CHAPTER 6

Opportunities and Challenges for ASEAN and East Asia from the Regional Comprehensive Economic Partnership on E-Commerce

Jane Kelsey
Faculty of Law, University of Auckland, New Zealand

Kelsey, J. (2022), 'Opportunities and Challenges for ASEAN and East Asia from the Regional Comprehensive Economic Partnership on E-Commerce', in Kimura, F., S. Urata, S. Thangavelu, and D. Narjoko (eds.), *Dynamism of East Asia and RCEP: The Framework for Regional Integration* . Jakarta: ERIA, pp.119-144.

The Regional Comprehensive Economic Partnership (RCEP) is a microcosm of the current tensions in negotiations on digital trade involving parties that have divergent positions on the digital economy, data, and regulation, including within the Association of Southeast Asian Nations (ASEAN) itself. It adopts a prudent approach that recognises the state parties need flexibility and policy space at the national and regional levels to develop of policy and regulation in the rapidly changing digital ecosystem and seeks to advance their collective interests through dialogue and cooperation. This paper contrasts that approach with the disciplinary nature of binding legal obligations that are enforceable by other states and their investors, as in the Trans-Pacific Partnership Agreement and similar recent treaties. The analysis of key differences focuses on matters of particular importance to ASEAN, such as local content and government procurement, data rules and flexibilities, financial data, source codes, and transparency. RCEP's cautious approach enables ASEAN members to deepen their national and regional understanding of the opportunities and challenges these agreements present, whilst developing and implementing their own digital development strategies. Yet those good efforts may be undermined through the binding and enforceable trade in services rules.

Introduction

Electronic commerce, also called digital trade, is the most prominent 'new issue' in international trade negotiations and has become increasingly controversial. Novel rules on e-commerce that were adopted in the Trans-Pacific Partnership (TPP) Agreement in 2016 were originally designed by and for the United States (US) technology companies that dominate the digital domain globally (Kelsey, 2018). These binding and enforceable rules presumed a hands-off approach to regulation, consistent with the US model, and were carried through unchanged to the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) following the United States stepping away from the original agreement.

The TPP/CPTPP precedent has since informed negotiations on digital trade in various free trade agreements (FTAs) and in a plurilateral initiative at the World Trade Organization (WTO). The most expansive agreements to date are the US–Mexico–Canada Agreement (USMCA)[1] and the Singapore–Australia Digital Economy Agreement,[2] both of which

[1] US–Mexico–Canada Agreement, signed 10 December 2019, entered into force 1 July 2020. For example, Chapter 19 on Digital Trade extended the protection for owners of source codes in the TPP/CPTPP from disclosure requirements to include algorithms (Article 19.16).

[2] Singapore–Australia Digital Economy Agreement, signed 6 August 2020, entered into force 8 December 2020. This agreement also extended protections for algorithms (Article 7) and has stronger requirements for cross-border data transfer (Art 23) and online consumer protection laws (Article 15).

entered into force in 2020. Agreements involving the European Union (EU), such as the EU Mercosur Trade Agreement,[3] use a different configuration and legal tools to achieve broadly similar goals, whilst protecting areas of sensitivity to the EU, notably on personal privacy.

However, a global convergence around a TPP-based norm should not be assumed. A regulatory regime for the digital domain needs to balance economic interests, digital development, indigenous and human rights, and national security. There are many international forums that might be considered appropriate to develop this regime. Trade agreements that have a bias towards commercial interests, rely on compliance through enforcement of legal obligations, and are commonly negotiated in secret, are particularly ill-suited to that task (UNCTAD, 2021).

There is an increasingly mature understanding amongst a number of governments, especially from developing countries, that these rules may have negative impacts on digital development, social wellbeing, and national security. There is also scepticism over the real-world effect of rules that may, on their face, look helpful to developing countries, because the unlevel global playing field means they are likely to entrench the dominance of first movers over the world's digitalised infrastructure and economy. Other provisions will constrain revenue and governments' policy and regulatory options. Some procedural and institutional obligations will also stretch countries' institutional capacity.

This caution is evident in the Regional Comprehensive Economic Partnership (RCEP) amongst the 10 ASEAN members and five other countries from the Asian region,[4] as it implicitly recognises the need for flexibility to determine appropriate modes of regulation and digital development strategies through cooperation and dialogue at the regional level. The final text omitted, or significantly altered, several core elements of the CPTPP e-commerce chapter. Some rules included flexibilities that give governments more policy space and ASEAN and East Asian businesses more opportunities to compete with the dominant big tech corporations than provided in the TPP/CPTPP. The moratorium on the right to impose tariffs on cross-border electronic transmissions remains temporary and tied to a multilateral decision at the WTO, whereas the TPP and some other recent FTAs have made it permanent. Crucially, RCEP's e-commerce chapter is not enforceable, subject to future review. It remains to be seen how this approach will influence the way that ASEAN countries respond to pressure to negotiate on e-commerce in future FTAs and at the WTO.

[3] European Union Mercosur Trade Agreement, Agreement in Principle 28 June 2019, Sub-section 6 E-commerce of Section 3 Regulatory Framework, in Title XXX Trade in Services and Establishment.

[4] India was a participant in the negotiations but withdrew in November 2019 before the RCEP agreement was signed.

The RCEP outcome also reflects a compromise between powerful states that have divergent positions on the digital economy, data, and regulation. Whereas the TPP was driven by US interests, and later championed by Singapore, Australia, and Japan in the CPTPP, the WTO and their own FTAs, China and India brought their own commercial and nationalist aspirations to the RCEP negotiating table.

Section 2 of this paper outlines the context and structure of the electronic commerce provisions in RCEP, addressing the complex configurations amongst the 16 RCEP negotiating countries in relation to e-commerce, the dominance of big tech incumbents, and the spread of e-commerce-related provisions across the e-commerce, trade in services, and financial services chapters.

Section 3 focuses on the more traditional trade-related provisions in RCEP's e-commerce chapter that deal with paperless trading, e-signatures, e-authorisation, and a legal framework for electronic transactions.

In section 4 a number of key differences between the TPP/CPTPP and RCEP are examined to highlight current sensitivities over digital trade rules, including on enforcement, revenue, local content and government procurement, data rules and flexibilities, financial data, source codes, and transparency.

Section 5 briefly discusses the general regulatory provisions that require governments to have consumer protection and personal privacy laws without specifying any minimum standards.

The paper concludes that RCEP is a microcosm of the current tensions in negotiations on digital trade. It has adopted a prudent approach that recognises that state parties need flexibility and policy space at the national and regional levels to develop policies and regulations in the rapidly changing digital ecosystem and seeks to advance their collective interests through dialogue and cooperation, in contrast to the coercive approach of legal obligations that are enforceable by other states and their investors adopted in the TPP/CPTPP.

