article29880220.ece>. See also Piyush Goyal, Minister of Commerce & Industry, "Personally, entering the RCEP would have been the death knell for Indian manufacturing and other sectors. RCEP was a free trade agreement with China. On 4<sup>th</sup> November 2019, PM Modi declined to join the RCEP because it does not meet the principles on which it was first conceptualised. We already have a free trade agreement with all the ASEAN countries, with Japan and Korea, so 12 countries are covered. Today, Australia gets covered."

<sup>30</sup> *Id.*

<sup>31</sup> Frank Ko-Ho Wong, *What the CPTPP and RCEP Mean for China and Asia-Pacific Trade*, CHINA BRIEFING (Dec. 10, 2018), <https://www.china-briefing.com/news/cptpp-rcep-impact-china-asia-pacific-trade/>.

<sup>32</sup> Kate Whiting, *An expert explains: What is RCEP, the world's biggest trade deal?*, WORLD ECON. FORUM (May 18, 2021), <https://www.weforum.org/agenda/2021/05/rcep-world-biggest-trade-deal/>.

<sup>33</sup> Sebastian Strangio, *Indonesian Parliament Ratifies RCEP Free Trade Mega-Pact*, THE DIPLOMAT (Aug. 31, 2022), <https://thediplomat.com/2022/08/indonesian-parliament-ratifies-rcep-free-trade-mega-pact/> ("Indonesia's parliament passed a law formalizing the country's membership of the Regional Comprehensive Economic Partnership (RCEP) trade pact.").

12. UK (formally applied to join on February 1, 2021) <sup>34</sup>	12. Lao PDR
13. China (formally applied to join on September 16, 2021) <sup>35</sup>	13. Myanmar
14. Taiwan (formally applied to join on September 22, 2021) <sup>36</sup>	14. Philippines
15. South Korea (actively and seriously considering joining as per reports on October 8, 2021) <sup>37</sup>	15. Thailand
16. Ecuador (applied to join on December 17, 2021) <sup>38</sup>	16. India (dropped-out in November 4, 2019 before the conclusion citing the RCEP's economic impact on Indian farmers MSMEs and the dairy sector. India can join again without waiting for 18 months as required for accessions per the protocol). <sup>39</sup> The Indian government has hinted that it will not join the agreement as it currently stands. <sup>40</sup>
17. Costa Rica (formally applied to join the CP-TPP on August 11, 2022 as per reports) <sup>41</sup>	17. Hong Kong <sup>42</sup>
18. Guatemala (expressed interest to join the CP-TPP) <sup>43</sup>	

**Source:** Australian Government, Department of Foreign Affairs and Trade (DFAT), 'About Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CP-TPP)', <https://www.dfat.gov.au/trade/agreements/in-force/cptpp/comprehensive-and-progressive-agreement-for-trans-pacific-partnership>; 'About the Regional Comprehensive Economic Partnership Agreement (RCEP)', <https://www.dfat.gov.au/trade/agreements/not-yet-in-force/rcep>.

<sup>34</sup> Chris Smith, *In Focus: UK membership of the trans-Pacific trade agreement*, UK PARLIAMENT, HOUSE OF LORDS LIBRARY (Jan. 26 2022), <https://lordslibrary.parliament.uk/uk-membership-of-the-trans-pacific-trade-agreement/#:~:text=On%201%20February%202021%2C%20the,objectives%20for%20the%20accession%20negotiations>.

<sup>35</sup> Mireya Solis, *Order from Chaos: China moves to join the CPTPP, but don't expect a fast pass*, BROOKINGS (Sept. 23, 2021), <https://www.brookings.edu/blog/order-from-chaos/2021/09/23/china-moves-to-join-the-cptpp-but-dont-expect-a-fast-pass/>.

<sup>36</sup> Bernie Lai, *Taiwan's bid to join the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)*, PARLIAMENT OF AUSTL. (Dec. 20 2021), [https://www.aph.gov.au/About\\_Parliament/Parliamentary\\_Departments/Parliamentary\\_Library/FlagPost/2021/December/Taiwan\\_CPTPP\\_bid#:~:text=Taiwan's%20bid%20to%20join%20the,Trans%2DPacific%20Partnership%20\(CPTPP\)&text=On%2022%20September%202021%2C%20Taiwan,CPTPP\)%20following%20years%20of%20preparation](https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/FlagPost/2021/December/Taiwan_CPTPP_bid#:~:text=Taiwan's%20bid%20to%20join%20the,Trans%2DPacific%20Partnership%20(CPTPP)&text=On%2022%20September%202021%2C%20Taiwan,CPTPP)%20following%20years%20of%20preparation).

<sup>37</sup> Jeffrey J. Schott, *Policy Brief: China's CPTPP bid spurs South Korea to act on Asia-Pacific trade pacts*, PIIIE (June 2022), <https://www.piiie.com/publications/policy-briefs/chinas-cptpp-bid-spurs-south-korea-act-asia-pacific-trade-pacts>.

<sup>38</sup> Hidetake Miyamoto, *Ecuador applied for CPTPP membership to diversify trade*, NIKKEI ASIA (Dec. 29, 2021), <https://asia.nikkei.com/Economy/Trade/Ecuador-applies-for-CPTPP-membership-to-diversify-trade2>.

<sup>39</sup> Suhasini Haider & T.C.A Sharad Raghavan, *India storms out of RCEP, says trade deal hurts India farmers*, THE HINDU (Dec. 3, 2021), <https://www.thehindu.com/news/national/india-decides-against-joining-rcep-trade-deal/article61623346.ece>.

<sup>40</sup> Surupa Gupta & Sumit Ganguly, *Why India Refused to Join the World's Biggest Trading Bloc: New Delhi chose protectionism over the RCEP. History suggests it made the wrong call*, FOREIGN POLICY (Nov. 23, 2020), <https://foreignpolicy.com/2020/11/23/why-india-refused-to-join-rcep-worlds-biggest-trading-bloc/>.

<sup>41</sup> *Eyes on Asia: Costa Rica finalizes petition to join CPTPP*, WORLD TRADE ONLINE (Aug. 11, 2022), <https://insidetrade.com/trade/eyes-asia-costa-rica-finalizes-petition-joincptpp#:~:text=Costa%20Rica%20has%20formally%20applied,announced%20the%20move%20on%20Wednesday>.

<sup>42</sup> *Belt and Road Summit: Hong Kong seeks early accession to RCEP*, ZAWYA (Sept. 1, 2022), <https://www.zawya.com/en/projects/bri/belt-and-road-summit-hong-kong-seeks-early-accession-to-rcep-etdasto5>.

<sup>43</sup> Deborah Elms, *Asia Trade: What's in store for Asia-Pacific Trade Agreements in 2023*, BORDERLEX (Jan. 18, 2023), <https://borderlex.net/2023/01/18/asia-trade-whats-in-store-for-asia-pacific-trade-agreements-in-2023/>.

The WTO discussions on digital trade began in May 1998 with the Second Ministerial Conference in Geneva, whereby the ministers adopted the Declaration on Global Electronic Commerce, initiating a comprehensive work program to examine the “trade-related issues on global electronic commerce”.<sup>44</sup> The Declaration stated that the work program will involve all the relevant WTO bodies, taking into account the economic, financial, and developmental needs of countries as well as recognizing the work undertaken in other international forums.<sup>45</sup> In MC11 2017, a group of countries proposed to convert the work program with a new ministerial declaration into negotiations without any success.<sup>46</sup> Failure to pursue their negotiating agenda within the multilateral context led the group of WTO members to opt for alternate ways.<sup>47</sup> The alternate ways to approach the issue led to the Joint Statement Initiative on e-commerce (eJSI) in 2017, as presented by seventy-one WTO members representing 77% of global trade.<sup>48</sup> The eJSI stated that the participating WTO members aim to initiate “exploratory work toward building foundations for future WTO negotiations on trade-related aspects of digital trade, open to all WTO members without prejudice to their negotiating stance in the future.”<sup>49</sup>

The eJSI is one of the four open-ended plurilateral initiatives, wherein the other three covered issues are investment facilitation, MSMEs, and service domestic regulation.<sup>50</sup> Subsequently, at the 11th Ministerial Conference in Buenos Aires on December 13, 2017, seventy-one WTO Members confirmed their intention to initiate exploratory work towards the WTO negotiations on trade-related aspects of e-commerce.<sup>51</sup> Consequently, seventy-six WTO member states issued a joint statement in Davos on January 5, 2019, promulgating their intention to begin the exploratory negotiations on digital trade.<sup>52</sup>

The current eJSI has eighty-eight participating member states.<sup>53</sup> These negotiations are being undertaken outside the ambit of the WTO legal framework.<sup>54</sup> These are exploratory digital trade negotiations, which may become part of the WTO legal framework as either a plurilateral agreement or as a supplement to the GATS schedules of the participating WTO member states.<sup>55</sup> The current eJSI draft text is a stocktaking exercise, as it has square brackets throughout the text that represent areas of no agreement —specifically areas like privacy, cybersecurity, and other regulatory issues.<sup>56</sup> Future negotiations aim to enable alliances of like-minded member states on key regulatory issues, even though the actual conclusion of an

---

<sup>44</sup> *Declaration on Global Electronic Commerce*, WORLD TRADE ORG. DOC. W/L/274 (1998), <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/L/274.pdf&Open=True>.

<sup>45</sup> *What is at stake...*, *supra* note 2; see also Michael Kende & Nivedita Sen, *Cross-border e-commerce: WTO discussions and multi-stakeholder roles – stocktaking and practical ways forward*, GENEVA GRADUATE INS. Working Paper CTEI-2019-01 (2019), <https://repository.graduateinstitute.ch/record/297080?ln=en>; Yasmin Ismail, *E-commerce joint Statement Initiative Negotiations Among World Trade Organization Members: State of Play and the impacts of COVID-19*, INT’L INST. FOR SUSTAINABLE DEV. (April 29, 2021), <https://www.iisd.org/system/files/2021-06/e-commerce-negotiations-wto-members-covid-19-en.pdf>.

<sup>46</sup> *Id.*

<sup>47</sup> *Id.*

<sup>48</sup> *Id.*

<sup>49</sup> *Id.*

<sup>50</sup> *Id.*

<sup>51</sup> *What is at stake...*, *supra* note 2; see also Kende & Sen, *supra* note 45; Ismail, *supra* note 45.

<sup>52</sup> *Id.*

<sup>53</sup> *Id.*; see, e.g., *E-commerce negotiations enter final lap, Kyrgyz Republic joins initiative*, WTO (Feb. 16, 2023), [https://www.wto.org/english/news\\_e/news23\\_e/ecom\\_17feb23\\_e.htm](https://www.wto.org/english/news_e/news23_e/ecom_17feb23_e.htm).

<sup>54</sup> UNCTAD, *supra* note 45.

<sup>55</sup> *Id.*

<sup>56</sup> *Id.*



agreement, and its insertion into the WTO legal framework, may take a long time in part due to the consensus principle.<sup>57</sup>

A group of countries led by India and South Africa have persistently expressed objections against the eJSI plurilateral negotiations specifically on digital trade outside the multilateral context.<sup>58</sup> They emphasize that such plurilateral negotiations can lead to the marginalization or exclusion of other difficult trade-related issues that remain critical for the future of WTO negotiations, especially on agriculture and development.<sup>59</sup> They provide that plurilateral negotiations undermine the political and economic balance in agenda setting, negotiation processes, and outcomes within the multilateral trade forum to the detriment of developing and least-developed countries (LDCs).<sup>60</sup>

Jane Kelsey discusses the challenges of JSIs, as raised by India and South Africa vis-à-vis the eJSI.<sup>61</sup> Kelsey argues that, although the main aim of eJSI is “restoring the functionality of the WTO negotiating arm,”:

. . . it risks triggering an almost irresolvable internal fracturing of its Members.<sup>62</sup> Developing countries that rely on issue linkage to secure some concessions from economically and geopolitically more powerful states will be disenfranchised.<sup>63</sup> Already marginalized developing and least-developed countries will become even more so.<sup>64</sup> With no obvious limit to what might be done in the name of ‘open plurilateralism’, the rule takers will lose any effective voice at the WTO.<sup>65</sup>

There is no simple answer to the dilemma of “plurilateralism” versus “consensus-based multilateralism.” Plurilateralism reinforces multilateralism and vice versa. The WTO Member states, especially the developing and LDCs, should consider the opportunities that the eJSI negotiations offer in terms of a global regulatory understanding on e-commerce. Further, they should weigh the pros and cons of a plurilateral e-commerce agreement “within versus outside” the WTO.

## II. GENERAL CLASSIFICATION OF DIGITAL TRADE PROVISIONS

We classify all the digital trade provisions in CP-TPP,<sup>66</sup> RCEP,<sup>67</sup> and eJSI<sup>68</sup> into three regulatory themes. These regulatory themes are classified as: (a) market access (tariff-related measures); (b) regulatory (non-tariff-related measures); and (c) cooperation, development, and

---

<sup>57</sup> *Id.*

<sup>58</sup> *Id.*

<sup>59</sup> *Id.*

<sup>60</sup> UNCTAD, *supra* note 45.

<sup>61</sup> Jane Kelsey, *The Illegitimacy of Joint Statement Initiatives and Their Systematic Implications for the WTO*, 25 J. INTL. ECON. L. 11 (2022), <https://academic.oup.com/jiel/article/25/1/2/6533600?login=false>.

<sup>62</sup> *Id.*

<sup>63</sup> *Id.*

<sup>64</sup> *Id.*

<sup>65</sup> *Id.*

<sup>66</sup> THE COMPREHENSIVE AND PROGRESSIVE AGREEMENT FOR TRANS-PACIFIC PARTNERSHIP (CP-TPP) (2018), <https://www.dfat.gov.au/trade/agreements/in-force/cptpp/official-documents>.

<sup>67</sup> THE REGIONAL COMPREHENSIVE ECONOMIC PARTNERSHIP (RCEP) (2020), <https://www.dfat.gov.au/trade/agreements/in-force/rcep/rcep-text>.

<sup>68</sup> WTO ELEC. COMM. NEGOT.: CONSOLIDATED NEGOTIATING TEXT – DECEMBER 2020 (eJSI) (2020), [https://www.bilaterals.org/IMG/pdf/wto\\_plurilateral\\_ecommerce\\_draft\\_consolidated\\_text.pdf](https://www.bilaterals.org/IMG/pdf/wto_plurilateral_ecommerce_draft_consolidated_text.pdf).

facilitation measures. These three regulatory themes encapsulates all the digital trade provisions. This classification is equally applicable to other digital trade agreements.

**Table 2: General classification of digital trade provisions**

S.NO.	GENERAL CLASSIFICATION OF DIGITAL TRADE PROVISIONS	CP-TPP	RCEP	eJSI
<b>1.</b>	<b>MARKET ACCESS (TARIFF-RELATED MEASURES)</b>			
1.1.	Customs Duties	◦	◦	◦
1.2.	Goods Market Access			◦
1.3.	Services Market Access			◦
1.4.	Taxation			◦
1.5.	Temporary Entry and Sojourn of Electronic Commerce-related Personnel			◦
<b>2.</b>	<b>REGULATIONS (NON-TARIFF-RELATED MEASURES)</b>			
2.1.	Unsolicited Commercial Electronic Messages	◦	◦	◦
2.2.	Competition			◦
2.3.	Cross-Border Transfer of Information by Electronic Means	◦	◦	◦
2.4.	Cybersecurity	◦	◦	◦
2.5.	Domestic Electronic Transactions Framework	◦	◦	◦
2.6.	General & Security Exceptions	◦	◦	◦
2.7.	ICT Products that use Cryptography			◦
2.8.	Location of Computing Facilities	◦	◦	◦
2.9.	Location of Financial Computing Facilities for Covered Financial Service Suppliers			◦
2.10.	Non-Discriminatory Treatment of Digital Products	◦		◦
2.11.	Online Consumer Protection	◦	◦	◦
2.12.	Personal Information Protection	◦	◦	◦
2.13.	Principles on Access to and Use of the Internet for Electronic Commerce	◦		◦
2.14.	Prudential Measures			◦
2.15.	Source Code	◦		◦
2.16.	Updating the WTO Reference Paper on Telecommunications Services			◦
<b>3.</b>	<b>COOPERATION, DEVELOPMENT &amp; FACILITATION MEASURES</b>			
3.1.	Access to and Use of Interactive Computer Services			◦
3.2.	Access to Government Data			◦
3.3.	Capacity-Building and Technical Assistance			◦
3.4.	Committee on Trade-related aspects of Electronic Commerce			◦
3.5.	Customs Procedures			◦
3.6.	De Minimis			◦
3.7.	Electronic Authentication and Signature	◦	◦	◦
3.8.	Electronic Availability of Trade-related Information			◦
3.9.	Electronic Contracts			◦
3.10.	Electronic Invoicing			◦
3.11.	Electronic Payments Service			◦
3.12.	Enhanced Trade Facilitation			◦
3.13.	Improvements to Trade Policies			◦
3.14.	Interactive Computer Services (Infringement)			◦
3.15.	Interactive Computer Services (Limiting Liability)			◦
3.16.	Internet Interconnection Charge-Sharing	◦		
3.17.	Logistics Services			◦
3.18.	Paperless Trading			◦
3.19.	Provision of Trade Facilitating and Supportive Services	◦	◦	◦
3.20.	Single Windows Data Exchange and System Interoperability			◦
3.21.	Transparency, Cooperation and Dialogue	◦	◦	◦
3.22.	Use of Technology for the Release and Clearance of Goods			◦

**Source:** *See supra* notes 66-68 and accompanying text.

Future trade agreements should have the same three classification measures for digital trade provisions to streamline the discussions among stakeholders.

### III. COMPARATIVE REGULATORY APPROACHES FOR DIGITAL TRADE REGULATION IN CP-TPP, RCEP, AND EJSI

The main purpose behind digital trade regulation is to manage the cross-border data flows under a common legal framework for trade-led economic development. Digital trade regulations govern three main layers of digital communications: (a) the physical layer (network plus the hardware attached); (b) the logical layer (software, applications, and protocols); and (c) the content layer (actual human-readable content).<sup>69</sup> Whilst exponential economic digitalization blurs the boundaries between regulating economy or society, the digital trade regulations need to be anticipatory in nature.

In the following sections, the article provides a comparative analysis of fundamental digital trade provisions in the CP-TPP, RCEP, and eJSI.