The Context and Content of e-Commerce in RCEP

The RCEP negotiations were launched in November 2012 and concluded 7 years later in November 2019. The agreement was signed in November 2020. It entered into force on 1 January 2022 after notification of ratification by more than the requisite six of the 10 ASEAN member states[5] and three of the five non-ASEAN signatory states.[6] Subsequent ratifications take effect 60 days after notification.[7]

E-Commerce Positions of Negotiating Parties

The 16 states that participated in the RCEP negotiations are diverse. ASEAN operated as a single entity applying its principle of consensus, which was sometimes hard to reach; some final obligations of its members differ. The six non-ASEAN participants – Australia, China, India, Japan, New Zealand, and the Republic of Korea – all have FTAs with ASEAN, hence their collective label as ASEAN Foreign Partners. Each brought its own geopolitical, strategic, and commercial objectives to the table, which only occasionally converged. India actively pursued its specific interests throughout the negotiations before it withdrew in November 2019, shortly before the agreement was announced.

Table 6.1 RCEP Participants' Plurilateral Digital Trade Obligations

Country	Ratified RCEP	ASEAN	TPP/CPTPP	WTO JSI
Australia	X		X	X
Brunei Darussalam	X	X	*	X
Cambodia	X	X		
China	X		+	X
India	^			
Indonesia	*	X		X
Japan	X		X	X
Lao PDR	X	X		X
Malaysia	X	X	*	X

[5] Brunei, Cambodia, Lao People's Democratic Republic, Singapore, Thailand, Viet Nam, as per Regional Comprehensive Economic Partnership agreement, signed 15 November 2020, entered into force 1 January 2022 (RCEP) Art 20.6.2.
[6] In fact, four non-ASEAN signatories (Australia, China, Japan, New Zealand) became original parties.
[7] RCEP Article 20.6.3. Malaysia and the Republic of Korea subsequently submitted instruments of ratification.

Country	Ratified RCEP	ASEAN	TPP/CPTPP	WTO JSI
Myanmar	*	X		X
New Zealand	X		X	X
Philippines	*	X		X
Singapore	X	X	X	X
Republic of Korea	X		+	X
Thailand	X	X		X
Viet Nam	X	X	X	

ASEAN = Association of Southeast Asian Nations, CPTTP = Comprehensive and Progressive Agreement for Trans-Pacific Partnership, JSI = Joint Statement Initiative, RCEP = Regional Comprehensive Economic Partnership, TPP = Trans-Pacific Partnership, WTO = World Trade Organization.

Notes: ^ withdrew before signing, * signed but not yet ratified, + applied to join.

Source: Compiled by the author (as of May 2022).

Negotiating positions on e-commerce were complicated by the participating states' other FTA obligations. Seven of the sixteen, including four ASEAN Member States, are also signatories to the CPTPP: Australia, Brunei Darussalam, Japan, Malaysia, New Zealand, Singapore, and Viet Nam, although Malaysia and Brunei have not ratified the agreement. All the TPP/CPTPP countries are also participating in the plurilateral negotiations on electronic commerce at the WTO – often called the Joint Statement Initiative (JSI) – which Australia, Singapore, and Japan have jointly convened, and whose draft text broadly follows the TPP model.[8]

ASEAN had significant internal tensions on e-commerce. The group adopted an aspirational agreement on e-commerce in 2019,[9] which entered into force in 2021 alongside a broad digital masterplan (ASEAN Secretariat, 2021); the recently revised ASEAN Trade in Services Agreement is also pertinent. Whilst several ASEAN states had commitments under the TPP/CPTPP, others were developing innovative national digital strategies that required protections for their policy space. Indonesia, for example, was actively considering how to regulate and tax the digital domain (Kelsey, 2021). Viet Nam, a TPP/CPTPP Party, was still regulating data and digital transactions during its transition period before those obligations entered into force.[10]

[8] The text has not been released publicly but the Revised WTO Electronic Commerce Negotiations. Updated consolidated negotiating text – September 2021, INF/ECOM/62/Rev.2 is available at https://www.bilaterals.org/?-other-292-.

[9] ASEAN Agreement on Electronic Commerce 2019 signed on 22 January 2019. https://agreement.asean.org/media/download/20190306035048.pdf.

[10] Trans-Pacific Partnership Agreement (TPP) signed on 4 February 2016, and Comprehensive Agreement for Trans-Pacific Partnership (CPTPP) signed on 8 March 2018, entered into force 30 December 2018, Article 14.18 provides for non-enforcement for 2 years after the TPP's entry into force. Additional side-letters extended this for Viet Nam's laws related to cyber security for 5 years after the CPTPP's entry into force for Viet Nam. See, for example, the exchange of letters between the Governments of Viet Nam and New Zealand dated 2 March 2018. https://www.mfat.govt.nz/assets/Trade-agreements/CPTPP/Viet-Nam-New-Zealand-Cyber-Security.pdf

China and India both approached the RCEP negotiations with strong, but different, offensive and defensive interests in the digital domain. India vigorously promoted measures to benefit its cross-border services, such as outsourcing and back-office operations (known as mode 1 of trade in services) and non-permanent migration of its information technology professionals (known as mode 4). Whilst the main reason for India's withdrawal from RCEP was the potential impact of commodity imports on its domestic economy, especially from China, the failure to secure significant concessions on cross-border mobility of its professionals was another justification for its exit. India remains a strong critic of the plurilateral negotiations on e-commerce at the WTO (Sen, 2021), partly because of the institutional consequences of the unmandated JSI negotiations and because they will enable India's offensive interests to be bypassed.

China's approach was consistent with its Digital Silk Road strategy that focuses on infrastructure and the digital eco-system. Some TPP/CPTPP-style rules benefit China's tech giants, such as AliBaba and Tencent, with their integrated search engines, trading platforms, e-finance, logistical hubs, as well as data mining and engineering. China also has interests in reducing tariffs and easing technical standards for information technology and smart products and in customs facilitation for products traded through regional supply chains. At the same time, China was concerned to protect its stringent restrictions on digital operators and users within, and increasingly outside, the country under the broad rubric of 'national security'. China has taken a similar approach at the WTO (Gao, 2020). It remains to be seen how China intends to navigate these issues in its application to accede to the CPTPP.

The tensions between these diverse, and often conflicting, strategic, commercial, regulatory, security, and geopolitical interests are evident in the final RCEP text.

First Mover Beneficiaries of e-Commerce Rules

These political complexities blunted the influence of the powerful US tech industry lobbyists on the RCEP outcome, and the final RCEP e-commerce rules walked back the binding and enforceable rules that they had secured in the TPP/CPTPP.