#### A. INTRODUCTORY PROVISIONS

The scope of digital trade provisions in the CP-TPP, RCEP, and eJSI are legally defined through a specific list of applicable legal definitions, exclusions, and country-specific annexes listing certain measures or activities that are excluded from specific obligations in certain chapters, also known as non-conforming measures. In the legal interpretation of any particular provision within a digital trade agreement, we need to appreciate the applicable legal scope and preamble as relevant legal context.

##### A.I. PREAMBLE

The three trade agreements relevant to our analysis, CP-TPP, RCEP, and eJSI, consist of preambles that outline specific larger goals and objectives behind the agreement. There are various goals mentioned in the preambles, highlighting issues of pertinent interest to the parties. However, instead of reading them individually, when we take a step back it is apparent that the list of goals or objectives are designed to essentially balance specific economic and non-economic objectives. Although the nature of trade agreements is primarily to achieve certain basic economic objectives, they cannot and do not function in isolation from impending socio-political and economic challenges nationally and globally. This realization has led to an emphasis on achieving “deep trade agreements,” which encompasses separate chapters on sustainable development goals relevant to trade policy, e.g., the US and the EU’s trade agreement chapters on trade and sustainable development.<sup>70</sup>

Generally, the principal economic objectives of trade agreements are, according to the CP-TPP, RCEP, and eJSI: economic integration, growth and all the social benefits that it brings

---

<sup>69</sup> MIRA BURRI, UNDERSTANDING AND SHAPING TRADE RULES FOR THE DIGITAL ERA in THE SHIFTING LANDSCAPE OF GLOBAL TRADE GOVERNANCE Ch. 4, 73-106 (Manfred Elsig, Michael Hahn, and Gabriele Spilker eds., Cambridge Univ. Press 2019).

<sup>70</sup> Vandana Gyanchandani, *Soft vs Hard Governance for Labour and Environmental Commitments in Trade Agreements: Comparing the US and EU Approaches*, CTEI WORKING PAPERS (Aug. 1 2018), <https://ssrn.com/abstract=3324950>.

forth, e.g., decline in poverty, support to MSMEs, improved living standards, ensured employment or business opportunities, as well as more diverse choices for consumers.<sup>71</sup> Non-economic values, as highlighted by the preambles, include appropriate regulatory autonomy to set national legislative or regulatory priorities in areas such as environment, conservation of living and non-living exhaustible natural resources, and the integrity of financial systems and public morals. Non-economic values also include transparency, good governance, eliminating corruption, and promoting cultural diversity and identity.<sup>72</sup>

Specifically, the digital trade chapters in CP-TPP, RCEP, and eJSI provide dedicated preambular objectives.<sup>73</sup> They categorically list three preambular objectives for digital trade: (1) to promote economic growth and development through digital trade opportunities, (2) ensure regulatory frameworks that provide for consumer confidence in digital trade, and (3) assist in avoiding unnecessary and disguised barriers to its use and development.<sup>74</sup>

The RCEP additionally provides that the digital trade chapter aims to “enhance cooperation among the Parties regarding development of digital trade.”<sup>75</sup> The eJSI uniquely adds that digital trade can be used as a tool for social and economic development.<sup>76</sup> In pursuance, the member states emphasize on promoting: “(a) clarity, transparency, and predictability of their domestic regulatory framework in facilitating to the maximum extent possible the development of digital trade; (b) interoperability, innovation and competition and (c) increased participation in digital trade by MSMEs.”<sup>77</sup> Lastly, it is only the eJSI that highlights the importance of open and free internet for all legitimate, commercial, and development purposes including “by allowing increased access to information, knowledge and new technologies.”<sup>78</sup>

Below, we highlight the main economic and non-economic objectives of digital trade agreements which will be useful for future research.<sup>79</sup>

**Table 3: Preambular economic and non-economic objectives for digital trade**

Preambular Objectives	
Economic Objectives	
1.	Economic integration, growth, and development
2.	Increased trade opportunities
3.	Development of digital trade
4.	Consumer confidence
5.	Interoperability
6.	Innovation
7.	Competition
8.	Increased participation by MSMEs

<sup>71</sup> See Comprehensive and Progressive Agreement for Trans-Pacific Partnership [hereinafter CP-TPP] preamble, Dec. 30, 2018; Regional Comprehensive Economic Partnership Agreement [hereinafter RCEP] preamble, Jan. 1, 2022; WTO Electronic Commerce Negotiations Stocktake Text [hereinafter eJSI] preamble, Aug. 19, 2020.

<sup>72</sup> *Id.*

<sup>73</sup> *Id.*

<sup>74</sup> *Id.*

<sup>75</sup> *Id.*

<sup>76</sup> *Id.*

<sup>77</sup> See CP-TPP, *supra* note 71; RCEP, *supra* note 71; eJSI *supra* note 71.

<sup>78</sup> *Id.*

<sup>79</sup> *Id.*

Non-Economic Objectives	
1.	Reasonably open internet
2.	Necessary regulatory autonomy
3.	Transparency
4.	Good governance
5.	Eliminating corruption
6.	Cultural diversity and identity
7.	Inclusive socio-economic development

**Source:** Collection from the legal texts by authors.

Generally, the CP-TPP has an extensive set of preambular objectives promoting a broader set of economic and non-economic values as relevant legal context.<sup>80</sup> The RCEP has a moderate set of objectives as compared to CP-TPP.<sup>81</sup> The eJSI, which is very specific to digital trade and does not delve into any other issue, has a set of targeted objectives for the digital trade liberalization.<sup>82</sup> Although not very elaborate, it is wise to underline the relevance of preambular recitals in GATT 1994 and GATS in order to appreciate the larger economic and non-economic objectives of trade liberalization in general.<sup>83</sup>

Here we list the general preambular objectives of the CP-TPP vs. RCEP to decipher central comparative preambular trade values:

**Table 4: Preambular goals - CP-TPP vs. RCEP**

PREAMBULAR GOALS	CP-TPP	RCEP
1. Raise living standards	°	°
2. Account for different levels of economic development	°	°
3. Special and Differential Treatment		°
4. Build upon rights and obligations as provided in the WTO's Marrakesh Agreement	°	°
5. Right to regulate to secure public welfare objectives	°	°
6. Good governance	°	°
7. Legal stability and predictability of business environment	°	°
8. Sustainable development goals	°	°
9. Promote bonds of friendship and cooperation among people	°	
10. Promote participation in regional and global supply chains	°	°
11. Promote competition	°	
12. Development of MSMEs	°	
13. Efficient and effective customs to enable seamless trade	°	
14. Inherent right to regulate health care system	°	
15. Establish rules for SOEs to ensure fair and level playing field in trade	°	
16. High levels of environmental protection	°	
17. Promote enforcement of labour rights	°	
18. Promote rule of law	°	
19. Eliminate corruption and bribery	°	
20. Recognise relevant macroeconomic regulatory decisions	°	
21. Promote cultural diversity and identity	°	
22. Contribute to broader cooperation at the regional and global level	°	°
23. Address future trade and investment regulatory concerns	°	
24. Promote state accession to build a foundation for future FTA in the Asia-Pacific	°	

**Source:** Segregation from the original texts by authors.

Future digital trade agreements should provide for broad socioeconomic goals which are related to digital economy. It is a positive development that the preambular recitals outlined in

<sup>80</sup> *Id.*

<sup>81</sup> *Id.*

<sup>82</sup> *Id.*

<sup>83</sup> See CP-TPP, *supra* note 71; RCEP, *supra* note 71; eJSI *supra* note 71.

this article have broad coverage of socioeconomic goals, especially in the CP-TPP. The preambular recitals in trade agreements should specifically express support for the development of indigenous data governance issues. It should aim to build effective cooperation mechanism to support the vulnerable communities affected by digital trade as this will ensure that the policymaking is inclusive given the extreme polarities between winners and losers in the context of digital trade.

## A.II. DEFINITIONS

### A.II.1. DEFINITION OF “DIGITAL TRADE OR E-COMMERCE”

The eJSI defines “digital trade or e-commerce” as “the production, distribution, marketing, sale or delivery of goods and services by electronic means.”<sup>84</sup> However, the CP-TPP and RCEP do not provide any definition of digital trade or e-commerce. The CP-TPP, RCEP, and eJSI provide that the digital trade or e-commerce chapter “shall apply to measures adopted or maintained by a Party” that affects trade by “electronic means” (CP-TPP and eJSI) or “electronic commerce” (RCEP).<sup>85</sup> We note that the definition of “digital trade or e-commerce” as provided by the eJSI is specific and detailed. The definition of “digital trade or e-commerce” is a critical provision as it weighs in on the scope of e-commerce or digital trade activities covered in a trade agreement. The definition provided by the eJSI is specific as it includes digital activities encompassing “production, distribution, marketing, sale or delivery” of goods and services as compared to simply “trade by electronic means” in the CP-TPP and RCEP.

The definition of “digital trade or e-commerce” should be given careful thought in trade negotiations because digital trade goes beyond traditional trade in many ways.<sup>86</sup> Digital trade regulates “cross-border data flows including personal data” that create and enable different forms of goods and services which are seamlessly produced, distributed, and delivered in many innovative ways than conventionally understood.<sup>87</sup> For example, technology-enabled instrument that allows for a virtual or augmented reality experience to access education, work, or entertainment services in a digital space at any place and time.<sup>88</sup> The amalgamation of experiences as derived from digitally-delivered goods and services within a given time or space highlights the complexity of defining “e-commerce or digital trade” in trade agreements. In this regard, the specific definition as proposed by the eJSI is more supportive of this complexity than the general and vague definition in the CP-TPP and RCEP.

Lack of a specific definition of “e-commerce or digital trade” can lead to an erroneous assumption that any economic activity in an electronic form will be covered by the digital trade agreement. This erroneous assumption is detrimental to support future accessions by developing and least-developed countries who are already hesitant to liberalize their digital economies.

---

<sup>84</sup> eJSI, *supra* 68, at Annex 1: Scope and General Provisions.

<sup>85</sup> RCEP Agreement, Chapter 12: Electronic Commerce, Article 12.3: Scope, AUSTL. GOV'T DEP'T OF FOREIGN AFF. AND TRADE, <https://www.dfat.gov.au/sites/default/files/rcep-chapter-12.pdf>.

<sup>86</sup> *The impact of digitalisation on trade*, OECD, <https://www.oecd.org/trade/topics/digital-trade/>.

<sup>87</sup> *Id.*

<sup>88</sup> *Previous Global Future Council on Augmented Reality and Virtual Reality*, WORLD ECON. FORUM, <https://www.weforum.org/communities/gfc-on-virtual-reality-and-augmented-reality>.

### A.II.2. DEFINITION OF “DIGITAL PRODUCT”

Both the CP-TPP and eJSI define “digital product” as “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.”<sup>89</sup> Both the CP-TPP and eJSI clarify that the digital product does not include a “digitized representative of a financial instrument including money.”<sup>90</sup> Further, it provides that the definition of digital product should not reflect any Party’s view on whether trade in digital products should be categorized as trade in services or goods.<sup>91</sup> No such definition of digital product is provided by the RCEP. The lack of definition of digital product in the RCEP leaves it open to diverse interpretation by parties or adjudicatory panels on a case-by-case basis.

The definition of digital product is pertinent to decipher the specific legal scope of the digital trade obligations. The definition provided by the CP-TPP and eJSI covers various forms of digital goods and services that are or can be enabled through the cross-border data flows. The lack of specific definition of digital products in RCEP leaves it open to legal interpretation by the parties as to whether the new forms of digital goods or services are foreseen or covered by the agreement or not. As discussed previously, there are new forms of digital experiences enabled by future technologies that challenge one’s previous understanding of goods vs. services at any given time and space. Any erroneous assumption that the scope of digital trade chapter is either too broad or narrow due to lack of a clear definition of digital products will be counter-effective to the viability of such agreements for future accessions by developing or least-developed countries. There needs to be sustained deliberations on the definition of digital products to make it relevant in the evolving context of digital trade.

### A.II.3. DEFINITION OF “COVERED PERSONS”

The CP-TPP and RCEP specifically provide that the digital trade obligations apply to select “covered persons” only: “covered investment,” “investor of a Party,” and “service supplier”.<sup>92</sup> The CP-TPP, RCEP, and eJSI exclude “financial institutions, financial service suppliers or investors from any e-commerce obligations.”<sup>93</sup>

The CP-TPP, RCEP, and eJSI further specifically exclude “government procurement.”<sup>94</sup> The eJSI provides that government procurement includes “service supplied in the exercise of governmental authority.”<sup>95</sup> The CP-TPP, RCEP, and eJSI elaborate that the exclusion of government procurement encompasses “information held or processed by or on behalf of a Party, or measures related to such information, including measures related to its collection.”<sup>96</sup> However, it is only the eJSI that clarifies that there are general obligations pertaining to the protection of personal information which applies to any government activity in the digital trade sector.<sup>97</sup>

---

<sup>89</sup> CP-TPP, *supra* note 66.

<sup>90</sup> *Id.*

<sup>91</sup> *Id.*

<sup>92</sup> CP-TPP, *supra* note 71, at art. 14.1: Definitions. RCEP, *supra* note 71, at art. 12.1: Definitions. eJSI, *supra* note 71, at B.2.: Flow of Information by electronic means/Cross-border data flows.

<sup>93</sup> *Id.*

<sup>94</sup> *Id.*

<sup>95</sup> *Id.*

<sup>96</sup> *Id.*

<sup>97</sup> *Id.*

The practical application of government procurement provision, specifically in the context of third-party involvements, will depend on the facts of a given case. We need to be careful to not emphasize on too broad or too narrow scenarios and appreciate that the correct legal application will fall somewhere in between the two extremes. Although it is hard to pinpoint the precise application of the exclusion in abstract, we should be guided by indicia such as whether the Party would ordinarily have access to the information being processed or held by a private entity, whether the processing or holding of the information is in pursuit of a public purpose, and whether the nature of the information is such that it would ordinarily be processed and held by the private entity.

We propose that the negotiators pay special attention in defining the concepts “digital trade or e-commerce”, “digital products”, and “covered persons” to design the legal scope of digital trade chapters. These concepts help delineate the legal scope and application of digital trade obligations. A clear definition of such concepts will generate requisite support for developing and least-developed countries as regards future accessions to these agreements. We submit that a general or ambiguous definition leaves the interpretation of legal scope or applicability to a trade panel. It is not the most effective way to promote legal predictability as it only induces legal speculation than a firm common understanding. Specifically we note that, given the increasingly blurred distinction between goods vs. services with the rise of new digital technologies, for example Metaverse,<sup>98</sup> it is wise to define “digital products” in digital trade agreements by being thoughtful about the nature of evolving digital technologies at play. It is practical to ensure an active discussion forum within digital trade agreements to regularly assess and debate key technological developments affecting digital trade and update the relevant definitions accordingly.

#### A.II.4. CO-APPLICATION

The CP-TPP and RCEP emphasize on a harmonious co-existence between the obligations of each respective agreement and any other multilateral or regional trade agreement involving at least two member states being party to the same agreement.<sup>99</sup> It provides that in the case of a conflict between any obligation under either the CP-TPP or RCEP and a multilateral or regional trade agreement, the parties upon request should aim to resolve the conflict with a mutually satisfactory solution.<sup>100</sup> The RCEP further provides that if the parties reach an agreement resulting in a more favorable treatment than that provided for under the RCEP, it is not an inconsistency.<sup>101</sup>

---

<sup>98</sup> “The metaverse is an integrated network of 3D virtual worlds. ... This is the popular conception of the metaverse: a VR-based world independent of our physical one where people can socialize and engage in a seemingly unlimited variety of virtual experiences, all supported with its own digital economy. ... To see the metaverse in action, we can look at popular massively multiplayer virtual reality games such as Rec Room or Horizon Worlds, where participants use avatars to interact with each other and manipulate their environment. But the wider applications beyond gaming are staggering. Musicians and entertainment labels are experimenting with hosting concerts in the metaverse. The sports industry is following suit, with top franchises like Manchester City building virtual stadiums so fans can watch games and, presumably purchase virtual merchandise. Perhaps the farthest-reaching opportunities for the metaverse will be in online learning and government services.” Adrian Ma, *What is the metaverse, and what can we do there?*, THE CONVERSATION (May 23 2022, 8:23 AM), <https://theconversation.com/what-is-the-metaverse-and-what-can-we-do-there-179200>.

<sup>99</sup> CP-TPP, *supra* note 66; RCEP CHAPTER 20: FINAL PROVISIONS, *supra* note 67; EJSI, *supra* note 68.

<sup>100</sup> *Id.*

<sup>101</sup> *Id.*



The eJSI provides that the plurilateral digital trade agreement under annexes 1a–1c of the WTO agreement builds on the existing WTO legal framework. Wherever there is a conflict between the plurilateral agreement and the provisions of agreements under annex 1 of the Marrakesh Agreement, the latter shall prevail.<sup>102</sup> The eJSI lays out commonly shared principles and values for digital trade.<sup>103</sup> The RCEP also provides specific guiding objectives for the digital trade chapter.<sup>104</sup> No such provision is found in the CP-TPP.<sup>105</sup>

Specifically, the CP-TPP and RCEP provide for the co-application of obligations under the chapter on investment, trade in services, and financial services. This includes any specific exceptions or non-conforming measures applicable to services which are delivered or performed electronically.<sup>106</sup> The eJSI provides that “nothing in the agreement should be construed to diminish the rights and obligations under the agreements in annex 1 to the Marrakesh Agreement establishing the WTO. If there is any inconsistency between the eJSI and the agreements in annex 1, then the latter shall prevail.”<sup>107</sup>

The underlying rationale for co-applicability is to promote a harmonious co-existence of all trade-related regulatory provisions, as well as to ensure that the underlying WTO framework is complemented with new plurilateral agreements on digital trade.<sup>108</sup> However, such co-application can promote harmonious co-existence and raise new interpretative conflicts.<sup>109</sup> Thus, it will become necessary to establish a common understanding among different regulatory agreements—as they aim to govern digital trade activities in different contexts—in order to avoid divergent practices, enforcement, or outcomes.<sup>110</sup> For example, a legitimate public policy which is protected by the digital trade chapter should not be negated by a parallel ISDS or related trade in services dispute.<sup>111</sup>

A defined anticipatory approach needs to be taken on the issue of co-applicability. It is helpful to have common legal principles, because when different trade regulations are applied in the sphere of digital trade it may raise issues that impact the regulatory autonomy of states.<sup>112</sup> The current approach to promote co-application between digital trade and other trade provisions, especially trade-in services, and investment is vague. Any legal clarity in relation to the co-application of trade regulations is entirely dependent on treaty interpretation by a given panel of experts on a case-by-case basis. Given the importance of digital trade regulations vis-à-vis other trade issues, specific guidance, or a common approach to resolving plausible conflicts must be considered and elaborated in trade agreements.

---

<sup>102</sup> *Id.*

<sup>103</sup> *Id.*

<sup>104</sup> *Id.*

<sup>105</sup> CP-TPP, *supra* note 66; RCEP CHAPTER 20: FINAL PROVISIONS, *supra* note 67; EJSI, *supra* note 68.

<sup>106</sup> *Id.*

<sup>107</sup> *Id.*

<sup>108</sup> *Id.*

<sup>109</sup> *Id.*

<sup>110</sup> CP-TPP, *supra* note 66; RCEP CHAPTER 20: FINAL PROVISIONS, *supra* note 67; EJSI, *supra* note 68.

<sup>111</sup> *Id.*

<sup>112</sup> *Id.*

## B. NON-DISCRIMINATORY TREATMENT OF DIGITAL PRODUCTS

The CP-TPP and eJSI provide for the non-discriminatory treatment of digital products.<sup>113</sup> The main provision that provides for the non-discriminatory treatment of digital products is similar in both the CP-TPP<sup>114</sup> and eJSI,<sup>115</sup> except that the CP-TPP uses “digital products” and eJSI uses “digital product”:

No Party/Member shall accord less favourable treatment to digital products (CP-TPP)/a digital product (eJSI) created, produced, published, contracted for, commissioned or first made available on commercial terms in the territory of another Party/Member, or to a digital product of which the author, performer, producer, developer or owner is a person of another Party/Member, than it accords to other like digital products. For greater certainty, to the extent that a digital product of a non-Party/non-Member is a ‘like digital product’, it will qualify as any ‘other like digital product’ for the purposes of this paragraph.<sup>116</sup>

Simon Lester explains that there is a difference between “digital product” and “digital products”<sup>117</sup> as it concerns the GATT/WTO debate over whether to compare the entire group of foreign and domestic products or to compare individual foreign and domestic products.<sup>118</sup> He gives an example:

...imagine a hypothetical world where there are ten search engines, five Canadian and five American. Canada then passes a law which adversely effects in a *de facto* way, without targeting nationality, explicitly – one of the American search engines and one of the Canadian search engines. Common sense would tell you that this law does not have a discriminatory effect on the basis of nationality, as the number of adversely affected products is equal between the two countries. For each country, four products are not adversely affected, while one is adversely affected. However, under the strain of thinking that says there is an adverse treatment of any individual foreign product under a measure is enough to count as a discriminatory effect, a violation can be found. If the one adversely affected American company fares worse under the measure than any one of the Canadian companies, there will be a violation, even if overall the American and Canadian companies come out the same for each country. 20 percent of the companies get worse treatment.<sup>119</sup>

The legal phrase “digital product(s) ‘development and developers’” in the context of a non-discriminatory treatment obligation is quite broad, encompassing any digital product so “created, produced, contracted for, commissioned or first made available on commercial terms in the territory of another Party, or to digital products of which the author, performer, producer, developer or owner is a person of another Party.”<sup>120</sup>

---

<sup>113</sup> CP-TPP, *supra* note 71, at art. 14.4: Non-Discriminatory Treatment of Digital Products; eJSI, *supra* note 71, at B.1: Non-Discrimination and Liability.

<sup>114</sup> *Id.*

<sup>115</sup> *Id.*

<sup>116</sup> Simon Lester, *Digital Trade Agreements and Domestic Policy*, CATO INSTITUTE (Apr. 14, 2021), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3828112](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3828112).

<sup>117</sup> *Id.*

<sup>118</sup> *Id.*

<sup>119</sup> *Id.*

<sup>120</sup> *Id.*

Essentially, it protects both the “development and developers of digital products” as GATS protects both “like services and service suppliers” from discrimination.<sup>121</sup> The fact that they use the term “digital products” and not “digital services” makes it obvious why they could not use the term “like digital services and service suppliers.”<sup>122</sup> Instead, they use “digital products” as a common term to clarify the non-discrimination obligation on both the “development and developers of digital products” in the participating member states.<sup>123</sup>

The non-discrimination obligation encompasses both the MFN and national treatment obligations for digital products with the use of phrase “than it accords to other like digital products.”<sup>124</sup> The definition for “like digital products” is not specifically provided in the CP-TPP and eJSI.<sup>125</sup> A clarification is provided which states: “...to the extent that a digital product of a non-Party/non-Member is a “like digital product”, it will qualify as any “other like digital product.”<sup>126</sup> It implies that the definition is flexible and it accepts degrees of “likeness” (“to the extent”) between digital products. Such varied likenesses can qualify two digital products as “like” for the purposes of this provision.<sup>127</sup> In the WTO jurisprudence, the concept of “likeness” has a narrow scope, applying to “directly competitive and substitutable products”.<sup>128</sup> The “likeness” is determined between the products by assessing four essential factors: “(a) product’s end-uses in a market; (b) consumers’ tastes and habits in a market; (c) product’s properties, nature and quality and (d) tariff classification of the product.”<sup>129</sup>

The definition of “like digital products” is not clearly delineated. The only clarification provided is “to the extent that a digital product of a non-Party/non-Member is a like digital product, it will qualify as any other like digital product.” Although any effort to define “like digital products” is useful, we do not consider that the present clarification is sufficient. Further, the “likeness” debate in the context of WTO jurisprudence has noticed various disagreements in the past.<sup>130</sup> Therefore, we need a deliberate approach to tackle this complex issue in the context of digital trade by assessing how “likeness” should be legally assessed in the new context of digital trade.

### C. CROSS-BORDER TRANSFER OF INFORMATION BY ELECTRONIC MEANS

The CP-TPP and RCEP provide that the parties recognize that each may have its own regulatory requirements concerning the transfer of information by electronic means.<sup>131</sup> Both mandate all member states to allow the cross-border transfer of information, however they use varied language to express the obligation.<sup>132</sup>

---

<sup>121</sup> *Id.*

<sup>122</sup> Lester, *supra* note 117.

<sup>123</sup> *Id.*

<sup>124</sup> *Id.*

<sup>125</sup> *Id.*

<sup>126</sup> *Id.*

<sup>127</sup> *Id.*

<sup>128</sup> Lester, *supra* note 117.

<sup>129</sup> *Id.*

<sup>130</sup> Joost Pauwelyn, *The Unbearable Lightness of Likeness*, GRADUATE INST. OF INT’L AND DEV. STUD. (2006), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2030940](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2030940). See also Mirelle Cossy, *Determining “likeness” under the GATS: Squaring the circle?*, WORLD TRADE ORGANIZATION ECONOMIC RESEARCH AND STATISTICS DIVISION STAFF WORKING PAPER ERSD-2006-08 (2006), [https://www.wto.org/english/res\\_e/reser\\_e/ersd200608\\_e.pdf](https://www.wto.org/english/res_e/reser_e/ersd200608_e.pdf).

<sup>131</sup> RCEP, *supra* note 71, at art. 12.15, fn. 13-14.

<sup>132</sup> *Id.*

Firstly, both the CP-TPP and RCEP consist of a similar legal provision on cross-border transfer of information by electronic means.<sup>133</sup> However, the RCEP does not specify that “cross-border transfer of information” includes “personal information” when compared to the CP-TPP:

CP-TPP, Article 14.11.2

Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.

RCEP, Article 12.15.2

A Party shall not prevent cross-border transfer of information by electronic means where such activity is for the conduct of the business of a covered person.

Secondly, out of the three eJSI proposals, the proposal by Japan, Brazil, Singapore, and UK is identical to the CP-TPP article 14.11.2 as described above.<sup>134</sup>

Thirdly, the eJSI proposal by US, Central African Republic, Korea, and Canada is different, as it adds “if/where this activity is for the consumers to access, distribute and use services and application” beyond the “conduct of an enterprise/business of a covered person/business”.<sup>135</sup>

eJSI B.2. Flow of Information

(1) Cross-border transfer of information by electronic means/cross-border data flows

“(5) (Alt 1) No Party shall prohibit or restrict/prevent the cross-border transfer of information, including personal information, by electronic means, (if/where) this activity is for the conduct of an enterprise/the business of a covered person/the business or for the consumers to access, distribute and use services and applications.”

This expands the scope of the obligation beyond the business activities of member states to include “consumers” who aim to “access, distribute, and use services or applications” in any member state party to the agreement.<sup>136</sup>

Fourthly, the last eJSI proposal by the EU is very different from the CP-TPP, RCEP, as well as the two eJSI proposals discussed above.<sup>137</sup> The EU’s eJSI proposal underlines that the “parties/members are committed to ensuring cross-border data flows to facilitate trade in the digital economy.”<sup>138</sup> Then, very critically, it provides that “to that end, cross-border data flows ‘shall’ not be restricted” by a list of four specific data localization requirements:

---

<sup>133</sup> *Id.*

<sup>134</sup> eJSI, *supra* note 71, at B.2: Flow of Information, (1) Cross-Border Transfer of Information by Electronic Means/Cross-Border Data Flows. Alt 2 is based on text proposals by Japan, Brazil, Singapore, and the UK.

<sup>135</sup> *Id.* Alt 1 is based on text proposals by the US, China, Korea, and Canada.

<sup>136</sup> *Id.* Alt 3 is based on text proposals by the EU.

<sup>137</sup> *Id.*

<sup>138</sup> *Id.*

- requiring the use of computing facilities or network elements in the Party's/Member's territory for the processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of a Party;
- requiring the localization of data in the Party's/Member's territory for storage or processing;
- prohibiting storage or processing in the territory of other Parties/Members;
- making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Party's/Member's territory or upon localization requirements in the Party's/Member's territory.<sup>139</sup>

A digital network infrastructure is constituted by four basic elements: hardware, software, protocols, and a connection medium.<sup>140</sup> The restrictions on cross-border data flows relating to network elements mean mandatory requirements to use specified network elements related to those four basic elements.<sup>141</sup> Essentially, there are three types of specific restrictions on data flows provided by the EU: (1) mandatory requirement to use specified network elements or computing facilities; (2) requirement of data localization for storage and processing in a member's territory; and (3) prohibiting storage or processing of data in another jurisdiction.<sup>142</sup> The EU's eJSI text proposal is specific but narrow in scope as compared to other provisions on cross-border data flows given the specific identification of a mandatory list of restrictions on cross-border data flows.<sup>143</sup>

#### C.I. 'LEGITIMATE PUBLIC POLICY OBJECTIVES' & 'NECESSITY' VS. 'GREATER THAN REQUIRED' TEST

The CP-TPP, RCEP, and eJSI proposals provide for varied provisions as regards to the legitimate policy space.<sup>144</sup> Essentially, they provide that nothing in this agreement "shall" prevent any member state from "adopting or maintaining" measures "to achieve legitimate public policy objectives".<sup>145</sup> However, the specific provisions do not provide "legal definition, clarification or any specific illustrative list of concerns" relating to the "legitimate public policy objectives." Only the eJSI proposal by Korea includes protection of privacy.<sup>146</sup> Therefore, it is dependent upon a legal interpretation of the phrase "legitimate public policy objective", given the relevant WTO jurisprudence which can help decipher the list of domestic policy concerns.

The interpretation of term "legitimate" in the context of CP-TPP, RCEP or eJSI can be based on the interpretation of the term "legitimate objective" in the analogous context of the TBT Agreement. Article 2.1 of the TBT Agreement requires a WTO panel to examine whether the detrimental impact that a measure has on imported products stems exclusively from

---

<sup>139</sup> *Id.*

<sup>140</sup> eJSI, *supra* note 71, at B.2: Flow of Information, (1) Cross-Border Transfer of Information by Electronic Means/Cross-Border Data Flows.

<sup>141</sup> *Id.*

<sup>142</sup> *Id.*

<sup>143</sup> *Id.*

<sup>144</sup> *Id.*; CP-TPP, *supra* note 71, at art. 14.11.3: Cross-Border Transfer of Information by Electronic Means; RCEP, *supra* note 71, at art. 12.15.3.

<sup>145</sup> *Id.*

<sup>146</sup> eJSI, *supra* note 71, at B.2: Flow of Information, (1) Cross-Border Transfer of Information by Electronic Means/Cross-Border Data Flows. Alt 3 is based on text proposals by Korea.

legitimate regulatory distinction rather than from discrimination against a group of imported products.<sup>147</sup>

Article 2.1 of the TBT Agreement provides that the legitimate regulatory distinction will account for the detrimental impact on imported products.<sup>148</sup> The term “legitimate” in relation to an “objective” refers to “an aim or target that is lawful, justifiable, or proper”, including by reference to objectives protected elsewhere in the agreements. If an impugned measure can be explained and substantiated in terms of protecting “cultural identity”, preserving “traditional knowledge and cultural expressions”, and promoting “indigenous rights”, such a measure would highly likely qualify as “achieving a legitimate public policy objective.”

The CP-TPP, RCEP, and eJSI provide for an obligation that the member states adopt or maintain measures to achieve legitimate public policy objectives.<sup>149</sup>

CP-TPP, Article 14.11

Cross-Border Transfer of Information by Electronic Means

Nothing in this Article shall prevent a party from adopting or maintaining measures inconsistent with Paragraph 2 to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on transfer of information greater than are required to achieve the objective.<sup>150</sup>

The CP-TPP provides that member states shall not be prevented from adopting or maintaining measures to achieve a legitimate public policy objective given that the measure “is not applied in a manner” which would constitute a “means of arbitrary or unjustifiable discrimination or a disguised restriction on trade.”<sup>151</sup> It further adds that such measures should not impose restrictions on transfers of information “greater than are required to achieve the objective.”<sup>152</sup>

---

<sup>147</sup> World Trade Organization, Technical Barriers to Trade Agreement, art. 2.1: Preparation, Adoption and Application of Technical Regulations by Central Government Bodies, Jan. 1, 1995. “Members shall ensure that in respect of technical regulations, products imported from the territory of any Member shall be accorded treatment no less favourable than that accorded to like products of national origin and to like products originating in any other country.”

<sup>148</sup> *Id.*

<sup>149</sup> CP-TPP, *supra* note 71, at art. 14.11: Cross-Border Transfer of Information by Electronic Means; RCEP, *supra* note 71, at art. 12.15: Cross-Border Transfer of Information by Electronic Means; eJSI, *supra* note 71, at B.2: Flow of Information, (1) Cross-Border Transfer of Information by Electronic Means/Cross-Border Data Flows. Alt 1 is based on text proposals by Japan, the US, China, Canada and the UK. Alt 2 is based on text proposals by Singapore and Brazil. Alt 3 is based on text proposal by Korea. Alt 4 is based on text proposals by the EU.

<sup>150</sup> *Id.*

<sup>151</sup> *Id.*

<sup>152</sup> *Id.*

RCEP, Article 12.15Cross-Border Transfer of Information by Electronic Means

(2) Nothing in this Article shall prevent a party from adopting or maintaining:

Any measure inconsistent with Paragraph 2 that it considers necessary to achieve a legitimate public policy objective, provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; or any measure it considers necessary for the protection of its essential security interests. Such measures shall not be disputed by other parties.<sup>153</sup>

The RCEP clarifies that the member states “shall” not be prevented from adopting or maintaining measures that are necessary to achieve a legitimate public policy objective.<sup>154</sup> However, such measures should not be “applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade.”<sup>155</sup> Further, it provides that the member states can adopt “any measures it considers necessary” for the protection of its “essential security interests.”<sup>156</sup> The provision does not define “essential security interests.”<sup>157</sup> However, under Article 29.2, it provides an indicative list of measures which can be classified as necessary to protect “essential security interests.”<sup>158</sup> Specifically, such measures include “protection of critical public infrastructures”, incorporating communications, power and water infrastructure, and whether such infrastructure is publicly or privately owned.<sup>159</sup> Lastly, it provides such measures that are considered necessary for the protection of essential security interests “shall” not be disputed by other member states of RCEP.<sup>160</sup>

The eJSI proposal by Japan, U.S., Canada, U.K. (Alt 1), Singapore, Brazil (Alt 2), and Korea (Alt 3) provides that nothing in the obligation on cross-border data flows “shall” prevent any member to adopt or maintain any measure “that is necessary to achieve a legitimate public policy objective.”<sup>161</sup> However, such a measure should not be applied “in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade.”<sup>162</sup> It further provides that such a measure “does not impose restrictions on transfers of information greater than necessary or required to achieve the objective.”<sup>163</sup>

---

<sup>153</sup> *Id.*

<sup>154</sup> *Id.*

<sup>155</sup> CP-TPP, *supra* note 71, at art. 14.11: Cross-Border Transfer of Information by Electronic Means; RCEP, *supra* note 71, at art. 12.15: Cross-Border Transfer of Information by Electronic Means; eJSI, *supra* note 71, at B.2: Flow of Information, (1) Cross-Border Transfer of Information by Electronic Means/Cross-Border Data Flows.

<sup>156</sup> *Id.*

<sup>157</sup> *Id.*

<sup>158</sup> *Id.*

<sup>159</sup> *Id.*

<sup>160</sup> *Id.*

<sup>161</sup> CP-TPP, *supra* note 71, at art. 14.11: Cross-Border Transfer of Information by Electronic Means; RCEP, *supra* note 71, at art. 12.15: Cross-Border Transfer of Information by Electronic Means; eJSI, *supra* note 71, at B.2: Flow of Information, (1) Cross-Border Transfer of Information by Electronic Means/Cross-Border Data Flows.

<sup>162</sup> *Id.*

<sup>163</sup> *Id.* In comparison to the eJSI proposal by Japan, the US, Canada, and the UK, the eJSI proposal by Singapore and Brazil provides that “such a measure should not be applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade or barrier to the transfer of information and to trade through electronic means.”