Nevertheless, the digital multinational enterprises (MNEs) still stand to be the principal beneficiaries of RCEP's e-commerce chapter as the main suppliers of services in or into the region. The Asian Internet Coalition, for example, represents Airbnb, Amazon, Apple, Booking.com, Cloudfare, Facebook (now Mega), Google, Expedia, Line, Linkedin, Rakuten, Sap, Twitter, and Yahoo.[11] These and other tech industry giants have shown themselves to be pass masters at regulatory and tax arbitrage, with complex corporate structures

[11] For an example of the tech industry's lobbying position, see GSMA Asia-Pacific (2017).

that provide coverage under trade rules, whilst minimising their exposure in domestic jurisdictions. The RCEP e-commerce rules facilitate that model. Even though the US is not a party to RCEP, if governments' regulatory frameworks seek to differentiate between those companies and other regional or local firms, the US might initiate investigations under Section 301 of the Trade Act of 1974 and threaten unilateral sanctions, as it has done over digital services taxes (Kelsey, 2021).

Notionally, businesses in ASEAN and East Asian countries should also benefit from the RCEP rules. However, not all tech companies are equal. The digital trade rules facilitate the concentration of operations from a regional, if not global, hub. This enables the incumbents to collect, consolidate, mine, and engineer data, the essential raw material in the global digitalised economy, so as to strengthen their oligopolies. It will remain difficult for most domestic businesses to compete, or even to enter the mainstream digital market. That is especially so for micro, small, and medium-sized enterprises (MSMEs). Rules that prevent requirements for data to be stored locally will also fetter the ability of states and their businesses to benefit from data generated within their own territory to advance their digital development strategies. Those, and other, rules will constrain how governments can address a wide range of other public policy, revenue, and security issues.

Concerns over these commercial realities, the dominance of incumbents over the digital eco-system, and constraints on regulation imposed by the rules are reflected in the flexibilities and exceptions written into RCEP, in contrast to other recent agreements.

An Overview of e-Commerce in RCEP

When a chapter carries the title of a particular subject there is a risk that people do not look beyond that to other chapters that also bear on the subject. That risk is particularly high with electronic commerce. Three substantive chapters – on Electronic Commerce, Trade in Services, and Investment – together constitute RCEP's e-commerce rules, although other agreement-wide provisions, such as definitions and exceptions, and aspects of the Intellectual Property chapter are also relevant.

Chapter 12 of RCEP is titled 'Electronic Commerce'. The chapter applies to '*measures* adopted or maintained by a Party that *affect* electronic commerce'. 'Measures' are defined expansively in the agreement to be any law, regulation, rule, procedure, decision, administrative action, or any other form of government action.[12] 'Affect' has a broad sweep, not limited to measures that directly target e-commerce. 'Electronic commerce' itself is not defined, but the provisions in the chapter extend far beyond cross-border online commercial transactions and include matters like personal privacy and spam.

[12] RCEP Article 1.2.q.

The Chapter on Electronic Commerce has five sections as set out in Table 6.2. Section A *General Provisions* covers Definitions, Principles and Objectives, Scope, and Cooperation. Section B has two *Trade Facilitation* provisions: Paperless Trading, and Electronic Authentication, and Electronic Signature.

Table 6.2 RCEP Chapter 12 on Electronic Commerce

Section A. General Provisions	
12.1	Definitions
12.2	Principles and Objectives
12.3	Scope
12.4	Cooperation
Section B. Trade Facilitation	
12.5	Paperless Trading
12.6	Electronic Authentication and Electronic Signature
Section C. Creating a Conducive Environment for Electronic Commerce	
12.7	Online Consumer Protection
12.8	Online Personal Information Protection
12.9	Unsolicited Commercial Electronic Messages
12.10	Domestic Regulatory Framework
12.11	Customs Duties
12.12	Transparency
12.13	Cyber Security
Section D. Promoting Cross-Border Electronic Commerce	
12.14	Location of Computing Facilities
12.15	Cross-border Transfer of Information by Electronic Means
Section E. Other Provisions	
12.16	Dialogue on Electronic Commerce
12.17	Settlement of Disputes

Source: Prepared by author from the RCEP text.

Section C, *Creating a Conducive Environment for Electronic Commerce*, has one genuine trade provision, dealing with Customs Duties. The remaining provisions in Section C – Online Consumer Protection, Online Personal Information Protection, Unsolicited Commercial Electronic Messages (also known as spam), Domestic Regulatory Frameworks, Transparency and Cyber Security – are more general regulatory issues. The increasing overreach of the 'trade' rubric into such broad areas of domestic regulation has become a significant source of criticism of the development of these e-commerce or digital trade rules.

Similarly, the two rules in Section D, *Promoting Cross Border Electronic Commerce*, which cover Location of Computer Facilities and Cross-border Transfer of Information by Electronic Means, restrict Parties' regulation of data flows and their ability to require that domestically sourced data is retained and accessible within the country.

The chapter's final section, *Other Provisions*, provides for Dialogue on Electronic Commerce, especially TPP/CPTPP matters omitted from RCEP. Crucially, it also excludes the chapter from coverage of the state–state dispute settlement chapter, for now.

Complementing the e-commerce chapter, 'measures affecting the supply of a service delivered electronically' are also covered by the relevant obligations in Chapter 8 Trade in Services and Chapter 10 Investment, subject to sectoral commitments and reservations made by Parties in those chapters.

Chapter 8 contains rules on non-discrimination, not limiting access to the domestic market, and not requiring cross-border suppliers to have a local presence; obligations in this chapter are enforceable. The chapter applies to a broad range of computer and related services, advertising, distribution, cultural, health, education, transportation, and business services, amongst others, with sectoral annexes on financial services, telecommunications, and professional services. Those rules will significantly constrain the regulation of digital and cross-border service suppliers and activities. Their application to individual Parties is subject to complex scheduling that is unlike any of their previous agreements.[13]

Financial institutions, public entities, and financial service suppliers are excluded from coverage of the e-commerce chapter, as are investors in financial services and institutions. However, Annex 8-A Financial Services applies some related, but different, rules to those entities and activities.

[13] RCEP Articles 8.3, 8.7, and 8.8.

The e-commerce chapter makes several explicit references to these other chapters. The rules that restrict data localisation apply to a 'covered person', which refers to service suppliers as defined in Chapter 8 Trade in Services, and to a covered investment[14] and covered investors defined in Chapter 10 Investment.

This multi-chapter interface comes with further complexities. The sectoral commitments and reservations made by Parties in the services and investment chapters are imported to the e-commerce chapter only for the data transfer and location provisions, and only to the extent that measures a government adopts are protected in those schedules – which is difficult to interpret, because these commitments and reservations are framed to address different rules from those in the electronic commerce chapter.

The accumulation of these chapters creates a legal minefield for domestic regulators and digital companies.

Facilitating Traditional Electronic Commerce Transactions

RCEP does not define electronic commerce. Clearly, it covers trade in traditional commodities which are transacted with the assistance of digital technologies. Chapter 12 has two provisions designed to facilitate that kind of trade, covering three kinds of measures: paperless trading, electronic signatures, and electronic authentication. The first two measures reflect the RCEP preference for flexibility and good faith commitments over enforceable obligations and seek to balance assistance to exporters and importers with the burdens of compliance on businesses and governments.

Paperless Trading

The general obligation on Paperless Trading is mandatory ('shall').[15] However, it only requires parties to 'work towards' implementing paperless trading initiatives and to 'endeavour' to accept trade administration documents as the legal equivalent of paper versions and make trade administration documents available to the public in electronic form. The three ASEAN least-developed countries (LDCs) – Cambodia, the Lao People's Democratic Republic (Lao PDR), and Myanmar – have a grace period for compliance of 5 years after RCEP enters into force for them.

[14] RCEP Article 10.1 uses a wide asset-based definition of investment to include enterprises, shares, intellectual property rights, rights under contracts and licenses, and more.
[15] RCEP Article 12.5.

e-Signatures

The provision on e-signatures uses a different legal formulation to provide governments with even more flexibility: a Party cannot deny the legal validity of a signature solely because it is in electronic form 'except in circumstances otherwise provided for under its laws and regulations'.[16] That enables a Party to adopt or maintain laws that do not accept e-signatures as legally valid. The word 'solely' also implies that e-signatures could be denied validity on grounds additional to the fact they are in electronic form. Cambodia and Lao PDR again have a 5-year transition period, but not Myanmar.

Full implementation of these obligations would make transactions easier for ASEAN businesses to operate across the border, and potentially within the domestic economy, provided those businesses have access to the necessary technology and the relevant platforms. That proviso could be problematic for smaller businesses and those from countries with limited technology and connectivity. At the same time, full compliance could impose significant implementation costs on governments, which is why the provisions only require 'endeavours' to comply.

e-Authentication

There is less flexibility in the third kind of measure, e-authentication,[17] which more closely aligns with the TPP/CPTPP. Governments must allow participants in e-transactions to decide what they consider are appropriate authentication technologies and implementation models (such as multi-factor, certificate based, biometric or token-based authentication) and not limit recognition of those technologies and models. The Party can still have laws on electronic authentication, but transactors must have the opportunity to show that the e-authentication methods they have chosen are compliant with those laws.

Whilst financial services are excluded from Chapter 12 Electronic Commerce, regulations on e-authentication might also be considered to be 'measures affecting' the supply of services electronically, such as computer and related services and financial services, under the Trade in Services chapter and its Financial Services Annex. It is unclear whether the negotiators discussed that possibility as the negotiating history is not publicly available.

The e-authentication provision potentially benefits all businesses by providing assurance of identity in sensitive transactions and minimising risks of fraud. In practice, the

[16] RCEP Article 12.6.1.
[17] RCEP Article 12.6.2.

technology will be dictated by the more powerful party/ies in a commercial relationship, and MSMEs may not have access to the technology or be able to afford the technology and license fees.

The provision provides some flexibility for governments to impose performance standards or certification requirements on a particular category of e-transactions. Whilst the scope of this flexibility is limited to performance measures or certification, and must apply to specified categories, the content of those measures and the number of categories is not prescribed. However, the provision appears to prevent RCEP governments from requiring the use of particular forms of cybersecurity, etc, such as two-factor authentication or encryption of personal details, unless the government frames them as 'performance standards' and designates special categories to which those standards apply.

Legal Framework for Electronic Transactions

The Parties to RCEP must also establish or maintain a domestic legal framework to govern 'electronic transactions'.[18] Again, there is a lack of clarity for policymakers. Electronic transactions are not defined. It is unclear, for example, whether this refers only to commercial transactions or also covers non-monetised online activities where users access 'free' services for the price of their data.

The framework is not prescribed but must 'take into account' the relevant United Nations Commission on International Trade Law (UNCITRAL), United Nations (UN), or other international conventions and model laws on electronic commerce. The UN Convention on the Use of Electronic Communications in International Contracts, which is specifically cited, applies only to use of electronic communications in international contracts; however, the UNCITRAL Model Law on Electronic Commerce inscribes fundamental legal notions of non-discrimination, technological neutrality and functional equivalence, which makes it vital for governments to understand the scope of its application.[19]

Parties must 'endeavour' to avoid this legal framework imposing an 'unnecessary regulatory burden', implying a light-handed approach. Endeavour provides some flexibility, but it is still a positive obligation. Only Cambodia has a 5-year grace period for implementation.

[18] RCEP Article 12.11.

[19] The TPP/CPTPP more strictly requires the framework to be consistent with the UNICTRAL Model Law or UN Convention, TPP/CPTPP Article 12.14.5.1.

Significant Differences Between the TPP/CPTPP and RCEP

The substance of the trade-related provisions discussed above were very similar across RCEP and the TPP/CPTPP; the difference was in the degree of legal obligation. At first glance, most other parts of the e-commerce chapters also seem very similar. However, there are at least six important differences between the two agreements that illustrate the tension over the balance between the commercial and regulatory elements of e-commerce rules in contemporary trade agreements.

Enforcement

By far the most significant difference between the agreements involves enforcement. The e-commerce chapter of the TPP/CPTPP is fully enforceable through the state–state dispute settlement system. The TPP/CPTPP also provides for investor–state dispute settlement; whilst tech companies established in another Party could not directly enforce the e-commerce chapter rules, they could seek awards of compensation for the same measures by claiming that they breach the investor protection rules in the Investment Chapter.[20]

By contrast, the RCEP e-commerce chapter is not enforceable by state–state dispute settlement.[21] Disputes between the Parties over interpretation of and compliance with Chapter 12 are subject to good faith consultations. Application of the dispute settlement process to the chapter will be part of the 5-yearly general review of RCEP,[22] after which some RCEP Parties could elect to have it apply to them. Any such decision would only bind those RCEP Parties that so agree.