The eJSI proposal by Korea uniquely specifies that any member state can adopt or maintain measures “it considers necessary for the protection of its essential security interests.”<sup>164</sup>

None of the eJSI proposals discussed above define or explain the phrase “legitimate public policy objectives”, “essential security interests” with clear examples, nor provides for an “illustrative list of public policy objectives.”<sup>165</sup> However, the eJSI proposal by Korea distinctively states that the “legitimate public policy objectives” include “the protection of privacy.”<sup>166</sup>

In contrast to the three eJSI proposals discussed above, the proposal by the EU is quite different.<sup>167</sup> It provides that the members “may”, as appropriate, adopt or maintain measures to “ensure the protection of personal data and privacy.”<sup>168</sup> Further, such measures or safeguards “may” include the “adoption and application of rules for cross-border transfer of personal data.”<sup>169</sup> Specifically, it states that: “[N]othing in the agreed disciplines and commitments shall affect the protection of personal data and privacy afforded by the members’ respective safeguards.”<sup>170</sup> Here, we note that the language is different, there is no mention of “legitimate public policy objective” or “essential security interests” instead the EU’s eJSI proposal provides “... safeguards ... appropriate to ensure the protection of personal data and privacy.”<sup>171</sup> The EU’s eJSI proposal falls short of the larger expectations to consider or define purposefully the importance of the phrase “legitimate public policy objectives” beyond data privacy.<sup>172</sup>

The legal scope of “necessary” is narrow in the CP-TPP, compared to “greater than required”, as provided in the RCEP.<sup>173</sup> According to the principle of effectiveness in treaty interpretation, when treaty terms have been intentionally differentiated in this way, they need to be given different meaning.<sup>174</sup> As the parties deliberately chose the word “necessary” rather than “required”, given that the WTO jurisprudence ascribes different meaning to the measures that use “necessary” with regard to “essential” to achieve an objective or those described as simply “relating to” an objective.<sup>175</sup>

In this regard, it is noteworthy that the term “required” is also used in Article 5.6<sup>176</sup> of the Agreement on the Application of Sanitary and Phytosanitary (SPS agreement) in a similar

---

<sup>164</sup> *Id.*

<sup>165</sup> *Id.*

<sup>166</sup> *Id.*

<sup>167</sup> CP-TPP, *supra* note 71, at art. 14.11: Cross-Border Transfer of Information by Electronic Means; RCEP, *supra* note 71, at art. 12.15: Cross-Border Transfer of Information by Electronic Means; eJSI, *supra* note 71, at B.2: Flow of Information, (1) Cross-Border Transfer of Information by Electronic Means/Cross-Border Data Flows.

<sup>168</sup> *Id.*

<sup>169</sup> *Id.*

<sup>170</sup> *Id.*

<sup>171</sup> *Id.*

<sup>172</sup> *Id.*

<sup>173</sup> CP-TPP, *supra* note 71, at art. 14.11: Cross-Border Transfer of Information by Electronic Means; RCEP, *supra* note 71, at art. 12.15: Cross-Border Transfer of Information by Electronic Means; eJSI, *supra* note 71, at B.2: Flow of Information, (1) Cross-Border Transfer of Information by Electronic Means/Cross-Border Data Flows.

<sup>174</sup> *Id.*

<sup>175</sup> *Id.*

<sup>176</sup> World Trade Organization, Sanitary and Phytosanitary Agreement, art. 5: Assessment of Risk and Determination of the Appropriate Level of Sanitary or Phytosanitary Protection, Apr. 15, 1994. “Without prejudice to paragraph 2 of Article 3, when establishing or maintaining sanitary or phytosanitary measures to



context, namely “measures being not more restrictive than required to achieve the legitimate public policy objectives.”<sup>177</sup> Further, it is clarified in the footnote to Article 5.6 of the SPS agreement that this language is intended to afford a higher degree of deference to regulators.<sup>178</sup> Specifically, a measure is only more trade-restrictive than required if there is evidence of a significantly less trade-restrictive alternative.<sup>179</sup> Accordingly, the use of the term “required” instead of “necessary” indicates an intention to afford a margin of deference to the government or regulatory authority adopting the measure at issue.<sup>180</sup> This is not to suggest that the existence of a less trade-restrictive alternative is irrelevant.<sup>181</sup> On the contrary, the language: “...greater...than...” in these provisions points to the comparative nature of the legal test.<sup>182</sup> A comparative test necessarily requires the impugned measure to be assessed against a comparator, which, in the context of provisions, would be a less trade-restrictive means of achieving the legitimate objective.<sup>183</sup>

C.II. “APPLIED IN A MANNER WHICH WOULD CONSTITUTE A MEANS OF ARBITRARY OR UNJUSTIFIABLE DISCRIMINATION OR A DISGUISED RESTRICTION ON TRADE”

A measure will be considered “arbitrary, unjustifiable or disguised” if it bears no rational connection with the legitimate public policy objective at issue. The contextual elements of CP-TPP, RCEP, and eJSI shed light on what will comprise an arbitrary and unjustifiable discrimination in any specific instance. In WTO parlance, similar legal issue is concerned mainly with the application and implementation of the measure. The principle of good faith is the essence wherein the state is obliged to exercise its rights in a bona fide manner and not in an abusive manner. Essentially, the test aims to find a thin line of equilibrium between rights and obligations of the states in the agreement so that neither completely cancels out the other. The line of equilibrium is not fixed but is subject to the context of a given case. In understanding the constituents of “arbitrary, unjustifiable and disguised restriction on trade”, we need to appreciate whether the measure is not unreasonable to certain states and whether a good faith approach was undertaken in the application of such measures so that any inadvertent discrimination was reasonably and amicably resolved.

The US has a broader approach as compared to the EU on the protection of cross-border data flows.<sup>184</sup> Although a prohibited list of data localization measures as proposed by the EU

---

achieve the appropriate level of sanitary or phytosanitary protection, Members shall ensure that such measures are not more trade-restrictive than required to achieve their appropriate level of sanitary or phytosanitary protection, taking into account technical and economic feasibility.”

<sup>177</sup> *Id.*

<sup>178</sup> *Id.*

<sup>179</sup> *Id.*

<sup>180</sup> *Id.*

<sup>181</sup> *Id.*

<sup>182</sup> WTO Sanitary and Phytosanitary Agreement at art. 5.

<sup>183</sup> *Id.*

<sup>184</sup> We note the divergent approaches to provide cross-border transfer of information by electronic means in the CP-TPP, RCEP, and three eJSI proposals. We specially note the two eJSI proposals that are different than the CP-TPP and RCEP. These two eJSI proposals, as led by the US and the EU, provide an innovative clue into the future design of provisions on cross-border transfer of information by electronic means in digital trade agreements. The eJSI proposal by the US covers activities of “consumers” alongside “businesses” for the protection of the cross-border transfer of information in digital trade: “if/where this activity is for the consumers to access, distribute and use services and application” beyond the “conduct of an enterprise/business of a covered person/business.” We should appreciate that the consumers create an enormous amount of digital activity which supports both the private and public sector in generating economy of scales by supplying necessary digital goods in the economy. The eJSI proposal by the US should be understood in this context and considered by future digital trade negotiations. Lastly, as noted above, the eJSI proposal by the EU on the protection of cross-border transfer of information specifically

will support better cross-border data flows, the importance of a broad regulatory foresight as supported by the US is even better because it covers digital activity of consumers as the main catalyst for cross-border data flows.

#### D. PERSONAL INFORMATION PROTECTION

##### D.I. “DEFINITION OF PERSONAL INFORMATION/DATA”

The CP-TPP and RCEP provides for an identical legal definition of “personal information” as “any information, including data, about an identified or identifiable natural person.”<sup>185</sup> The eJSI provides for the legal definition of “personal information” in three proposals.<sup>186</sup>

The eJSI proposal by the US, Hong Kong, Korea, and Canada provides for an identical definition of “personal information” to the CP-TPP and RCEP.<sup>187</sup> However, the definition provides a bracket, i.e., an indecision among the members on whether to use “about” or “relating to” to provide that the “personal information” should be connected to an “identifiable or identified person”.<sup>188</sup> The use of legal terminology “about” is narrower in scope than “relating to”, which is broad in scope. It has an impact on the actual scope of personal information covered by the obligation.

The eJSI proposal by the EU, Russia, and Brazil uses the phrase “personal data” instead of “personal information” to define the concept.<sup>189</sup> Further, it clarifies that the types of information include both direct and indirect information “about or relating to” an “identified or identifiable person.”<sup>190</sup> It is pertinent for two reasons. First, it is understood that the term “data” is different from “information.”<sup>191</sup> The term “data” does not serve any purpose unless given to something, whereas the term “information” is arrived at when specific data points are interpreted and assigned to a meaning or process.<sup>192</sup> Secondly, federal agencies in the US are accustomed to a definition of “personally identifiable information”, which is a broad term, but it is interpreted in a narrow manner to include only “reasonable risks to individual privacy”, as compared to the widely known definition of “personal data” that is a specific term but broadened by the EU’s GDPR to recognize all plausible risks or concerns relating to individual privacy.<sup>193</sup>

---

restricts four types of data localization measures: (1) mandatory requirement to use specified network elements or computing facilities; (2) requirement for data localization for storage and processing in a member’s territory; (3) prohibiting storage or processing in the territory of other Parties/Members; and (4) making cross-border transfer of data contingent upon use of computing facilities or network elements in the Party’s or Member’s territory or upon localization requirement in the Party’s territory. None of the three CP-TPP, RCEP, or eJSI clearly delineate an illustrative list of legitimate public policy objectives to regulate cross-border data flows. South Korea’s eJSI proposal provides an attempt by stating that legitimate public policy objective includes protection of privacy. We submit that the legal contours of “legitimate public policy objectives” should be clearly delineated in the context of digital trade, specifically per key regulatory provision as well as comprehensively in the general and security exceptions.

<sup>185</sup> CP-TPP, *supra* note 71; RCEP, *supra* note 71; eJSI, *supra* note 71.

<sup>186</sup> *Id.*

<sup>187</sup> *Id.*

<sup>188</sup> *Id.*

<sup>189</sup> *Id.*

<sup>190</sup> *Id.*

<sup>191</sup> CP-TPP, *supra* note 71; RCEP, *supra* note 71; eJSI, *supra* note 71.

<sup>192</sup> *Id.*

<sup>193</sup> *Id.*

The eJSI proposal by China is very different from the two proposals as led by the US and the EU.<sup>194</sup> The eJSI proposal by China provides that “personal information” means “various types of information.”<sup>195</sup> It can either be “recorded by electronic or other means.”<sup>196</sup> Further, such information can be used “individually or in combination” with other information for “identifying the identity of natural person.”<sup>197</sup>

The phrase “various types of information” clarifies that China wishes to have a broad coverage of all kinds of personal data within the ambit of personal information.<sup>198</sup> Instead of stating “personal information”, China provides “various types of information”, which can impact right to privacy of any person.<sup>199</sup> It is broad terminology to use in the context of personal information protection.<sup>200</sup> Further, it clarifies that such information can either be recorded through electronic means or non-electronic means for the purposes of digital trade activities.<sup>201</sup> This clarification is not provided in the US and the EU’s eJSI proposals: CP-TPP or RCEP.<sup>202</sup> Lastly, the most critical addition in the definition of personal information by China is the recognition that such information “individually or in combination” has the capability to violate the privacy of a person.<sup>203</sup> This clarification is provided neither in the EU or US eJSI proposals nor in CP-TPP or RCEP.<sup>204</sup>

There are distinct approaches by the US, EU, and China in regard to the definition of “personal information or data.”<sup>205</sup> In the context of digital trade, the US has a narrow approach, as compared to the broader approach to define personal data or information by the EU and China.<sup>206</sup>

## D.II. ECONOMIC AND SOCIAL BENEFITS OF DATA PRIVACY

The CP-TPP and eJSI proposal by Japan, Singapore, Hong Kong, Korea, China, Russia, Canada, and UK provide that there is a general recognition among member states in regard to the economic and social benefits relating to the protection of personal information or data to enhance consumer confidence and trust in digital trade.<sup>207</sup>

The eJSI proposal by the EU expresses its approach to personal information protection in general.<sup>208</sup> It is worth restating the same:

---

<sup>194</sup> *Id.*

<sup>195</sup> *Id.*

<sup>196</sup> *Id.*

<sup>197</sup> CP-TPP, *supra* note 71; RCEP, *supra* note 71; eJSI, *supra* note 71.

<sup>198</sup> *Id.*

<sup>199</sup> *Id.*

<sup>200</sup> *Id.*

<sup>201</sup> *Id.*

<sup>202</sup> *Id.*

<sup>203</sup> CP-TPP, *supra* note 71; RCEP, *supra* note 71; eJSI, *supra* note 71.

<sup>204</sup> *Id.*

<sup>205</sup> *Id.*

<sup>206</sup> *Id.*

<sup>207</sup> CP-TPP, *supra* note 71, at art. 14.2: Scope and General Provisions; eJSI, *supra* note 71, at C.2: Privacy, (1) Personal Information Protection/Personal Data Protection, (3). Alt 1 is based on text proposals by Japan, Singapore, Hong Kong, China, Russia, Canada and the UK. Alt 2 is based on text proposal by the EU. Alt 3 is based on text proposal by the US.

<sup>208</sup> *Id.*

...Parties/Members recognize that the protection of personal data and privacy is a fundamental right and that high standards in this regard contribute to trust in the digital economy and to the development of trade.<sup>209</sup>

It frames the subject-matter of privacy as protecting a “fundamental right”, underlying the democratic constitutional and human rights framework, generally.<sup>210</sup> Critically, it underlines that protection of privacy is a matter of fundamental human right to ensure “trust” in the digital economy, which is important for the development of digital trade.<sup>211</sup>

The eJSI proposal by the US differs from the EU on its legal approach to personal information protection.<sup>212</sup> It states that “the Parties/Members recognize the importance of ensuring compliance with measures to protect personal information and ensuring that any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented.”<sup>213</sup>

The eJSI proposal by the US provides that, although compliance with measures to protect privacy are important, any such measure needs to be “necessary and proportionate” to the risks to data privacy.<sup>214</sup> It is a different approach as compared to the EU’s eJSI proposal, which frames the issue of data privacy protection as respecting fundamental human rights of citizens, i.e., such rights should be properly considered against the need for cross-border data flows in case of conflict,<sup>215</sup> whereas the US’s eJSI proposal aims to invoke the requirements of “necessity and proportionality.”<sup>216</sup>

#### D.III. LEGAL FRAMEWORK FOR DATA PRIVACY

The CP-TPP provides that it is mandatory for the member states to adopt or maintain a legal framework for personal information protection of digital trade users.<sup>217</sup> It further clarifies that in developing such legal framework the states “should” consider relevant international principles and guidelines of international bodies.<sup>218</sup> Thus, the obligation to adopt or maintain a legal framework for personal information protection is mandatory, but following internationally-recognized principles or guidelines is only a recommendation.<sup>219</sup>

Importantly, footnote 6 to article 14.8.2 of the CP-TPP states:

For greater certainty, a Party may comply with the obligation in this paragraph by adopting or maintaining measures such as a comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, or

---

<sup>209</sup> *Id.*

<sup>210</sup> *Id.*

<sup>211</sup> *Id.*

<sup>212</sup> *Id.*

<sup>213</sup> CP-TPP, *supra* note 71, at art. 14.2: Scope and General Provisions; eJSI, *supra* note 71, at C.2: Privacy, (1) Personal Information Protection/Personal Data Protection, (3).

<sup>214</sup> *Id.*

<sup>215</sup> *Id.*

<sup>216</sup> *Id.*

<sup>217</sup> CP-TPP, *supra* note 71, at art. 14.8 fn. 5.

<sup>218</sup> *Id.*

<sup>219</sup> *Id.*

laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy.<sup>220</sup>

It clarifies that the legal framework adopted or maintained by a state to comply with the obligation can include a “comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, or voluntary undertakings by enterprises.”<sup>221</sup>

In contrast, the RCEP provides for a legally mandatory requirement for both obligations.<sup>222</sup> It mandates the states to adopt or maintain a legal framework for the protection of personal information as well as mandatorily follow “international standards, principles, guidelines, and criteria of relevant international organisations or bodies’ in pursuance of the same.”<sup>223</sup>

It is important to note the difference in the obligations under CP-TPP and RCEP on abiding by internationally recognized principles, i.e., the former recommends whereas the latter mandates the states to follow them.<sup>224</sup> In pursuance, the RCEP clearly elaborates that such principles include “international standards, principles, guidelines, and criteria of relevant international organisations or bodies”.<sup>225</sup>

Importantly, the RCEP under footnote 8 of article 12.8.1 states that the obligation to adopt or maintain a legal framework on personal information protection can be complied with the adoption of a “comprehensive privacy or personal information protection law, sector-specific laws or laws which provide for the enforcement of contractual obligations assumed by juridical persons.”<sup>226</sup>

The eJSI provides three proposals to require that the states need to maintain a legal framework for the protection of personal information or data.<sup>227</sup> The eJSI proposal by Japan, US, Singapore, Hong Kong, Brazil, Ukraine, Korea, China, Canada, and UK mandates that the states “shall” adopt or maintain ‘a legal framework or measures’ for the protection of personal information.<sup>228</sup> The states can either have a national regulatory framework or various sector-wise regulations in pursuance of same.<sup>229</sup>

As noted earlier, the US’s approach is different from the EU, as the former considers it necessary to legally balance the data privacy-related measures with the requirement for cross-border data flows by employing terms such as “necessity and proportionality”, whereas the

---

<sup>220</sup> *Id.*

<sup>221</sup> *Id.*

<sup>222</sup> RCEP, *supra* note 71, at art. 12.8: Online Personal Information Protection.

<sup>223</sup> *Id.*

<sup>224</sup> *Id.*

<sup>225</sup> *Id.*

<sup>226</sup> *Id.*

<sup>227</sup> eJSI, C.2. Privacy, *supra* note 68, (1) Personal information protection/personal data protection, (4) [Alt 1 based on text proposals by Japan, US, Singapore, Hong Kong, Brazil, Ukraine, Korea, China, Canada and UK]. [Alt 2 based on text proposal by EU]. [Alt 3 based on text proposal by Russia].

<sup>228</sup> *Id.*

<sup>229</sup> *Id.*

latter wishes to ensure “highest standards” for data privacy protection as a fundamental constitutional and human rights principle to promote consumer trust in digital trade.<sup>230</sup>

The eJSI proposal by the EU in the context of “legal framework for the protection of personal information/data” provides that the states “may” adopt and maintain “safeguards” for the protection of personal information.<sup>231</sup> These safeguards may include rules on cross-border transfer of personal data.<sup>232</sup> It provides for a mandatory exception which states that “nothing in this agreement ‘shall’ affect the protection of personal data and privacy afforded by Parties/Members’ respective safeguards.”<sup>233</sup> It aims to provide an exception for the chosen level of protection by the states in order to protect personal data.<sup>234</sup> As it uses the phrase “afforded by Parties’ respective safeguards.”<sup>235</sup>

The eJSI proposal by Russia provides a legal mandate for the states that they ‘*shall* adopt or maintain measures to ensure protection of personal data.’<sup>236</sup> It further provides that such measures include rules on cross-border transfer and processing of personal data to promote “fundamental values of respect for privacy and protection of personal data.”<sup>237</sup>

Importantly, sub-paragraph 6 of the eJSI provides that the states can comply with the obligation to have a legal framework on personal information protection by adopting a “comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertaking by enterprises.”<sup>238</sup> The flexibility to have a *national or sector-specific data protection laws or voluntary undertaking by enterprises* is constructive for countries with distinct legal systems to efficaciously regulate data protection issues.

#### D.IV. INDICATIVE LIST OF INTERNATIONAL FRAMEWORKS FOR DATA PRIVACY

The eJSI proposals provide for the list of international frameworks which can be used as guidance by the member states to develop their respective legal frameworks on data privacy.<sup>239</sup> The eJSI proposal by Japan, Hong Kong, Brazil, Korea, China, Canada, and UK provides that the states should take into consideration principles, guidelines, standards or criteria of relevant international bodies or organisations, e.g. the *OECD recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data (2013)*.<sup>240</sup> The obligation can either be recommendatory or mandatory in nature as the proposal is finalized.<sup>241</sup>

<sup>230</sup> eJSI, C.2. Privacy *supra* note 68, (1) Personal Information Protection/Personal Data Protection, (4) (Alt 1) [Alt 1 based on text proposals by Japan, US, Singapore, Hong Kong, Korea, China, Russia, Canada and UK]. (Alt 2) [Alt 2 based on text proposal by EU]. (Alt 3) [Alt 3 based on text proposal by Russia].

<sup>231</sup> *Id.*

<sup>232</sup> *Id.*

<sup>233</sup> *Id.*

<sup>234</sup> *Id.*

<sup>235</sup> *Id.*

<sup>236</sup> eJSI, C.2. Privacy, (1) Personal Information Protection/Personal Data Protection, *supra* note 68.

<sup>237</sup> *Id.*

<sup>238</sup> *Id.*

<sup>239</sup> eJSI, C.2. Privacy, *supra* note 68 ( (1) Personal Information Protection/Personal Data Protection, (5) (Alt 1) [Alt 1 based on text proposals by Japan, Hong Kong, Brazil, Korea, China, Canada and UK.] (Alt 2) [Alt 2 based on text proposals by Singapore].

<sup>240</sup> *Id.*

<sup>241</sup> *Id.*

The eJSI proposal by Singapore provides that the states “to the extent possible” shall consider the “principles and guidelines of relevant international bodies” in developing a legal framework for protection of personal information.<sup>242</sup> Only the EU’s eJSI proposal provides that the subjection of national legal regulations to international legal framework or guidance is not mandatory.<sup>243</sup> The eJSI proposal by Japan, US, Singapore, Hong Kong, Brazil, Ukraine, Korea, Canada, and UK provide a bracket “[should/may/shall]” for the member states to follow international legal principles or guidance to formulate domestic legal framework on personal data protection.<sup>244</sup>

The CP-TPP provides that “in the development of its legal framework for the protection of personal information each Party ‘should’ consider principles and guidelines of relevant international bodies.”<sup>245</sup>

The RCEP under article 12.8.2 states that: “...in the development of its legal framework for the protection of personal information, each Party ‘shall’ consider international standards, principles, guidelines, and criteria of relevant international organizations or bodies.”<sup>246</sup>

We propose that digital trade agreements should promote a mandatory requirement for member states to design their national data protection regulations in consideration of internationally accepted data protection principles. Further, the digital trade agreements should regularly update the list of applicable international guidelines on data protection, e.g., the *OECD Declaration on Government Access to Personal Data Held by Private Sector Entities, 2022*.<sup>247</sup>

#### D.V. NON-DISCRIMINATORY PRACTICES FOR PERSONAL DATA PROTECTION

The CP-TPP and two eJSI proposals provide that the states should consider non-discriminatory practices when protecting personal information or data of e-commerce users.<sup>248</sup> Comparatively, the RCEP does not provide for a similar obligation.<sup>249</sup> The CP-TPP and two eJSI proposals provide that the states “shall endeavor” to adopt non-discriminatory practices to protect users of digital trade from privacy violations.<sup>250</sup> The eJSI proposals by Japan, Hong Kong, Ukraine, Korea, China, Singapore, Canada and the UK further provide that the protection is from either personal information or data protection violations or criminal acts (link to cybersecurity crimes involving personal data and information) occurring within the jurisdiction.<sup>251</sup> The eJSI proposal by Brazil additionally elaborates that the “protection is meant for the citizens, consumers, and medical patients from any privacy violations.”<sup>252</sup>

---

<sup>242</sup> *Id.*

<sup>243</sup> *Id.*

<sup>244</sup> eJSI, C.2. Privacy, (1) Personal Information Protection/Personal Data Protection, *supra* note 68 (5)(Alt 1) (Alt 1 based on text proposals by Japan, Hong Kong, Brazil, Korea, China, Canada and UK.) (Alt 2) (Alt 2 based on text proposal by Singapore).

<sup>245</sup> CP-TPP, Chapter 14 – Electronic Commerce, Article 14.8: Personal Information Protection, *supra* note 66 at Sub-clause 2.

<sup>246</sup> RCEP, Chapter 12 – Electronic Commerce, Article 12.8.2, *supra* note 67.

<sup>247</sup> OECD Legal Instruments, ‘Declaration on Government Access to Personal Data Held by Private Sector Entities, 2022’ (OECD/LEGAL/0487) <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487>.

<sup>248</sup> CP-TPP, Article 14.8, *supra* note 66.

<sup>249</sup> *Id.*

<sup>250</sup> *Id.*

<sup>251</sup> *Id.*

<sup>252</sup> *Id.*

Non-discrimination practices in protecting users of digital trade from personal data violations is a substantive legal obligation even though in some instances on a best endeavor basis. It implies that in implementing personal data protection regulations, the member states should protect both citizens and non-citizen residents (users) of digital trade equally within their jurisdiction.<sup>253</sup> Any discrimination among users based on their nationality within a jurisdiction restricts digital trade. Generally, the data protection laws comply with this obligation as the GDPR apparently applies to both the EU citizens (home or abroad) and non-EU natural persons residing within EU's jurisdiction<sup>254</sup>; the new proposed (not yet adopted) American Data Privacy and Protection Act (ADPPA) applies to all natural persons residing in the US<sup>255</sup>; and the Personal Information Protection Law (PIPL) applies to all "natural persons" residing within China.<sup>256</sup> However, the obligation should be supported with practical explanations given complex data protection practices by countries.

#### D.VI. CONSENT

The eJSI proposal by Russia provides that the states "shall ensure" that "directly expressed consent" is obtained for cross-border transfer and processing of personal data.<sup>257</sup> Neither the CP-TPP nor RCEP provides for obtaining consent for cross-border transfer or processing of personal data.<sup>258</sup> "Consent" is an important data protection principle, especially in relation to cross-border data flows. It should be properly articulated in the context of cross-border data flows in digital trade agreements.

#### D.VII. TRANSPARENCY AND COOPERATION MECHANISMS FOR INTEROPERABILITY

Article 14.8.4 of CP-TPP provides that states "should" publish information on the protections of personal information of digital trade users.<sup>259</sup> It includes the legal remedies available to individuals as well as how business can comply with the legal requirements.<sup>260</sup> Article 12.8.3 of RCEP provides for the same obligation, however, makes it mandatory with the use of term "shall" instead of "should."<sup>261</sup>

The eJSI proposal provides for the same obligation under subparagraph 9 as proposed by Japan, US, Singapore, Hong Kong, Brazil, Korea, China, Canada and UK.<sup>262</sup> However, it uses

<sup>253</sup> Jane Drake-Brockman et al., *Digital Trade and the WTO: Negotiation Priorities for Cross-border Data Flows and Online Trade in Services*, Jean Monnet TIIA Network Working Paper No. 11-2011, September 2021, page 7, <https://iit.adelaide.edu.au/ua/media/1551/wp-2021-11-j.drake-brockman-et-al.pdf>.

<sup>254</sup> GDPR, Article 3: Territorial Scope ("This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.") <https://gdpr-info.eu/art-3-gdpr/>.

<sup>255</sup> H.R. 8152 – American Data Privacy and Protection Act, (Section 2: Definitions, (19) Individual: The term "individual" means a natural person residing in the United States.) <https://www.congress.gov/bill/117th-congress/house-bill/8152/text#toc-H0299B60817D742978DC3C447CD110A88>.

<sup>256</sup> DigiChina, Stanford University, 'Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021, (Article 3: "This Law applies to the activities of handling the personal information of natural persons within the borders of the People's Republic of China")' <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/>.

<sup>257</sup> eJSI, C.2. Privacy, (1) Personal Information Protection/Personal Data Protection, *supra* note 68 at 8.

<sup>258</sup> *Id.*

<sup>259</sup> CP-TPP, Article 14.16: Cooperation on Cybersecurity Matters, *supra* note 66.

<sup>260</sup> *Id.*

<sup>261</sup> RCEP, Article 12.8.3: Online Personal Information Protection, *supra* note 67

<sup>262</sup> eJSI, C.2. Privacy, (1) Personal Information Protection/Personal Data Protection, *supra* note 68.,



a bracket that means the proposal is not finalized whether the obligation is mandatory or recommendatory with the use of term “shall” or “should.”<sup>263</sup> Further, the proposal provides that the personal information/data protections of “users or digital trade or e-commerce, citizens, consumers and medical patients” is covered by the obligation.<sup>264</sup>

Specifically, article 12.7 of RCEP, subparagraph 3 mandates that the states “shall” encourage “juridical persons”, e.g., businesses, or entities to “publish, including on the internet, their policies and procedures related to the protection of personal information.”<sup>265</sup> The obligation to “publish” information relating to personal information protection enhances regulatory transparency in digital trade.<sup>266</sup> The obligation to publish policies and procedures relating to the protection of personal information must be made mandatory for all the member states as well as specific juridical persons.<sup>267</sup> Cooperation through dedicated platforms, especially among the key multistakeholder and inter-governmental organisations is critical in this sphere. Significant developments and information should be collated and published online for transparency in a coordinated manner.<sup>268</sup> The information should provide meticulous update on various regulatory policies or procedures per jurisdiction.<sup>269</sup> A dedicated platform on personal information protection policies and procedures will be critical for long-term capacity-building, enabling trust among digital trade stakeholders, and effective negotiated outcomes among states to promote regulatory coherence.<sup>270</sup>

#### D.VIII. INTEROPERABILITY OF DOMESTIC MECHANISMS

The CP-TPP, RCEP, and eJSI emphasize on cooperation among states to protect personal information.<sup>271</sup> The cooperation is envisaged along with the development of mechanisms for mutual recognition of regulatory outcomes.<sup>272</sup> The CP-TPP additionally clarifies that such regulatory recognition mechanisms can be awarded autonomously, by mutual arrangement, or a broader international framework.<sup>273</sup> In pursuance, the states “shall endeavour” to exchange information on such mechanisms and explore ways to promote compatibility between the same.<sup>274</sup> The eJSI provides for similar obligation and further states that such mechanisms of mutual regulatory recognition may include: “...appropriate recognition of comparable protection afforded by their respective legal frameworks, national Trustmark or certification frameworks, or other avenues of transfer of personal information among states.”<sup>275</sup>

#### D.IX. TARGETED DISCRIMINATION OF COMMUNITIES THROUGH PERSONAL INFORMATION

The eJSI proposal by Canada provides that the states “shall” not use personal information as obtained from enterprises in a manner which constitutes targeted discrimination on

---

<sup>263</sup> CP-TPP, 65, Article 14.8.4, *supra* note 66; RCEP, Article 12.8.3, *supra* note 67; eJSI, C.2. Privacy, (1) Personal Information Protection/Personal Data Protection, *supra* note 68 at 9.

<sup>264</sup> *Id.*

<sup>265</sup> *Id.*

<sup>266</sup> *Id.*

<sup>267</sup> *Id.*

<sup>268</sup> *Id.*

<sup>269</sup> CP-TPP, 65, Article 14.8.4, *supra* note 66; RCEP, Article 12.8.3, *supra* note 67; eJSI, C.2. Privacy, (1) Personal Information Protection/Personal Data Protection, *supra* note 68 at 9.

<sup>270</sup> *Id.*

<sup>271</sup> CP-TPP, Article 14.16: Cooperation on Cybersecurity Matters, *supra* note 66.

<sup>272</sup> *Id.*

<sup>273</sup> *Id.*

<sup>274</sup> *Id.*

<sup>275</sup> *Id.*

manifestly unlawful grounds.<sup>276</sup> These unlawful grounds include race, colour, sex, sexual attributes, gender, language, religion, political or other opinion.<sup>277</sup> It further provides that the states shall endeavour to ensure that personal information accessed from an enterprise is protected against “loss, theft, unauthorized access, disclosure, copying, use or modification.”<sup>278</sup> Lastly, it clarifies that the personal information so accessed by any state from an enterprise should not be accessed, disclosed, used or modified by a government authority in a manner which can cause significant harm to an individual.<sup>279</sup> A footnote to this obligation provides that any public disclosure of personal information which can be reasonably expected to cause significant harm does not constitute a violation of the obligation provided that it is done for the purposes of legitimate law enforcement activities, judicial proceedings, compliance with regulatory requirements, or national security.<sup>280</sup> The eJSI under subparagraph 2 defines “significant harm” to include “bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.”<sup>281</sup>

The obligation that state access to personal data from private entities within their jurisdiction is not used in a manner that constitutes targeted discrimination or any such activity which causes significant harm to an individual is a novel data protection obligation by the eJSI proposal of Canada. We note that these obligations are incorporated in the new data protection laws such as the proposed (unadopted) American Data Protection and Privacy Act (ADPPA) 2022 that provides for a novel obligation titled “Civil Rights and Algorithms”. It states that personal data should not be used “*in a manner which discriminates on the basis of race, color, religion, national origin, sex, or disability.*”<sup>282</sup> The personal data protection provisions in digital trade should be updated by appropriately studying such novel obligations.

#### E. CYBERSECURITY

Article 14.16 of CP-TPP provides that the states should recognize the importance of “building capabilities” of their national cybersecurity response mechanisms which enables identification and mitigation of malicious intrusions or dissemination of malicious code affecting the electronic networks of other CP-TPP states.<sup>283</sup> Article 12.13 of RCEP provides that the states should recognize the importance of building capabilities of national cybersecurity response mechanisms through the exchange of best practices and cooperate using the existing collaboration mechanisms on relevant matters.<sup>284</sup>

The eJSI proposal on cybersecurity revolves around three broad topics: (a) recognizing the cybersecurity threat; (b) build capabilities and best practices; and (c) adopt risk-based approaches.<sup>285</sup>

---

<sup>276</sup> eJSI, C.2. Privacy, (1) Personal Information Protection/Personal Data Protection, *supra* note 68, at 45.

<sup>277</sup> *Id.*

<sup>278</sup> *Id.*

<sup>279</sup> *Id.*

<sup>280</sup> *Id.*

<sup>281</sup> *Id.*

<sup>282</sup> H.R. REP. NO. 117-669 (2022), Section 207: Civil Rights Obligations, *supra* note 256, ADPPA, Section 207: Civil Rights Obligations.

<sup>283</sup> CP-TPP, Article 14.16: Cooperation on Cybersecurity Matters, *supra* note 66.

<sup>284</sup> *Id.*

<sup>285</sup> eJSI, D.2. Cybersecurity, *supra* note 68, at 58.

On the first topic of recognizing the cybersecurity threat, the eJSI proposal by the US and UK provides that the ‘threats to cybersecurity undermines digital trade.’<sup>286</sup> The eJSI proposal by Ukraine provides that the states should recognize the increasing number of information systems which are processing personal data and consequently the risk in cybercrime and fraud.<sup>287</sup> It emphasizes that the impact of such activities should be minimized.<sup>288</sup>

As regards the second topic relating to “build capabilities and best practices”, the eJSI proposal by Korea, Japan, US, Ukraine and UK emphasizes on capacity-building of national entities responsible for the evolving nature of cybersecurity incident and enabling or strengthening existing collaboration mechanisms to address transnational cybersecurity threats as well as to share information for raising awareness and promoting best practices.<sup>289</sup> These existing cybersecurity threats include malicious intrusions or dissemination of malicious code that affect electronic networks.<sup>290</sup>

The eJSI proposal by Brazil provides that the states “shall endeavour” to build capacities to “prevent and respond” to cybersecurity threats with the adoption of “risk-based” approaches which help to mitigate threats and avoid trade restrictive and distortive outcomes.<sup>291</sup>

The eJSI proposal by China provides that the states “should”, as a recommendation, respect “internet sovereignty”, “exchange best practices”, “enhance electronic commerce security”, “deepen cooperation” as well as “safeguard cybersecurity.”<sup>292</sup>

The eJSI proposal by the US and UK provides that in light of the “evolving nature of cybersecurity threats”, the states need to recognize that “risk-based approaches” are more effective than “prescriptive regulatory approaches.”<sup>293</sup> Therefore, it states that the member states “shall endeavour to employ” and “shall encourage enterprises within its jurisdiction” to use “risk-based” approaches which relies on open and transparent industry standards or consensus-based standards as well as risk-management best practices to identify, detect and respond to the cybersecurity threats.<sup>294</sup>

We submit that the eJSI proposal on cybersecurity reflects the best cooperation and risk-based cautious approach. It builds on cooperation-led approaches in the CP-TPP and RCEP to incorporate risk-based shared capability development *via*: (a) early recognition of cybersecurity threats; (b) building capabilities and best practices; and (c) adopt risk-based approaches. We support the main message that risk-based cybersecurity policies are better than prescriptive ones.