The main operational provision promotes dialogue between the Parties, under the auspices of the RCEP Joint Committee, on a number of mandated matters:[23] cooperation to assist MSMEs and to enhance capacity in the regulatory space, information sharing, building trust, and promoting development of e-commerce in regional and multilateral forums; current and emerging issues, including source codes and data flows and storage; and matters relating to development of e-commerce, such as anti-competitive practices, online dispute resolution, and temporary movement of professionals. The outcome of the dialogue is to be considered as part of the 5-yearly general reviews of the Agreement as a whole.[24]

[20] TPP/CPTPP Article 9.6.3 says an investor cannot rely on a finding of a breach of another provision of the Agreement as establishing a breach of minimum standard of treatment for investors. However, that does not stop the investor making a claim about the same measure.
[21] RCEP Article 12.17.
[22] That is provided for in RCEP Article 20.8.
[23] RCEP Article 12.16.
[24] RCEP Article 20.8.

Chapter 10 on Investment is subject to the state–state dispute settlement chapter – but there is no investor dispute mechanism under RCEP, a matter also flagged for future discussion.[25] However, RCEP Chapter 8 Trade in Services is fully subject to state–state disputes, and a broad interpretation of its coverage could neutralise the unenforceability of Chapter 14.

The Moratorium on Levying Customs Duties on Electronic Transmissions

Customs duties or tariffs on commodities is a straightforward traditional trade issue. Border taxes on digitalised transactions, services, and products are more complicated. In 1998 the WTO adopted a temporary moratorium on customs duties on electronic *transmissions* (not electronic *transactions*) as an adjunct to a Work Programme on Electronic Commerce.[26] The temporary moratorium has been regularly renewed since then and remains in place today.

There is disagreement on what the moratorium applies to. 'Electronic transmissions' is not defined in the WTO (or RCEP).[27] On the one hand, the US says the moratorium applies to all material transmitted electronically, including content such as movies or 3D printing (Kanth, 2021). But Indonesia secured confirmation from the WTO Secretary General in 2017 that the moratorium does not apply to electronically transmitted goods and services.[28]

Despite this lack of clarity, developed countries want the ban made permanent in the WTO and have already done so in various FTAs.[29] Conversely, many developing countries want the moratorium removed because of its escalating impacts on revenue and on their ability to use tariffs to support their fledgling digital industrialisation (Kanth, 2021). Research published by UNCTAD in June 2020 shows the moratorium has disproportionate and significant tariff revenue losses and development impacts for developing countries, whatever definition of e-transmissions is applied (Kozul-Wright and Banga, 2020). A recent analysis for ERIA made similar findings for ASEAN countries (Montes and Lunenborg, forthcoming).

The TPP/CPTPP and RCEP reflect these conflicting positions. The former commits the Parties to a permanent ban on customs duties on an 'electronic transmission', which it defines as 'a transmission made using any electromagnetic means', but still leaves the distinction between digital carriage (just the technology) and digital content unresolved for the purposes of the ban. Parties to RCEP that have ratified the CPTPP (which Brunei and Malaysia have not) are bound by that obligation, as will be any country that subsequently accedes to the CPTPP.

[25] RCEP Article 10.18.
[26] WTO General Council (1998), 'Work Programme on Electronic Commerce', adopted 25 September 1998, WT/L/274 (30 September 1998).
[27] Taxes, fees, or other charges on electronic transmissions are explicitly excluded, but that simply clarifies the kind of tax, not what it applies to.
[28] World Trade Organization. 'Statement by Indonesia. Facilitator's consultation on electronic commerce. MC11 Declaration, and other relevant plenary sessions. 13 December 2017', WT/MIN(17)/68, 20 December 2017.
[29] Of course, any State can unilaterally remove all customs duties on e-transmissions, including content.

RCEP imports the current position at the WTO: a voluntary moratorium under the 1998 WTO Work Programme on Electronic Commerce that is renewed periodically.[30] If WTO Members alter the status quo – which could involve a permanent ban, a roll-over, a longer term, or letting the moratorium lapse – each RCEP Party will be able to decide whether to adjust its approach to reflect that new position.

A Broad-based Tax Exception

Taxing the digital economy faces major challenges: the extra-territorial operation of digital MNEs; sophisticated tax planning that enables profit shifting through related party arrangements, such as arms-length contractors, royalties, and management fees; and opaqueness of the business model that relies on mining of data secured from sources for 'free' (Kelsey et al., 2020; Kelsey, 2021).

For some years, the Group of 24 Finance Ministers from developing countries, and the more dominant OECD/G20 Inclusive Framework, have been considering how to update international tax norms to deal with Base Erosion and Profit Shifting by digital MNEs. As discussions within the Inclusive Framework stalled, a number of countries, including several from ASEAN, implemented or proposed to adopt taxes on digitalised services transactions and digital multinational enterprises' revenues.[31]

A digital services tax could be considered a 'measure that affects' e-commerce or trade in various services, such as computer and related services, advertising or distribution services for the purposes of RCEP's trade in services and e-commerce chapters. In addition to non-discrimination rules, a number of e-commerce provisions, especially those that prevent requirements for a local presence (located in the services chapter) and for localisation of data, could hinder a government's ability to tax the digital economy effectively.

Whilst the e-commerce chapter is not enforceable, tax measures may be subject to a state–state dispute under Chapter 8 Trade in Services, discussed earlier. In its defence, governments would have to invoke the taxation exception. As with the moratorium on customs duties, there are stark differences here between the TPP/CPTPP and RCEP.

The WTO-plus obligations in the TPP/CPTPP, including on e-commerce, apply to taxation measures. There is a convoluted tax exception with complex layers of carve-ins and carve-outs.[32] The taxation exception in RCEP is much simpler and significantly reduces the risks

[30] RCEP Article 12.11.
[31] Under the high-level agreement reached by the OECD/G20 Inclusive Framework in 2021 a proposed Multilateral Convention would require the removal of existing digital services taxes and prevent the introduction of such taxes in the future. See OECD/G20 (2021).
[32] TPPA Article 29.4.

of litigation from the adoption of new taxes.[33] The exception caps Parties' obligations with respect to taxation measures at those obligations which already apply in the WTO.[34] In other words, this protects taxation measures from new obligations in RCEP – whether in the e-commerce, trade in services, or any other chapter.

However, RCEP's tax exception only addresses problems that might be posed by its new rules. It does not resolve the existing difficulties with the WTO's exceptions on taxation of goods or services, in particular, Article XIV of the General Agreement on Trade in Services (GATS).[35] That exception is limited to breaches of the national treatment (non-discrimination) rule, and applies only where the measure aims to achieve the equitable and effective implementation or collection of direct taxes and the measure does not constitute arbitrary or unjustifiable discrimination between countries or a disguised restriction on trade.[36]

Locally Produced Digital Products and Services

As noted earlier, the digital domain of mass and metadata, analytics, search engines, servers, digital marketplaces, and artificial intelligence is not a level playing field. Big tech companies, principally from the US, are gatekeepers to the digital ecosystem. Competition laws are ineffectual in breaking open their oligopolies, especially when MNEs are outside the local jurisdiction. That creates problems nationally and on an enterprise level for most ASEAN countries where digital industrialisation involves small enterprises and start-ups and/or state-owned or supported companies. They will need positive assistance to take advantage of the opportunities that digital technologies can provide. Common forms of support include government procurement, subsidies, local content preferences and technology transfers. Whereas the TPP/CPTPP closes off many of those options, RCEP does not.