It is interesting to note that China’s eJSI text proposal specifically mentions “to respect internet sovereignty” in the context of cybersecurity which has its own unique context in relation to China’s national approach on data protection and cybersecurity in general.<sup>295</sup>

---

<sup>286</sup> *Id.*

<sup>287</sup> *Id.*

<sup>288</sup> *Id.*

<sup>289</sup> *Id.*

<sup>290</sup> *Id.*

<sup>291</sup> eJSI, D.2. Cybersecurity, *supra* note 68, at 58.

<sup>292</sup> *Id.*

<sup>293</sup> *Id.*

<sup>294</sup> *Id.*

<sup>295</sup> See, e.g., Justin Sherman, How much Cyber Sovereignty is Too Much Cyber Sovereignty? (2019) Council on Foreign Relations, <https://www.cfr.org/blog/how-much-cyber-sovereignty-too-much-cyber-sovereignty>.

## F. SOURCE CODE

## F.I. DEFINITION OF “ALGORITHM” VS. “SOURCE CODE”

The eJSI proposal by Canada, Central African Republic, Japan, Mexico, Peru, Ukraine, US, and UK provides that “algorithm” “means a defined sequence of steps taken to solve a problem or obtain a result.”<sup>296</sup> No definition of source code is provided in the eJSI.<sup>297</sup> No such definition is provided in the CP-TPP either of “source code” or “algorithm.” The RCEP does not have a provision on “source code.” The eJSI proposal, and other relevant trade agreements on the USMCA and Singapore-Australia Digital Economy Agreement (SADEA) makes a distinction between “source code” and “algorithms” – suggesting that in trade negotiations they are different things, that an “algorithm” is embedded or expressed in a “source code.”<sup>298</sup>

The Oxford learner’s dictionaries provides that “source code” means “a computer program written in text form that must be translated into another form such as machine code before it can run on a computer” and “algorithm” means “a set of rules that must be followed when solving a particular problem.”<sup>299</sup> An “algorithm” is a more sensitive information than a “source code” at a commercial level although both types of information contain certain commercial value and therefore are commercially valuable and confidential for digital entrepreneurs.<sup>300</sup>

## F.II. PROHIBITION AGAINST TRANSFER OF SOURCE CODE

The eJSI mandates that:

“[N]o Party ‘shall’ require the transfer of, or access to, source code of software owned by a person/natural or juridical person of another Party/Member, or the transfer of, or access to an algorithm expressed in that source code, as a condition for the import, distribution, sale, or use of that software, or of products containing that software, in its territory.”<sup>301</sup>

Firstly, the obligation is mandatory.<sup>302</sup> The key obligation being that the states are prohibited from requiring “transfer or access” of “source code” or an “algorithm expressed in that source code” from a “person/natural or juridical person” of another member state as a prerequisite for the “import, distribution, sale or use of that software, or products containing

<sup>296</sup> eJSI, C.3 Business Trust, (1) Source Code, (1) ‘Algorithm’ means a defined sequence of steps, taken to solve a problem or obtain a result, *supra* note 68, at 48.

<sup>297</sup> *Id.*

<sup>298</sup> eJSI, *Supra* note 68 at C.3. Business Trust: (1) Source Code);

USTR, *US-Mexico-Canada (USMCA)*, <https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf>.

Department of Foreign Affairs and Trade of Australia, ‘Singapore-Australia Digital Economy Agreement’, <https://www.dfat.gov.au/trade/services-and-digital-trade/australia-and-singapore-digital-economy-agreement>.

<sup>299</sup> Oxford Learner’s Dictionaries, ‘Source Code’, <https://www.oxfordlearnersdictionaries.com/definition/english/source-code?q=source+code>.

<sup>300</sup> Oxford Learner’s Dictionaries, ‘Algorithms’, <https://www.oxfordlearnersdictionaries.com/definition/english/algorithm?q=algorithm>.

<sup>301</sup> eJSI, *supra* note 68 at C.3 Business Trust [Paragraph 2, is based on text proposals by Canada, CT, Japan, Mexico, Korea, PE, UA, US, Singapore, UK and EU].

<sup>302</sup> *Id.*

the software in its territory.”<sup>303</sup> Clearly, it prohibits the member states from requiring the “source code” or “algorithm” from the owner of a digital product as a condition for its “import, distribution, sale or use within its territory.”<sup>304</sup> Importantly, the use of different terms “import distribution, sale or use” of the digital product requires that such an obligation is adhered to at the time of importation of such a digital product to its commercial dissemination, sale and use within a jurisdiction.<sup>305</sup> Lastly, the provision provides terms for “software” or “of products containing the software” which means that any kind of digital product having a software with source code and algorithm is covered by the obligation.<sup>306</sup>

A similar obligation is provided in the CP-TPP under:

Article 14.17, Source Code: (1) No Party shall require the transfer of, or access to, source code of software owned by a person or another Party, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory.<sup>307</sup>

However, the definition does not refer to “algorithm” as separate commercially confidential information, rather it uses the word “source code” only.<sup>308</sup>

In essence, both the provisions on “source code” aim to prevent the states from forcing technology transfers in exchange for market access.<sup>309</sup> The firms which sell software or operate on digital platforms generally will have invested significant resources in developing the “source code” underpinning their products.<sup>310</sup> Considering this investment, the “source code” will often represent a major part of the value of such products, and any requirement to disclose it will either deter those firms from entering a market or erode their competitive advantage significantly by exposing them to the potential that other firms may gain access to their source code.<sup>311</sup>

An example involves IBM and Microsoft’s agreement with the China Information Technology Security Certification Center (CNITSEC) to share source code against security risks to Chinese citizens and clients.<sup>312</sup> Both IBM and Microsoft agreed to the demands for examination of source code by the Chinese government in order to secure their market space in China’s economy for a long-term basis.<sup>313</sup> Microsoft announced opening of a software review lab in partnership with the Chinese government in Beijing.<sup>314</sup> The IBM clarified that the agreement with China was “carefully constructed which allowed only the capability to

---

<sup>303</sup> *Id.*

<sup>304</sup> *Id.*

<sup>305</sup> *Id.*

<sup>306</sup> *Id.*

<sup>307</sup> CP-TPP, *supra* note 66 at Article 14.17: Source Code, (1) *No Party shall require the transfer of, or access to, source code of software owned by a person or another Party, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory.*

<sup>308</sup> *Id.*

<sup>309</sup> *Id.*

<sup>310</sup> *Id.*

<sup>311</sup> *Id.*

<sup>312</sup> *Id.*

<sup>313</sup> CP-TPP, *supra* note 66 at Article 14.17: Source Code, (1) *No Party shall require the transfer of, or access to, source code of software owned by a person or another Party, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory.*

<sup>314</sup> *Id.*

conduct limited demonstrations of specific aspects of our technology in highly secure, controlled IBM environments without external communication links”.<sup>315</sup> Similarly, Microsoft clarified that: “...the opening of CNITSEC Source Code Review Lab is a significant step in fulfilling Microsoft’s long-term commitment in China. To create a trustworthy computing environment is the goal of Microsoft.”<sup>316</sup>

### F.III. LIMITATION OF MASS-MARKET SOFTWARE PRODUCTS

The eJSI proposal by Korea states that: “...for the purposes of this Article, software subject to paragraph 2 is limited to ‘mass-market’ software or products containing such software and does not include software used for critical infrastructure.”<sup>317</sup> The CP-TPP has an identical obligation.<sup>318</sup>

The eJSI proposal by Korea and CP-TPP provides that the obligation prohibiting transfer of source code is “limited to ‘mass-market’ software or products containing such software” only.<sup>319</sup> Further, it explicitly excludes software meant for “critical infrastructure.”<sup>320</sup>

Firstly, the term “mass-market”, implies digital products which are “produced for very large numbers of people.”<sup>321</sup> There is no defined *de minimis* margin which can clarify what percentage of market constitutes or fulfils “limited to mass-market” condition.<sup>322</sup>

Secondly, the obligation does not apply to digital products meant for “critical infrastructure.”<sup>323</sup> Generally, the term critical infrastructure refers to such “infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital that their incapacitation or destruction would have a debilitating effect on national security, economic security, national public health or safety, or any combination therefore.”<sup>324</sup> Examples of such critical infrastructure may include: “defence industrial base sector”, “energy sector”, “health and public health sector”, “transportation systems sector”, “emergency services sector”, “financial services sector”, “food and agriculture sector”, “government facilities sector”, “nuclear reactors”, “materials sector”, “critical manufacturing sector”, “information technology sector”, etc.<sup>325</sup>

The eJSI and CP-TPP does not exclusively define the legal contours of the term critical infrastructure. As different states will have their own specific policy perspective or an understanding on what sectors constitute critical infrastructure, if the terminology is given into

---

<sup>315</sup> *Id.*

<sup>316</sup> *Id.*

<sup>317</sup> eJSI, *supra* note 68 at C.3. Business Trust, (1) Source Code, (3) *For the purposes of this Article, software subject to paragraph 2 is limited to mass-market software or products containing such software and does not include software used for critical infrastructure.* [Paragraph 3 is based on text proposals by Korea].

<sup>318</sup> CP-TPP, *supra* note 66 at Article 14.17, Source Code, (2) *For the purposes of this Article, software subject to paragraph 1 is limited to mass-market software or products containing such software and does not include software used for critical infrastructure.*

<sup>319</sup> *Id.*

<sup>320</sup> *Id.*

<sup>321</sup> *Id.*

<sup>322</sup> *Id.*

<sup>323</sup> *Id.*

<sup>324</sup> Australian Government, *Protecting Critical Infrastructure and Systems of National Significance: Draft Critical Infrastructure Asset Definition Rules*, CRITICAL INFRASTRUCTURE CENTRE (April 2021) <https://www.homeaffairs.gov.au/reports-and-pubs/files/critical-infrastructure-asset-definition-rules-paper.pdf>.

<sup>325</sup> *Id.*

the subjective proposals by the states at any given time, then it can dilute the legal effectiveness of such obligations on prohibition against transfer of source code in the long run. Hence, it is proposed that a proper legal definition of the term “critical infrastructure” in the context of digital trade is proposed by member states as well as discussed in the eJSI negotiations with its legal contours properly delineated. These developments are pertinent to the future revision of digital trade chapters in RTAs.

#### F.IV. EXEMPTIONS

There are exemptions applicable to the obligation against transfer of source code in the CP-TPP, RCEP, and eJSI. These exemptions provide that any judicial authority can require transfer of source code or algorithm in pursuance of a specific legal investigation or proceedings.<sup>326</sup> Voluntary transfer or grant of access to source code of software, or an algorithm expressed in that source code is acceptable. We only highlight here that there are applicable exemptions beyond the General and Security Exceptions to the obligation against transfer of source code in trade agreements. Due to space constraint, we do not attempt to discuss further relevant legal provisions in this article.

#### G. LOCATION OF COMPUTING FACILITIES

The two eJSI proposals, CP-TPP and RCEP provide a mandatory prohibition with the use of word “shall” on “location of computing facilities as a condition for conducting business in a jurisdiction.”<sup>327</sup> All the three digital trade agreements clarify that the states can only do so to achieve a legitimate public policy objective.<sup>328</sup> However, they provide for the exception of legitimate public policy objective supported with different legal terms as provided in the table below.

**Table 5: Location of Computing Facilities - CP-TPP vs. RCEP vs. eJSI**

CP-TPP – Article 14.13.3	RCEP – Article 12.14.3	eJSI Section B Openness and Electronic Commerce, B.2.: Flow of Information: (1) Cross-Border Transfer of Information by Electronic Means/Cross-Border Data Flows
'Nothing in this Article shall prevent a Party/Member from adopting or maintaining any measure that it considers necessary for the protection of its essential security interests.'	'Nothing in this Article <u>shall</u> prevent a Party from adopting or maintaining: (a) any measure inconsistent with paragraph 2 that it considers necessary to achieve a legitimate public policy objective - (FN 12: for the purposes of this subparagraph, the Parties affirm that the necessity behind the implementation of such legitimate public policy shall be decided by the implementing Party) – provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; or (b) any measure that it considers necessary for the protection of its essential	'Nothing in this article <u>shall</u> prevent a Party/Member from adopting or maintaining measures inconsistent with paragraph 5 'necessary' to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on the use or location of computing facilities greater than are necessary/required to achieve the objective.'

<sup>326</sup> The eJSI subparagraph 5 (Alt 1) as proposed by Canada, Japan, Mexico, US, and UK. CP-TPP, Article 14.7.3. The eJSI subparagraph 5 (Alt 2) as proposed by the EU. The eJSI proposal by Korea and Singapore. A similar provision under Article 14.17.4 of the CP-TPP. The eJSI, subparagraph 4, Alt 2 based on the text proposal by the EU and UK.

<sup>327</sup> CP-TPP, Article 14.13: Location of Computing Facilities, *supra* note 66,

<sup>328</sup> *Id.*

	<u>security interests. Such measures shall not be disputed by other Parties’.</u>	
--	---	--

The CP-TPP provides an exception against the obligation on the prohibition against location of computing facilities.<sup>329</sup> The exception applies to measures which the state considers “necessary for the protection of its essential security interests.”<sup>330</sup> There is a narrow scope for an exception as compared with “necessary to achieve a legitimate public policy objective” which is provided by the RCEP and eJSI.<sup>331</sup> The RCEP provides that any measure which the members consider to be necessary to protect both the “legitimate public policy objectives” and “essential security interests” are allowed within the scope of the exceptions.<sup>332</sup> It additionally provides that such measure should not be “applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade.”<sup>333</sup> Critically, it provides under footnote 12 that “the necessity behind the implementation of such legitimate public policy shall be decided by the implementing Party – provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; or (b) any measure that it considers necessary for the protection of its essential security interests. Such measures shall not be disputed by other Parties.”<sup>334</sup> This gives an overarching policy space to the states when compared to the CP-TPP and eJSI.<sup>335</sup> If a state considers any measure to be necessary to achieve a legitimate public policy objective or essential security interest, then as per footnote 12, the decision by the member state satisfies the necessity requirement.<sup>336</sup> Further, given that the RCEP states that “such measures shall not be disputed by Parties”, it is clearly not subject to formal dispute settlement between the Parties or an objective adjudication scrutiny.<sup>337</sup>

The eJSI finds a middle-path between the narrow scope of CP-TPP and the broad scope of RCEP by clarifying that such measures which are “necessary to achieve a legitimate public policy objective” are covered within the scope of the exception.<sup>338</sup> However, it does not specifically provide for the phrase “essential security interest” like the CP-TPP or RCEP.<sup>339</sup> Similar to the RCEP, eJSI clarifies that any such measure “is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade.”<sup>340</sup> Additionally, it clarifies that such measures can be applied “provided that it does not impose restrictions on the use or location of computing facilities ‘greater than are necessary/required to’ achieve the objective.”<sup>341</sup> We note in the last subparagraph that the member states are undecided on whether to include “necessary” or “required to achieve the legitimate objective test” for any restrictions on the use or location of computing facilities.<sup>342</sup> Clearly, “necessity” is a narrow test as compared to “greater than required to achieve” test.<sup>343</sup>

---

<sup>329</sup> *Id.*

<sup>330</sup> *Id.*

<sup>331</sup> *Id.*

<sup>332</sup> *Id.*

<sup>333</sup> CP-TPP, Article 14.13: Location of Computing Facilities, *supra* note 66,.

<sup>334</sup> *Id.*

<sup>335</sup> *Id.*

<sup>336</sup> *Id.*

<sup>337</sup> *Id.*

<sup>338</sup> *Id.*

<sup>339</sup> CP-TPP, Article 14.13: Location of Computing Facilities, *supra* note 66.

<sup>340</sup> *Id.*

<sup>341</sup> *Id.*

<sup>342</sup> *Id.*

<sup>343</sup> *Id.*



The “greater than required test” gives a higher margin of deference to regulators as compared to the necessity test.<sup>344</sup> The “greater than” implies a comparative legal test.<sup>345</sup> This comparative test necessarily requires the impugned measure to be assessed against a comparator, which in this context would be a less trade restrictive means of achieving the legitimate objective.<sup>346</sup>

On the location of computing facilities provision there are divergences among the CP-TPP, RCEP, and eJSI proposals. We understand that the CP-TPP provides that location of computing facilities is only allowed for the protection of essential security interests whereas the RCEP and eJSI provides that it covers protection of “legitimate public policy objectives.” We highlight a recurring issue that there is no clear definition of such core concepts such as essential security interests, critical infrastructure, and legitimate public policy objectives, which can help stakeholders be certain of the practical meaning of such provisions in the digital trade domain.

#### H. CUSTOMS DUTIES

The CP-TPP, RCEP, and eJSI provides for prohibition against the imposition of customs duties on electronic transmissions.<sup>347</sup> The CP-TPP and eJSI proposal by Japan, U.S., Singapore, Hong Kong, Brazil, Korea, New Zealand, Canada, E.U., Ukraine, Russia, and U.K. provides a mandatory prohibition against the imposition of customs duties on both “electronic transmission and content transmitted electronically.”<sup>348</sup> We note that Japan, Canada, New Zealand, and Singapore are also members of the CP-TPP, so they naturally support an identical obligation in the eJSI negotiations.<sup>349</sup>

On the contrary, the eJSI proposal by Indonesia does not use the word “shall” to indicate that the obligation against imposition of customs duties is mandatory.<sup>350</sup> Rather, it provides that the “parties agree to maintain the current practice of not imposing customs duties.”<sup>351</sup> Further, it specifically excludes “content transmitted electronically” from the obligation apart from electronic transmission.<sup>352</sup> It clarifies that the member states can adjust their practice as per developments in the WTO ministerial meetings or agreements relating to the work program on e-commerce.<sup>353</sup> Critically, it provides that the member states “shall not” be precluded from applying customs procedures for public policy purposes.<sup>354</sup>

Importantly, the eJSI proposal by China and RCEP does not widen the scope of the moratorium to include “content transmitted electronically” like Indonesia.<sup>355</sup> The 1998 Declaration on Global Electronic Commerce’s operative text provides that: “Members will

---

<sup>344</sup> *Id.*

<sup>345</sup> CP-TPP, Article 14.13: Location of Computing Facilities, *supra* note 66.

<sup>346</sup> *Id.*

<sup>347</sup> CP-TPP, Article 14.3: Customs Duties, *supra* note 66,

<sup>348</sup> *Id.*

<sup>349</sup> *Id.*

<sup>350</sup> *Id.*

<sup>351</sup> *Id.*

<sup>352</sup> *Id.*

<sup>353</sup> CP-TPP, Article 14.3: Customs Duties, *supra* note 66.