The TPP/CPTPP requires non-discriminatory treatment of digital products, meaning preferences cannot be given to products created in the Party's territory or by its nationals, although this does not apply to subsidies and grants or to broadcasting. Local preferences for digital products and content, and requirements to use locally produced content, are not subject to restrictions in RCEP, except to the extent they are covered in the trade in services or (limited) government procurement chapters.[37] This matter has been flagged as a topic for future dialogue between the Parties.[38]

[33] RCEP Article 17.14.
[34] RCEP Article 17.14.
[35] WTO General Agreement on Trade in Services Article XIV(d).
[36] The US has targeted digital services taxes, in particular, by investigations under Section 301 of the US Trade Act 1974, resulting in threats of sanctions against countries who adopt or maintain them. The analysis in those Investigations would treat digital services taxes as failing this test. See discussion in Kelsey (2021).
[37] The RCEP government procurement chapter is much more limited than the TPP/CPTPP and is also not subject to dispute settlement.
[38] RCEP Article 12.16.

Government procurement is a second important means of supporting local initiatives by harnessing the purchasing power of central and local governments. Whilst use of procurement in this way this could disadvantage ASEAN exporters competing with local producers, the commercial reality is that few local firms, especially start-ups and MSMEs, will be able to compete with MNEs or large local firms for contracts at home or in other RCEP countries.

The e-commerce chapters in both the TPP/CPTPP and RCEP exclude government procurement from their scope. However, an agreement-wide definition of government procurement in the TPP/CPTPP limits the term to the process of procuring goods or services for the internal and non-commercial use of a government.[39] Therefore, the carveout for government procurement from the rules in the TPP/CPTPP e-commerce chapter does not apply to the substance of the procurement or inputs into governments' for-profit activities.

By contrast, RCEP does not have an agreement-wide definition of government procurement. That leaves it open for the carveout to cover both the process and substance of the procurement. This approach is consistent with the limited and non-enforceable Chapter 16 on Government Procurement.

Data and Rights over Source Code

The next set of differences goes to the core of the new digital trade rules. Tension between competing policy considerations is especially fraught in relation to control and use of data, source codes and algorithms - elements that constitute the blood supply and the brain of the digital eco-system. The larger the database, the more sophisticated the algorithms, artificial intelligence, 3D printing, and cutting-edge new technologies will be a dynamic that entrenches the dominance of corporations that already control massive amounts of data.

The principal objective of the tech industry lobby in the TPP negotiations was therefore to secure unfettered rights to collect, accumulate, process, and exploit data in their place of choice on their own terms (Kelsey, 2018). Tech-based firms, especially the big services MNEs, want to centralise their facilities and processing of data sourced from their operations across the Asian region to maximise its value and minimise costs. They also want to decide where to locate the data so they can engage in regulatory and jurisdictional, as well as tax, arbitrage.

[39] TPP/CPTPP Article 1.3.

Smaller businesses operating offshore likewise want to avoid duplicating facilities in the places where they operate. But they are dependent on the major players for cloud servers, and on platforms and marketplaces that determine access and product placement. Local companies, especially MSMEs, may struggle even to appear on the digital radar, let alone to compete.

Countries have to balance a variety of objectives when they are hosting foreign tech suppliers. As part of their digital development strategies, governments may want to ensure that their national firms have access to data generated locally. They may want to require companies with large holdings of data to use local storage facilities to justify their investment of public funds to build expensive infrastructure. They also need to address myriad non-commercial policy concerns about data security, cybersecurity, political manipulations, terrorist organisation and dissemination of content, human rights violations, unregulated blockchains, cryptocurrency trading, money laundering, privacy, consumer protection, and more.

Data Localisation

Both the TPP/CPTPP and RCEP require covered businesses to be allowed to transfer information outside the source country for the purpose of their business and prohibit governments from requiring them to use local computing facilities, such as servers. However, the TPP/CPTPP guarantees far greater protection to commercial firms and is far more restrictive of governments than RCEP.

Both the so-called 'data localisation' provisions have an important carveout for information 'held or processed on behalf of a party'. The problematic words are 'on behalf'. This exclusion would clearly apply to national or sectoral data bases that are run by the government, or where a private firm is contracted to store and process data for government. It is less clear when it comes to projects co-developed with private interests, including for surveillance, traffic control or smart city projects, especially when a private firm collects and controls the data and integrates it with its other activities. Private firms that provide data services for public and private providers, such as health systems, may also fall outside the exclusion, unless their contract provides otherwise.

There are three major differences in the flexibility that the TPP/CPTPP and RCEP provide for governments to adopt policy measures that are inconsistent with these two rules.

The first difference relates to public policy objectives. Both data localisation rules allow a Party to adopt inconsistent measures that it considers 'necessary' to achieve a 'legitimate public policy objective'. That flexibility is subject to a proviso that the measure

is not arbitrary or unjustifiable discrimination (which could involve different treatment of technologies or categories of data that impact most on foreign firms, not just different treatment of nationalities) or in a manner that constitutes a disguised restriction on trade (which can be problematic when the measure does benefit local interests).

Whether a measure is necessary has a specific and restrictive meaning in trade jurisprudence. The government can set the standard it wants to achieve but needs to adopt the least burdensome option reasonably available to achieve that standard. In the TPP/CPTPP, an inconsistent policy measure is open to challenge on the basis of its necessity, the legitimacy of the policy objective, and the proviso. Footnotes in RCEP neutralise part of that test by making the necessity of the measure self-judging, so the measure is open to challenge only on the grounds of the legitimacy of the public policy objective and the chapeau (recalling that the chapter not subject to state–state dispute).[40]

The second difference the protection of 'essential security interests'. Recent controversies over data mining, cyber-espionage, use of bots and encrypted messaging have heightened states' sensitivity. Governments have restricted sites, apps, and movement of data on the basis of national security for a variety of motivations. China's sweeping digital laws have been highlighted as being repressive (Kynge and Yu, 2021), but state censorship and surveillance in the name of national security is increasingly common in many countries.

The data transfer and storage provisions in RCEP exclude measures a Party considers necessary for its 'essential security interests'.[41] The exercise of this power is explicitly self-judging and reliance on the exception cannot be disputed by the other Parties. There is no similar exception in the equivalent TPP/CPTPP provisions on data localisation. However, that omission could be explained by the difference in the agreement-wide security exceptions. The TPP/CPTPP's general security exception is broad and explicitly self-judging,[42] whereas RCEP follows the more limited WTO approach of specifying criteria that need to be met.[43] The RCEP self-judging national security exception also applies only to the data transfer and storage provisions; it does not apply, for example, to the provision on e-authentication in the same chapter.

It is uncertain whether this security carveout could stretch to protecting measures that address cybersecurity risks, which may involve private and commercial data theft, industrial sabotage, and ransomware. Such an interpretation would overcome the weak provisions on cybersecurity in both agreements, which recognise the importance of cybersecurity and building national level capabilities, but merely encourage the exchange of best practices.[44] Even cooperation between the Parties is limited to recognising its

[40] RCEP Article 12.14.3(a) fn 12, Article 12.15.3(a) fn 14.
[41] RCEP Articles 12.14.3(b) and 12.15.3(b).
[42] TPP/CPTPP Article 29.2.
[43] RCEP Article 17.3
[44] TPPA/CPTPP Article 14.16; RCEP Article 12.13.

importance through current collaboration mechanisms. There is no obligation in either agreement to adopt cybersecurity laws, even of an unspecified nature, whereas there is a specific obligation to protect consumers or personal information.

The third major difference relates to phase in periods for developing countries. There is no ability for Parties to take reservations to these data-related obligations in either agreement. The CPTPP has granted Viet Nam a waiver of the dispute settlement provisions for its cybersecurity law for 5 years after entry into force, being January 2025. Brunei and Malaysia are also currently not subject to these rules, as they have not ratified the CPTPP. In RCEP all three LDCs have a grace period of 5 years from entry into force to comply, with a possible 3-year extension for both provisions. Viet Nam also has 5 years to comply. Of course, failure to meet these obligations in RCEP can only be pursued through the inter-Party consultative mechanisms, unless a complaint can be brought under Chapter 12 on Trade in Services relating to 'a measure affecting trade in services'. That would not be protected by the self-judging exceptions in the e-commerce chapter.

Financial Data

Both agreements exclude financial services from the scope of their e-commerce chapters.[45] The original exclusion from the TPP was at US insistence, informed by its difficulties accessing data held offshore during the finance sector collapse in 2007. Yet financial data is not excluded from either agreement altogether. Definitions of financial services in Chapter 11 of the TPP/CPTPP and Annex 8A in RCEP explicitly include the 'provision and transfer of financial information, and financial data processing and related software by suppliers of other financial services'. Similar financial services rules apply in both the TPP/CPTPP and RCEP (for example, on non-discrimination, cross-border trade, and new financial services[46]). In RCEP they apply more broadly to 'measures affecting' the supply of financial services, compared to the TPP/CPTPP's 'measures relating to'.[47]

However, RCEP also has an explicit financial data transfer provision that is not in the TPP/CPTPP.[48] Echoing the e-commerce chapter, it guarantees that finance firms can transfer data out of the source country for processing as an ordinary part of their business. A government can require a copy of information to be held in the country, provided that information can also be moved and stored offshore.

[45] TPPA/CPTPP Article 14.1; RCEP Article 12.1.

[46] RCEP Annex 8A, Article 3 provision on 'new financial services' is more flexible. It requires a Party to make 'best endeavours' to allow the supply of a financial service not already being provided in the country, or a new form of one that is already being provided, if it is being legally supplied and regulated in another RCEP country.

[47] RCEP Annex 8A Article 2 cf TPP/CPTPP Article 11.2.1.

[48] RCEP Annex 8A Article 9.

Governments can also maintain measures to protect privacy and confidentiality of financial data, require regulatory approval (for prudential reasons) of the recipients of that information, and require compliance with its laws about management and storage of data (including keeping a copy within the country). But the ability to adopt all these measures is subject to a potentially circular proviso that the measures cannot be used as a means of avoiding the commitment or obligation.

Source Code

A further very significant variation relates to exclusive rights over technology, specifically source code. The TPP/CPTPP prevents Parties from requiring the owners of the source code used in mass-market software to provide access to it as a condition of the code, or products that contain it, being sold, or used in their territory, except where the code is used for critical infrastructure.[49] The USMCA explicitly extends this protection to algorithms expressed in source code. There is no equivalent provision on source code in RCEP, although it is flagged as a matter for future dialogue between the Parties.[50]

Transparency

Finally, there is an important difference in the transparency requirements in the two agreements. The TPP/CPTPP requires prior consultation with other Parties and their commercial interests on proposed new regulation, to the extent possible.[51] The RCEP's transparency obligations are all post-regulation,[52] which reduces the potential for lobbying and threats by digital companies where governments regulate. Parties are required to make general measures that comply with this chapter available publicly, at least on the Internet, 'as promptly as possible' but only 'where feasible'. They must also respond as promptly as possible to requests from another Party for specific information about those measures.

[49] Later agreements, such as the USMCA, go further, covering all source code and algorithms contained in source code, although the USMCA has a broader exception than the TPP/CPTPPP to enable specific investigations by regulators.
[50] RCEP Article 12.16.
[51] TPPA/CPTPP Article 26.2.
[52] RCEP Article 12.13.

Over-reach into Non-trade Regulation

This paper would be incomplete without referring to Section C of Chapter 12 Electronic Commerce, which purports to create a conducive environment for e-commerce. The five provisions are designed to allow policy space for certain public policies and human rights that could be negatively impacted upon by the other e-commerce rules, especially the rules relating to data flows. However, these provisions are limited in scope and both the commercial orientation of the chapter and the exclusive focus of the chapter's objectives on promoting the use of e-commerce militate against a broad public policy interpretation.

The two most prominent provisions, on protection of consumers and of personal information, are broadly similar. Both limit the obligations on states and on digital suppliers. Parties to RCEP must have laws or regulations that provide 'protection for consumers using electronic commerce against fraudulent and misleading practices that cause harm or potential harm to such consumers'.[53] The equivalent TPP/CPTPP provision says consumer protection laws must *proscribe* fraudulent and deceptive commercial activities that cause such harm or potential harm to consumers. However, neither agreement sets a minimum threshold for the consumer protection that a government must provide, and neither extends to other harmful actions, such as anti-competitive practices. The LDCs in RCEP have a 5-year grace period to comply.

The personal privacy provisions in the TPP/CPTPP and RCEP are also similar. Personal information is defined as 'any information, including data, about an identified or identifiable individual'. In RCEP, Parties must have a legal framework that 'ensures the protection of personal information of the users of electronic commerce'.[54] The TPP only requires the law to *provide* for protection of personal information of an identifiable natural person.