<sup>354</sup> *Id.*

<sup>355</sup> *Id.*

continue their current practice of not imposing customs duties on electronic transmissions.”<sup>356</sup> Subsequent decisions on moratorium has replicated the operative text.<sup>357</sup>

There is a disagreement among the WTO members as to whether the scope of moratorium includes “content transmitted electronically” apart from “electronic transmission.”<sup>358</sup> Indonesia has submitted its interpretation to the WTO MC11 on the scope of the moratorium as follows:

“In regard to the discussion on the moratorium on customs duties on electronic transmissions, it is our understanding that such moratorium shall not apply to electronically transmitted goods and services. In other words, the extension of the moratorium applies only to the electronic transmission and not to products or content which are submitted electronically.”<sup>359</sup>

This interpretation implies that member states can impose custom duties on content transmitted electronically and not electronic transmission (bits and bytes).

India and South Africa have collaboratively questioned the economic viability of a broad scope of the moratorium.<sup>360</sup> They clarify that the scope of digitized and digitizable goods can be classified into five broad categories: “films, printed matter, video games, software, sound and music.”<sup>361</sup> This list is expected to expand with new digital technologies.<sup>362</sup> They underline that during 1998 when the moratorium was agreed, the digital economy was not as developed as it is today.<sup>363</sup> Specifically, with the advent of the 3D printing, big data, and artificial intelligence, the need to reconsider moratorium on digital products becomes necessary.<sup>364</sup> They argue that without a proper delineation of the scope of moratorium, the developing countries will lose the policy tool of tariffs for their economic development.<sup>365</sup> Specifically, with the 3D printing technology apart from new technologies in the industry 4.0, the meticulously negotiated GATT bound rates, which are traditionally higher in developing countries, will become zero for their digitized counterparts.<sup>366</sup>

An UNCTAD research paper estimated that on a mere identification of five types of digitizable goods as provided above, the tariff revenue loss of more than \$10 billion will be borne by the WTO member states—95% of it will impact the developing countries.<sup>367</sup> Apart from their concerns on the scope of moratorium on content transmitted electronically, they

<sup>356</sup> World Trade Organization, *Ministerial Declaration on Global Electronic Commerce* of 20 May 1998, WTO Doc. WT/MIN(98)DEC/2 (May 25, 1998), <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=Q:/WT/MIN98/DEC2.pdf&Open=True>.

<sup>357</sup> Committee on Trade and Development 118th Session, *Note on the Meeting of 20 June 2022*, WTO Doc. WT/COMTD/M/118 (July 15, 2022), <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/COMTD/M118.pdf&Open=True>.

<sup>358</sup> *Id.*

<sup>359</sup> WTO General Council, *Work Programme on Electronic Commerce*, WTO Doc. WT/GC/W/833 (November 8, 2021), <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/GC/W833.pdf&Open=True>.

<sup>360</sup> *Id.*

<sup>361</sup> *Id.*

<sup>362</sup> *Id.*

<sup>363</sup> *Id.*

<sup>364</sup> *Id.*

<sup>365</sup> *Id.*

<sup>366</sup> *Id.*

<sup>367</sup> Rashmi Banga, *Should digitally delivered products be exempted from customs duties*, UNCTAD (July 16, 2020), <https://unctad.org/news/should-digitally-delivered-products-be-exempted-customs-duties>.

explicitly reject any interpretation to broaden the scope of the moratorium which includes “services”:

“The moratorium covering digitizable goods is already a major challenge since it is about bringing a large portion, and in time, maybe even the majority of NAMA tariffs to zero. For this reason, according to the submissions by India and South Africa, the moratorium must be reconsidered as digitization becomes the mode of commerce. It would be unthinkable for the scope to go beyond this to also include other forms of digitized trade, an issue which has not been discussed.”<sup>368</sup>

The CP-TPP and RCEP clarify that this obligation “shall not preclude” any member state from imposing “internal taxes, fees or other charges.”<sup>369</sup> However, the CP-TPP states that this exemption is applicable for charges on content transmitted electronically whereas the RCEP provides “charges on electronic transmissions.”<sup>370</sup> Clearly, the RCEP does not prohibit customs duties on electronic transmissions contrary to CP-TPP.<sup>371</sup>

The eJSI proposal by Singapore, Hong Kong, Ukraine, Korea, New Zealand, Canada, Brazil, Russia, Indonesia, China and UK states that the member states “shall not be precluded” from imposing “internal taxes, fees[,] or other internal charges” or “electronic transmissions which include the/any content transmitted electronically.”<sup>372</sup> Additionally, it states that such duty, fee, or charge is applicable to “revenue and profit generated from digital trade” as well.<sup>373</sup> In both instances, the duty, fees, or charges need to be in compliance with the “WTO Agreement/eJSI” and “on a non-retroactive basis.”<sup>374</sup>

It is a novel provision. Firstly, both electronic transmission and content transmitted electronically are subject to duties, fees, or charges. Secondly, it subjects revenue and profit generated from digital trade to plausible duties, fees or charges as well. It clarifies that any such charges on covered issues should be in compliance with the obligations under the WTO agreement and eJSI. Critically, it provides that this provision applies on a non-retroactive basis. The eJSI proposal by the US provides for the same obligation—“member states shall not be precluded from imposing internal taxes on electronic transmissions which include content transmitted electronically.”

There is a divergence among states within and outside the WTO on customs duties which should be levied on content transmitted online vs. electronic transmissions. Indonesia, India, and South Africa have raised serious concerns that if the WTO moratorium on e-commerce includes content transmitted online then the various physical goods which are being digitalized will be able to cross borders without any customs duties which can be levied by developing and least-developed countries.<sup>375</sup> This has a serious consequence for the ability of developing and least-developed countries to use tools such as tariffs.<sup>376</sup>

---

<sup>368</sup> *Id.*

<sup>369</sup> CP-TPP, *supra* note 66; RCEP, *supra* note 67; eJSI, *supra* note 68.

<sup>370</sup> *Id.*

<sup>371</sup> *Id.*

<sup>372</sup> *Id.*

<sup>373</sup> *Id.*

<sup>374</sup> *Id.*

<sup>375</sup> Banga, *supra* note 367.

<sup>376</sup> *Id.*

We noted above that the CP-TPP and eJSI proposal by Japan, US, Singapore, Hong Kong, Brazil, Korea, New Zealand, Canada, EU, Ukraine, Russia, and UK provide a mandatory prohibition against customs duties on both electronic transmissions and content transmitted electronically. The RCEP and eJSI proposal by China as discussed above does not broaden the scope of moratorium to include content transmitted electronically. The eJSI proposal by Indonesia understandably makes the prohibition against customs duties non-binding and provides that the members should follow the developments and accordingly practice their imposition of customs duties in the digital domain. Further, the CP-TPP and RCEP provide for exemptions against the prohibition. However, the CP-TPP expressly limits the applicability of exemptions to content transmitted electronically whereas the RCEP broadly covers charges on electronic transmissions. The RCEP's approach is supported by the eJSI proposal as led by China, Singapore, and UK.

We submit that the customs duties in the field of digital trade is a very sensitive issue. There is no simple solution, and we don't presume to know the best solution. It is an issue which needs collaboration and dialogue based on good faith within and outside the WTO so that the essential goals of digital trade liberalization are secured with necessary policy space for the economic development of developing and least developed countries.

## I. GENERAL AND SECURITY EXCEPTIONS

### I.I. GENERAL EXCEPTIONS

The GATT 1994 and GATS provide for general exceptions under the WTO legal framework.<sup>377</sup> The RTAs have usually incorporated the provisions *mutatis mutandis* or adapted to the design of the general exceptions under the GATT 1994 and GATS. In a similar manner, the CP-TPP digital trade chapter provides that paragraphs (a), (b), and (c) of article XIV GATS are incorporated and made part of the digital trade chapter.<sup>378</sup> The RCEP digital trade chapter as well as the eJSI incorporates both the Articles XX GATT 1994 and XIV GATS *mutatis mutandis*.<sup>379</sup> Hence, it is essential to understand the general exceptions under GATT 1994 and GATS in the WTO framework before we discuss the specific general and security exception provisions in the CP-TPP, RCEP, and eJSI.

The general exceptions under GATT 1994 and GATS provide for a chapeau which outlines the critical test that a measure "is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between the countries where the ('same' - GATT)/('like' - GATS) conditions prevail, or a disguised restriction on ('international trade' - GATT)/('trade in services' - GATS)".<sup>380</sup> We note that the legal test of chapeau under both the GATT 1994 and GATS is similar but not identical. The evenhandedness test to ensure no discrimination "between countries" where "same or like conditions prevail" is narrow in scope in GATS as compared to GATT 1994. As the GATT 1994 uses the term "same" and GATS uses the term "like" for the even-handedness test.<sup>381</sup>

The various subparagraphs below the main chapeau of both the GATT 1994 and GATS provide for an illustrative list of legitimate public policy objectives which are covered within

---

<sup>377</sup> GATT 1994, Article XX: General Exceptions. GATT 1994, Article XXI: Security Exceptions.

<sup>378</sup> CP-TPP, Chapter 29, Exceptions and General Provisions, Section A: Exceptions, Article 29.1, *supra* note 66.

<sup>379</sup> *Id.*

<sup>380</sup> *Id.*

<sup>381</sup> *Id.*

the scope of the general exceptions.<sup>382</sup> The list of such objectives differ in their expression between the GATT 1994 and GATS.<sup>383</sup> Specifically, in the subparagraph on measures “necessary to protect public morals”, we see that the GATT 1994 does not include “to maintain public order” as compared to GATS.<sup>384</sup> Further, the footnote five to GATS clarify that “the public order exception may be invoked only where genuine and sufficiently serious threat is posed to one of the fundamental interests of the society.”<sup>385</sup> Thus, we note that the illustrative list of legitimate public policy objectives is clearly defined in the GATS as compared to GATT 1994.<sup>386</sup> The subparagraph (c) of GATS Article XIV is the most relevant legitimate public policy objective after “public morals” and “public order” for digital trade.<sup>387</sup> The subparagraph (c) provides that all measures which are “necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this agreement - are covered within the scope of general exceptions.”<sup>388</sup> Specifically, it outlines three kinds of laws or regulations which are explicitly covered: (a) prevention of deceptive and fraudulent practices or to deal with the effects of a default on service contracts, (b) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts, and (c) safety.<sup>389</sup>

The GATS clearly supersedes GATT for its relevance in the context of digital trade as it includes within the scope of general exception, all measures which are necessary “for the protection of privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts.”<sup>390</sup> This specific topic of legitimate policy objective is very pertinent in the sphere of digital trade.<sup>391</sup> Overall, the illustrative list of legitimate public policy objectives under GATS have an applicable and relevant list of legitimate public policy objectives vis-à-vis GATT on digital trade.<sup>392</sup>

The CP-TPP incorporates subparagraph (a), (b), and (c) of GATS *mutatis mutandis* whereas the RCEP and eJSI as proposed by Canada, China and Japan incorporates the whole provision on general exceptions under GATT 1994 and GATS *mutatis mutandis*.<sup>393</sup> However, we note that the eJSI proposal by Canada, China, and Japan provides a set list of legitimate public policy concerns in the context of digital trade as follows:

- a) cybersecurity;
- b) safeguarding cyberspace sovereignty;
- c) protecting the lawful rights and interests of its citizens;
- d) juridical persons and other organisations; and
- e) achieving other legitimate public policy objectives.<sup>394</sup>

---

<sup>382</sup> *Id.*

<sup>383</sup> *Id.*

<sup>384</sup> CP-TPP, Chapter 29, Exceptions and General Provisions, Section A: Exceptions, Article 29.1, *supra* note 66.

<sup>385</sup> *Id.*

<sup>386</sup> *Id.*

<sup>387</sup> *Id.*

<sup>388</sup> *Id.*

<sup>389</sup> *Id.*

<sup>390</sup> CP-TPP, Chapter 29, Exceptions and General Provisions, Section A: Exceptions, Article 29.1, *supra* note 66.

<sup>391</sup> *Id.*

<sup>392</sup> *Id.*

<sup>393</sup> *Id.*

<sup>394</sup> eJSI, (6) General Exceptions, (Alt 1), *supra* note 68.

It provides for a test similar to the chapeau test under the GATS excluding the even-handedness test by stating:

“ . . . provided that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade and are no more than necessary to achieve the objectives”.<sup>395</sup>

Contrary to the above proposal, the eJSI proposal by Brazil provides for a chapeau test similar to the GATS including the even-handedness test by stating:

“Subject to the requirement that such measures are ‘not applied in a manner’ which would constitute a means of arbitrary or unjustifiable discrimination between countries where ‘like conditions prevail’, or a disguised restriction on trade”.<sup>396</sup>

In providing the phrase “disguised restriction on trade”, the eJSI proposal by Brazil adds “and cross-border transfer of information by electronic means.”.<sup>397</sup> Hence, we note that Brazil’s eJSI proposal is very different from other proposals.<sup>398</sup> The Brazil’s eJSI proposal provides an illustrative list of legitimate public policy measures: “(a) necessary to protect public morals or to maintain public order; (b) necessary to ensure the equitable or effective imposition or collection of direct taxes in respect of trade through electronic means; (c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this agreement including those relating to: (i) the prevention of deceptive and fraudulent practices; (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts; and (iii) safety.”<sup>399</sup> We note that the two list of legitimate public policy objectives are directly adopted from the GATS.<sup>400</sup>

Overall, we note that the eJSI proposals are more innovative and elaborate in design as even after incorporating the general exceptions from both GATT 1994 and GATS *mutatis mutandis*, the eJSI proposals refine the provisions to suit the context of digital trade. It is relevant to list all the legitimate public policy objectives from the above discussion which are highly pertinent for the regulation of digital trade in international economic law.

**Table 6: List of pertinent legitimate public policy objectives for digital trade –  
GATT 1994 vs. GATS vs. eJSI**

GATT 1994	GATS	e-JSI
Necessary to protect public morals.	Necessary to protect public morals or to maintain public order (FN 5: The public order exception may be invoked only where a genuine and sufficiently serious threat is posed to one of the fundamental interests of society).	<ul style="list-style-type: none"> <li>Text proposal by Canada, China, and Japan:</li> </ul> Guaranteeing cybersecurity;

<sup>395</sup> *Id.*

<sup>396</sup> *Id.*

<sup>397</sup> *Id.*

<sup>398</sup> *Id.*

<sup>399</sup> *Id.*

<sup>400</sup> *Id.*

		<p><i>Safeguarding cyberspace sovereignty;</i></p> <p><i>Protecting the lawful rights and interests of its citizens, juridical persons, and other organizations;</i></p> <p><i>Achieving other legitimate public policy objectives.</i></p>
<i>Necessary to protect human, animal or plant life or health.</i>	<i>Necessary to protect human, animal or plant life or health.</i>	<ul style="list-style-type: none"> <li>• <u>Text proposal by Brazil:</u></li> </ul> <p><i>Necessary to protect public morals or to maintain public order.</i></p> <p><i>Necessary to ensure the equitable or effective imposition or collection of direct taxes in respect of trade through electronic means.</i></p> <p><i>Necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to:</i></p> <p><i>(i) the prevention of deceptive and fraudulent practices;</i>  <i>(ii) the protection of the privacy of individuals in relation to the proceeding and dissemination of personal data and the protection of confidentiality of individual records and accounts; and</i>  <i>(iii) safety.</i></p>
<i>Necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement, including those relating to customs enforcement, the enforcement of monopolies operated under paragraph 4 of article II and Article XVII, the protection of patents, trademarks and copyrights, and the prevention of deceptive practices.</i>	<i>Necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to: (i) the prevention of deceptive and fraudulent practices or to deal with the effects of a default on service contracts; (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts; (iii) safety.</i>	
<i>Relating to the products of prison labour.</i>	<i>(d) inconsistent with Article XVII, provided that the difference in treatment is aimed at ensuring the equitable or effective imposition or collection of direct taxes in respect of</i>	

	services or service suppliers of other Members.	
Relating to the conservation of exhaustible natural resources if such measures are made effective in conjunction with restrictions on domestic production or consumption.	(e) inconsistent with Article II, provided that the difference in treatment is the result of an agreement on the avoidance of double taxation or provisions on the avoidance of double taxation in any other international agreement or arrangement by which the Member is bound.	
Involving restrictions on exports of domestic materials necessary to ensure essential quantities of such materials is held below the world price as part of a government stabilization plan; Provided that such restrictions shall not operate to increase the exports of or the protection afforded to such domestic industry, and shall not depart from the provisions of this Agreement relating to non-discrimination.		

**Source:** Author's compilation from the legal texts<sup>401</sup>.

The legitimate public policy objective as per the WTO jurisprudence refers to “an aim or target that is lawful, justifiable, or proper” inclusive of objectives mentioned and protected elsewhere in the treaty.<sup>402</sup> In the context of the WTO, there are far fewer explicit endorsement of values and objectives as compared to the CP-TPP.<sup>403</sup> The term endorsement of values and objectives refers to the preambular recitals.<sup>404</sup> It needs to be emphasised that we should not conflate ambiguity with abstract, as the abstract nature of preambular values does not make them ambiguous.<sup>405</sup> The term finds application in particular fact patterns and in the abstract it would be difficult to delineate every single objective which could conceivably qualify as legitimate.<sup>406</sup> This difficulty does not necessarily make the language ambiguous.<sup>407</sup>

It is difficult to apply these tests in abstract as they depend on the detail of a given measure.<sup>408</sup> The test works so that a measure will be considered arbitrary or disguised if it bears no rational connection to the legitimate objective.<sup>409</sup> The contextual elements of the CP-TPP can shed light on what comprises arbitrary or unjustifiable discrimination in any given instance. For example, discrimination in the form of a competitive advantage to an indigenous community which directly results from the application of a given measure in pursuit of the legitimate objective would appear unlikely to be arbitrary, unjustifiable, or disguised, particularly if there is no less trade-restrictive alternative.<sup>410</sup>

<sup>401</sup> *Id.*

<sup>402</sup> Ministry of Justice, *The Report on the Comprehensive and Progressive Agreement for TPP* (2021) 135-137, [https://forms.justice.govt.nz/search/Documents/WT/wt\\_DOC\\_178856069/CPTTP%20W.pdf](https://forms.justice.govt.nz/search/Documents/WT/wt_DOC_178856069/CPTTP%20W.pdf).

<sup>403</sup> *Id.*

<sup>404</sup> *Id.*

<sup>405</sup> *Id.*

<sup>406</sup> *Id.*

<sup>407</sup> *Id.*

<sup>408</sup> Ministry of Justice, *supra* note 402.

<sup>409</sup> *Id.*

<sup>410</sup> *Id.*



## I.II. SECURITY EXCEPTIONS

The CP-TPP, RCEP, and eJSI provide that the agreement “shall not be construed” to require a “party to furnish any information the disclosure of which it considers contrary to its essential security interests.”<sup>411</sup> Further, they provide that nothing in this agreement “shall preclude” any member state from taking any “action” which it considers necessary for the protection of its “essential security interests.”<sup>412</sup> The concept of essential security interests is then further elaborated in GATT 1994, GATS, RCEP, and eJSI.<sup>413</sup> The CP-TPP does not elaborate the concept of essential security interest compared to other agreements.<sup>414</sup> “Maintenance of international peace and security” is excluded or treated as a different concept from essential security interest.<sup>415</sup> An elaboration of essential security interest is provided in the comparative table below to appreciate the varied expressions.

Clearly, the RCEP has an elaborate legal provision for a “security exception” as compared to both the CP-TPP and, specifically, eJSI proposals by China and Brazil. The RCEP is more advanced than GATT 1994 and GATS on outlining the concept of “essential security interests” by including “critical public infrastructure” whether publicly or privately-owned.<sup>416</sup> Critically, the RCEP expands the scope of “essential security interest” to expressly include public or private critical public infrastructure by stating “so as to protect critical public infrastructures” including “communications, power, and water infrastructures”, both public and privately-owned.<sup>417</sup> Further, the RCEP provides that measures relating to “fissionable and fusionable materials or the material from which they are derived, relating to the traffic in arms, ammunition and implements of war and to such traffic in goods and materials, or relating to the supply of services, as carried on directly or indirectly for the purpose of supplying or provisioning a military establishment” are also covered within the scope of the “essential security interests”.<sup>418</sup> This elaboration is found in GATT 1994 and Article XIV*bis* in GATS.<sup>419</sup>

The eJSI proposal by Brazil provides an illustrative list of security measures on transfer of information or taking any action in pursuance of essential security interests.<sup>420</sup> It states that:

Nothing in this Agreement shall be construed: (a) to require any [Party/Member] to furnish any information, the disclosure of which it considers (b) contrary to its essential security interests; or (c) to prevent any [Party/Member] from taking any action which it considers necessary for the protection of its essential security interests: (i) relating to the cross-border transfer of information carried out directly or indirectly for military

---

<sup>411</sup> CP-TPP, Chapter 29, Exceptions and General Provisions, Article 29.2: Security Exception, <https://www.dfat.gov.au/sites/default/files/29-exceptions-and-general-provisions.pdf>; RCEP, Chapter 17: General Provisions and Exceptions, 17.13: Security Exceptions, <https://www.dfat.gov.au/sites/default/files/rcep-chapter-17.pdf>; eJSI, Annex 1: Scope and General Provisions, (7) Security exception, [https://www.bilaterals.org/IMG/pdf/wto\\_plurilateral\\_ecommerce\\_draft\\_consolidated\\_text.pdf](https://www.bilaterals.org/IMG/pdf/wto_plurilateral_ecommerce_draft_consolidated_text.pdf).

<sup>412</sup> *Id.*

<sup>413</sup> *Id.*

<sup>414</sup> *Id.*

<sup>415</sup> *Id.*

<sup>416</sup> *Id.*

<sup>417</sup> *supra* note 416.

<sup>418</sup> *Id.*

<sup>419</sup> General Agreement on Tariffs and Trade, Oct. 30, 1947, 61 Stat. A-11, 55 U.N.T.S. 194 [hereinafter GATT]; General Agreement on Trade in Services, Apr. 15, 1994, art. XIV, 1869 U.N.T.S. 183 [hereinafter GATS].

<sup>420</sup> Comprehensive and Progressive Agreement for Trans-Pacific Partnership, ch. 29, Exceptions and General Provisions, art. 29.2 [hereinafter CP-TPP]. <https://www.dfat.gov.au/sites/default/files/29-exceptions-and-general-provisions.pdf>.

communication; (ii) taken in time of war or other emergency in international relations; or (iii) to prevent any [Party/Member] from taking any action under the United Nations Charter for the maintenance of international peace and security.

We note that the eJSI proposal further expands the scope of essential security interests beyond RCEP to include measures “relating to the cross-border transfer of information carried out directly or indirectly for military communication.”<sup>421</sup> All the digital trade agreements include within the security exceptions, the measures taken in pursuance of maintaining international peace and security.<sup>422</sup>

The CP-TPP security exception is not as specific as RCEP or eJSI. As eJSI applied the security exception under Article XXI GATT 1994 and Article XIV***bis*** of the GATS *mutatis mutandis*.<sup>423</sup> The important legal phrases in eJSI include: (a) essential security interest in all the three digital trade agreements; (b) critical public infrastructure in RCEP and eJSI; (c) in pursuance of its obligations under the UN Charter for the maintenance of peace and security in RCEP and eJSI, and (d) time of war or other international emergencies in international relations.<sup>424</sup>

The RCEP and eJSI’s security exception proposal by China and Brazil provides that the member states are not required to furnish any information “the disclosure of which it *considers* contrary to its essential security interests.” The CP-TPP similarly provides “disclosure of which it *determines* to be contrary to its essential security interests.”<sup>425</sup> Similarly, Article XXI:(a) GATT 1994 and Article XIV***bis*** GATS also provide for a provision similar to RCEP and two eJSI proposals by China and Brazil.<sup>426</sup>

The CP-TPP, RCEP, and eJSI proposals by China and Brazil provide that the security exception allows members to “take action which it considers ‘necessary’ for the protection of its essential security interests.”<sup>427</sup> However, they provide a varied list of measures which are specifically covered by the phrase “essential security interests”.<sup>428</sup> Importantly, the RCEP is unique as it clarifies under footnote 7 that “for greater certainty, this includes critical public infrastructure whether publicly or privately owned, including communications, power, and water infrastructures.”<sup>429</sup> The CP-TPP, RCEP, and eJSI do not provide a specific legal definition of the term “essential security interests.” The CP-TPP does not elaborate the term “essential security interests”, rather after providing that the members can take actions “necessary”, it states “for the fulfilment of its obligations with respect to the maintenance or restoration of international peace or security, or the protection of its own essential security interests.”<sup>430</sup>

---

<sup>421</sup> GATT, Oct. 30, 1947, art. XXI, 55 U.N.T.S. 194; GATS, Apr. 15, 1994, art. XIV *bis*, 1869 U.N.T.S. 183.

<sup>422</sup> CP-TPP, ch. 29, Exceptions and General Provisions, art. 29.2. <https://www.dfat.gov.au/sites/default/files/29-exceptions-and-general-provisions.pdf>.

<sup>423</sup> *Id.*

<sup>424</sup> *Id.*

<sup>425</sup> *Id.*

<sup>426</sup> GATT, Oct. 30, 1947, art. XXI, 55 U.N.T.S. 194; GATS, Apr. 15, 1994, art. XIV *bis*, 1869 U.N.T.S. 183.

<sup>427</sup> CP-TPP, ch. 29, Exceptions and General Provisions, art. 29.2. <https://www.dfat.gov.au/sites/default/files/29-exceptions-and-general-provisions.pdf>.

<sup>428</sup> *Id.*

<sup>429</sup> Regional Comprehensive Economic Partnership, Nov. 15, 2020, art. 17.13, 2689 U.N.T.S. 3 [hereinafter RCEP].

<sup>430</sup> CP-TPP, ch. 29, Exceptions and General Provisions, art. 29.2. <https://www.dfat.gov.au/sites/default/files/29-exceptions-and-general-provisions.pdf>.

The RCEP, on the contrary, provides a list of specific measures and actions which can be taken by the member if it is necessary for the protection of its essential security interests, specifically: (a) “relating to fissionable and fusionable materials or the materials from which they are derived”; (b) “relating to the traffic in arms, ammunition and implements of war and to such traffic in other goods and materials, or relating to the supply of services, as carried on directly or indirectly for the purposes of supplying or provisioning a military establishment”; (c) “taken so as to protect critical public infrastructures”; or (d) “taken in time of national emergency or war or other emergency in international relations” or “to prevent any Party from taking any action in pursuance of its obligations under the UN Charter for the maintenance of international peace and security.”<sup>431</sup> The list of specific contexts elaborated in RCEP is adopted from the GATT 1994 and GATS; however, the novelty is found in RCEP with “taken so as to protect critical public infrastructures” and the explanatory footnote 7.<sup>432</sup>

In similar fashion, the eJSI proposals by Brazil also elaborates specific context for the applicability of the security exception as regards the protection of essential security interests.<sup>433</sup> It provides that such measures include: “relating to the cross-border transfer of information carried out directly for military communication”; “taken in time of war or other emergency in international relations”; or “to prevent any Party/Member from taking any action in pursuance of its obligations under the UN Charter for the maintenance of international peace and security.”<sup>434</sup> The text proposal by Brazil is similar to the security exceptions we note under the GATT 1994 and GATS, except with new additions like “relating to cross-border transfer of information carried out directly for military communication.”<sup>435</sup> The eJSI proposal by China does not provide elaboration on the application of essential security interests, rather it provides a subparagraph (c)(iii) to add nothing in this agreement shall be construed “to prevent any [Party/Member] from taking any action in pursuance of its obligations under the United Nations Charter for the maintenance of international peace and security.”<sup>436</sup>

The CP-TPP incorporates paragraphs (a), (b), and (c) of Article XIV*bis* GATS into its digital trade chapter and RCEP as well as eJSI incorporates both Article XX GATT 1994 and XIV GATS, *mutatis mutandis*. The CP-TPP has a brief provision on security exceptions. In this article, we have outlined and tabulated the most pertinent list of legitimate public policy objectives covered by various provisions on general and security exceptions provided by the GATT 1994, GATS, CP-TPP, RCEP as well as eJSI proposals. We underline the relevance of GATS general and security exceptions which provide significant legal content in the context of digital trade for future deliberations, especially on the protection of personal data/information. The eJSI proposal by Canada, China, and Japan provide a relevant list of legitimate public policy concerns in the context of digital trade, e.g., cybersecurity policies, cyberspace sovereignty safeguards, etc. We specifically recommend the eJSI proposal by Brazil, China, and Japan on general and security exceptions for digital trade. It is highly innovative and relevant for future deliberations on digital trade.

In the context of security exceptions, the RCEP has a more elaborate legal provision for security exception as compared to the CP-TPP and eJSI proposals by China and Brazil. The

---

<sup>431</sup> RCEP, Nov. 15, 2020, art. 17.13, 2689 U.N.T.S. 3.

<sup>432</sup> *Id.*

<sup>433</sup> CP-TPP, ch. 29, Exceptions and General Provisions, art. 29.2. <https://www.dfat.gov.au/sites/default/files/29-exceptions-and-general-provisions.pdf>.

<sup>434</sup> *Id.*

<sup>435</sup> *Id.*

<sup>436</sup> *Id.*

RCEP is advanced in that it defines the concept of “essential security interests” by including “critical public infrastructure whether publicly or privately owned.” We commend the eJSI proposal by Brazil on security exception as it goes further than the RCEP to expand the scope of essential security interests by including measures “relating to the cross-border transfer of information carried out directly or indirectly for military communications.” We note that all the digital trade agreements include security exception measures taken in pursuance of maintaining international peace and security which is relevant in light of the cyberwarfare threats in the context of the recent Ukraine crisis.

The trade negotiators should properly define and clarify essential conceptual terms such as “essential security interests”, “legitimate public policy objectives”, “critical public infrastructure”, and maybe even “international peace and security”, as although these terms have a traditionally established meaning we need to appreciate the new digital context in which such established legal principles should operate.

#### J. TREATY OF WAITANGI WAIVER

The Treaty of Waitangi waiver<sup>437</sup> is an important provision in both the CP-TPP and RCEP in terms of indigenous community data governance issues. The eJSI does not have such a provision. It provides flexibility to New Zealand to adopt measures to accord more favourable treatment to the indigenous community – “Māori relating to issues covered by the obligations under the digital trade chapter provided that such measures are not adopted as a means of arbitrary or unjustified discrimination against persons of other Parties or as a disguised restriction on trade in goods, trade in services or investment.”<sup>438</sup> The waiver clarifies that any matter relating to the interpretation of rights and obligations under the Treaty of Waitangi arising under the agreement shall not be subject to the dispute settlement mechanism.<sup>439</sup> A trade panel can only be established to determine whether the measure is inconsistent with the rights of any member state.<sup>440</sup> Lastly, the provision on “traditional knowledge and traditional cultural expression”, unique to the CP-TPP, emphasizes that each member state may establish appropriate measures to respect, preserve, and promote traditional knowledge and cultural expressions.<sup>441</sup>

In the context of the Waitangi Tribunal findings which revolve around this specific provision on the Treaty of Waitangi waiver there was a genuine concern raised by the indigenous community on the lack of an informed and shared policy decision-making in the context of digital trade. The tribunal emphasised that there needs to be voluntary steps taken by the state vis-à-vis its indigenous communities to protect them against material risks in the digital sphere.

The issue of indigenous data governance warrants a holistic investigation altogether. In this article, we propose that there is scope for indigenous data governance in digital trade chapters. Given the novelty of digital trade negotiations, the stakeholders need to be realistic yet optimistic enough to take a concerted effort at national as well as international forums to make the discussions more inclusive. The inclusivity principle for digital trade negotiations

---

<sup>437</sup> CP-TPP, *supra* note 66, at art. 17.16.

<sup>438</sup> *Id.*

<sup>439</sup> *Id.*

<sup>440</sup> *Id.*

<sup>441</sup> CP-TPP, ch. 29, Exceptions and General Provisions, art. 29.2. <https://www.dfat.gov.au/sites/default/files/29-exceptions-and-general-provisions.pdf>.

underscores the importance of vulnerable communities or underrepresented sections of society who are impacted by digitalisation of trade yet have found it hard to voice their opinion or concern on the same.

This inclusivity will deliver results if it is maintained for a sustainable period of time. It will ensure a carve-out of pertinent issues relating to indigenous data governance and help garner political support for digital trade negotiations by vulnerable communities. It will help such communities to better understand the value and purpose of digital trade agreements so as to fruitfully utilise such arrangement than criticize them in oblivion.

Both the CP-TPP and RCEP provides for the Treaty of Waitangi waiver for New Zealand, no such provision is provided in eJSI. This provision enables New Zealand to take policy measures which allows preferential treatment to its Māori indigenous community. However, it is subject to the requirement that such measures are not adopted as a means of arbitrary or unjustified discrimination against persons of other Parties or as a disguised restriction on trade in goods, services, or investment.

There is an additional provision in the CP-TPP on “traditional knowledge and traditional cultural expression” which provides that the states may establish appropriate measures to respect, preserve and promote traditional knowledge and cultural expressions.

These are positive developments as digital trade needs to operate within a diverse socio-economic context. It cannot merely delve into economic issues and overlook social issues relevant to digital trade by arguing that such issues will be managed by concerned individual states or international organizations. Indigenous data governance is a new theme emerging within states and debated in the United Nations. It is a complex and rich topic which warrants a whole separate research agenda.

The states need to be sensitive to their indigenous and other minority communities impacted from digitalization of international trade. Digital trade can be disruptive to the societal fabric compared to traditional trade in unique ways. The states need to take a cautious approach from the beginning to make stakeholder deliberations for digital trade highly inclusive, especially for the vulnerable and indigenous communities. The digital trade agreements should enable special domestic mechanisms for capacity-building to help such communities to make such stakeholder deliberations more meaningful and inclusive both nationally and internationally. These stakeholder forums will help such communities to rationally utilize the value and purpose of such digital trade agreements or arrangements and not be swayed by unfounded criticisms.

## V. CONCLUSION

Digital trade agreements are a necessary tool to ensure legal predictability and stability in the global economy. This comparative analysis is a novel attempt to encapsulate key features of the fundamental regulatory provisions in the most pertinent digital trade agreements. It highlighted that there are diverse interests and approaches to regulate digital trade. Especially as it relates to the need for clear and updated definition of “digital trade/e-commerce”, “digital products”, “covered persons” to core regulatory deliberations on “cross-border data flows”, “non-discriminatory treatment of digital products – likeness test” in the context of digital trade, regulatory clarity on “personal information protection”, “cybersecurity”, “source code”, “location of computing facilities”, “custom duties”, “general and security exceptions” and “treaty of Waitangi exception”. The article argues for a careful and balanced

deliberation among stakeholders to improve digital trade regulations as per new economic and technological realities. It requires a sustained deliberation as rapid technological advancement requires continued vigilance with an optimistic anticipation for change.

The article proposes important recommendations to policymakers. They include the need to clearly define “digital trade/e-commerce”, “digital products” in consonance with new technological developments for legal stability and predictability. The concept of “like digital products” cannot be interpreted in the context of GATT 1994 or GATS due to vastly different legal and technological context. The policymakers need to clearly define the concept of “like digital products” in the context of digital trade. Further, the concepts of “legitimate public policy objective”, “essential security interests” and “critical infrastructure” should be specifically supported with an illustrative list of covered objectives, especially in relation to the general and security exceptions.

The digital trade agreements should promote new international guidelines to design national personal data/information and cybersecurity regulatory frameworks by member states. It will support a relative convergence of regulatory priorities and enable interoperability of mechanisms for cross-border data flows. Policymakers should make a clear legal distinction between “source code” and “algorithm” in the context of digital trade as well as the concept of “mass-market digital products” that are subject to the obligation against transfer of source code/algorithm as a condition for imports.

There is a political divergence among states on the application of custom duties on digital trade. It has led to a distinct interpretation of the legal scope of the WTO moratorium on e-commerce. It is advised that the policymakers should ensure a constructive national and international dialogue to enable a mutually beneficial agreement on this issue. Lastly, we believe that the indigenous community data governance will become an important economic and socio-political issue in the context of digital trade which needs constructive discussions among policy makers as well as a dedicated discussion forum for civil society organizations to reasonably voice their concerns and help shape socially viable digital trade policies.