As with consumer protection, there is no minimum privacy standard in either agreement. Both allow Parties to comply by adopting a comprehensive personal privacy law, or sector-specific laws, or by providing for enforcement of contractual obligations that enterprises adopt. A RCEP Party 'must' (TPP says 'should') 'take into account' international standards, guidelines, etc of relevant international bodies. The RCEP governments 'must' publish information on the protection they provide (TPP says 'should') and encourage enterprises to publish their policies online. All the LDCs have a 5-year grace period to comply with this obligation as well.

The weakness of those provisions reinforces concerns that commercially-oriented trade agreements are not appropriate legal forums for rules that address such fundamental rights and constrain their scope and application.

[53] RCEP Article12.8.
[54] RCEP Article12.9.

Conclusion

It is easy to see why developing country governments and businesses might be excited by the prospect that e-commerce or digital trade rules in free trade agreements could open doors to the opportunities offered by digital technologies. However, the vehicle of a free trade agreement, and the binding and enforceable e-commerce rules that have been developed in the TPP and since, will not deliver that outcome for most countries in ASEAN and certainly not for the most digitally marginalised communities of women, the informal sector and MSMEs. As the UNCTAD Digital Economy Report 2021 observes:

> there are serious questions about how suitable the trade regime is to regulate the issue of data. ... Provisions in trade agreements have implications for domestic policies – such as those related to privacy, national security and industrial development – through these implications are not sufficiently considered. Furthermore, ... developing countries might face the choice of 'trading away their right (or policy space) to regulate data flows' to protect other interests in the trade agenda (UNCTAD, 2021, p.166).

Given the unequal negotiating power of state parties and the lobbying power of the technology industry, such agreements are likely to consolidate the dominance of a small number of very powerful multinationals that already control the digital eco-system and the vital resource of data (UNCTAD, 2021, p.146). The rules that are designed to serve their model work to encourage tax, data and regulatory arbitrage and further disable governments that need to find a new balance between development strategies, support for innovation, and protective regulation in the 21st century digitalised economy. The overreach of FTAs into the general regulation of the digital domain beyond traditional areas of trade has also fuelled a growing resistance to digital trade rules, including the plurilateral e-commerce negotiations in the WTO.

This paper has highlighted the significance of RCEP in promoting a more flexible approach that encourages regional cooperation on the development of appropriate policy and regulation, instead of rigid, enforceable rules that are subject to limited and uncertain exceptions. The RCEP electronic commerce chapter reflects an increasingly sophisticated understanding about these issues amongst policymakers, academics, civil society, and media analysts in the years since the TPP chapter was agreed.

The wisdom of ASEAN countries holding back from making enforceable commitments on e-commerce should allow them to deepen their national and regional understanding of the opportunities and challenges these agreements present, including through the mechanisms of dialogue and cooperation, whilst developing and implementing their own digital development strategies. Unfortunately, those good efforts may yet be undone through the back door of the binding and enforceable trade in services rules.

References

ActionAid (2021), 'World's Largest Economies Losing up to $32 billion in Annual Tax Revenue from Silicon Valley's Top Five Tech Companies', 20 May. https://actionaid.org/news/2021/worlds-largest-economies-losing-32-billion-annual-tax-revenue-silicon-valleys-top-five

ASEAN Secretariat (2021), *ASEAN Digital Masterplan 2025*. Jakarta: ASEAN Secretariat. https://asean.org/book/asean-digital-masterplan-2025/

Gao, H. (2020), 'Across the Great Wall: E-Commerce Joint Statement Initiative Negotiation and China', *SSRN Paper*, 19 June. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3695382

GSMA Asia–Pacific (2017), GSMA and AIC Encourage greater Engagement Among RCEP Countries to Enable a Truly Pan-Asian Digital Economy', GSMA Asia–Pacific, 18 October. https://www.gsma.com/asia-pacific/whats-new/gsma-and-aic-encourage-greater-engagement-among-rcep-countries-to-enable-a-truly-pan-asian-digital-economy

Kanth R. (2021), 'US Warns over Moves to Discontinue Moratorium', *SUNS No. 9299*, 5 March. https://twn.my/title2/wto.info/2021/ti210307.htm

Kelsey, J. (2018), 'How a TPP-Style E-commerce Outcome in the WTO Would Endanger the Development Dimension of the GATS (and Potentially the WTO)', *Journal of International Economic Law,* 21, pp.273–95.

_____ (2021), 'Reconciling Tax and Trade Rules in the Digitalised Economy: Challenges for ASEAN and East Asia', *ERIA Discussion Paper Series No. 395, ERIA-DP-2021-28*, Jakarta: Economic Research Institute for ASEAN and East Asia. https://www.eria.org/publications/reconciling-tax-and-trade-rules-in-the-digitalised-economy-challenges-for-asean-and-east-asia/

Kelsey, J., J. Bush, M. Montes, and J. Ndubai (2020), 'How Digital Trade Rules would Impede Taxation of the Digitalised Economy in the Global South', Third World Network, Penang, Malaysia.

Kozul-Wright R. and R. Banga (2020) 'Moratorium on Electronic Transmissions: Fiscal Implications and Way Forward', *UNCTAD Research Paper No. 47*. https://www.un-ilibrary.org/content/papers/27082814/9

Kynge, J. and S. Yu (2021), 'China and Big Tech: Xi Jinping's blueprint for a digital dictatorship', *Financial Times*, 8 September. https://www.ft.com/content/9ef38be2-9b4d-49a4-a812-97ad6d70ea6f

Montes, M. F., and P. Lunenborg (forthcoming), 'Policy Dilemmas Arising from the Tariff Moratorium on Electronically Transmitted Goods', in L. Chen and F. Kimura (eds.), *Facilitating Digital Trade: Asia's Prospects.* Jakarta: Economic Research Institute for ASEAN and East Asia.

OECD/G20 (2021) 'Statement on a Two-Pillar Solution to Address the Tax Challenges Arising from the Digitalisation of the Economy', 8 October. https://www.oecd.org/tax/beps/statement-on-a-two-pillar-solution-to-address-the-tax-challenges-arising-from-the-digitalisation-of-the-economy-october-2021.pdf

Sen, A. (2021), 'India, South Africa Oppose Plurilateral Initiative for e-Commerce at WTO', *Hindu Business Line*, 6 March. https://www.thehindubusinessline.com/economy/policy/india-south-africa-oppose-plurilateral-initiative-for-e-commerce-at-wto/article34004906.ece

United Nations Conference on Trade and Development (UNCTAD) (2021), *Digital Economy Report 2021. Cross-border Data Flows and Development. For Whom the Data Flow*. New York, NY, US: UNCTAD. https://unctad.org/webflyer/digital-economy-report-2021