**IMPORTANT DIFFERENCES BETWEEN**

**THE FINAL RCEP ELECTRONIC COMMERCE CHAPTER AND THE TPPA   
AND LESSONS FOR E-COMMERCE IN THE WTO[[1]](#footnote-1)#**

The Electronic Commerce chapter of the Regional Comprehensive Economic Partnership (RCEP) has become available. The text is important, as RCEP is one of two major mega-regional negotiations to be concluded since the Trans-Pacific Partnership Agreement (TPPA), which has been promoted as the template for new global rules on digital trade. The US Mexico Canada Agreement (USMCA) extended the TPPA’s digital trade rules to provide even more extensive guarantees and benefits for the already-dominant technology corporations. The RCEP puts a break on those developments.

Six of the sixteen RCEP negotiating parties are also signatories to the TPPA and include the three coordinators of the Joint Statement Initiative (JSI) on electronic commerce at the World Trade Organization (WTO): Australia, Singapore and Japan. Other RCEP Parties include China and, until recently, India who have offensive and defensive interests in regulation of the digital domain, and ASEAN countries like Indonesia and Vietnam who have been actively regulating data and digital transactions.

After protracted negotiations, the agreed RCEP text has omitted or significantly altered several core elements of the TPPA e-commerce chapter and is not enforceable. This retreat from the TPPA template reflects a more mature understanding of the implications of its rules and the need for governments to retain effective policy space to regulate the digital domain. However, the chapter still gives rise to concerns, and leaves unanswered the fundamental objection that rules on Internet governance, data, competition and privacy should not be negotiated in secret under the guise of ‘trade’.

Although there is an express statement that the Parties’ positions in the RCEP chapter are without prejudice to their position in the WTO, the text provides an important point for reflection as countries come under increasing pressure to negotiate on e-commerce in the WTO.

**How RCEP retreats from the TPPA**

There are five fundamental differences between the RCEP and TPPA:

1. **The** **RCEP e-commerce chapter is not enforceable by state-state dispute settlement** (Article 17). Any agreement to allow enforcement in the future, during what is understood to be a five-yearly general review, will only bind those RCEP Parties that agree. Disputes between the Parties over interpretation and compliance are subject only to good faith consultations and potentially reference to the Joint Committee of the Parties.
2. **There is no provision on source code**, which in the TPPA prevents Parties from requiring the owners of the source code of software to disclose it, except where it is used for critical infrastructure. However, there could still be a strong trade secrets provision in the Intellectual Property chapter.
3. **The right of covered businesses to transfer of data offshore, and a ban on requiring them to use or locate servers within a Party’s territory, are made subject to a self-judging public policy test** (Articles 15 and 16). However, only the need to adopt the measure is self-judging, not the legitimacy of the public policy objective. The measure must also not constitute a means of arbitrary or unjustifiable discrimination (which could involve different treatment of technologies or kinds of data, not just of nationalities) or in a manner that constitutes a disguised restriction on trade (which can be problematic when the measure benefits local interests).
4. **The obligations on transfer of data and local computing facilities are also subject to a completely self-judging and non-disputable national security exception.** A Party can adopt any measures it considers necessary for its essential security interests, and such measures cannot be disputed by the other parties. At this stage, the general security exception for the whole of RCEP is not known. However, the explicit protection of such measures from any dispute suggests in these provisions suggests there may not be an equivalent protection in the general security provision.
5. **The moratorium on customs duties on electronic transmissions is not made permanent** (Article 12). This practice is expressly maintained in accordance with the WTO Ministerial Conference decisions related to the WTO Work Programme on Electronic Commerce. Adjustments to this RCEP provision are tied expressly to further ministerial decisions on the Work Programme – and not to the breakaway plurilateral JSI negotiations. If the WTO moratorium lapses, as some developing countries proposed during discussions on its renewal in December 2019, an RCEP Party could unilaterally adjust its practice accordingly.

**Remaining matters of concern in RCEP**

Despite these differences, many worrying features remain. It is possible that governments agreed to these provisions because the chapter is not enforceable. But it might become enforceable in the future and acceptance of the provisions risks establishing them as precedents for other negotiations.

***The scope of RCEP***

* The *objectives* of the chapter are all about promoting the use of e-commerce. There is no attempt to balance regulatory, social or human rights objectives.
* The chapter applies to ‘measures adopted or maintained by a Party that *affect* electronic commerce,’ not just those that directly target it. Judging by earlier leaked texts, a similar broad scope will apply to rules on trade in services, including financial services, which are likely to impose additional constraints on the regulation of digital and cross-border service suppliers and activities.
* The exclusion of *government procurement* refers to the limited definition in the entire agreement. If that follows the common pattern, it will refer only to the *process* of procuring goods or services for the *internal and non-commercial* use of a government.
* The scope of the exclusion for information ‘*held or processed on behalf of a party’* is vague. For example, it is unclear whether it would cover national or sectoral data bases that are co-developed with private interests, or data collected by a private firm as part of a smart city project.
* The previously leaked RCEP investment chapter shows that *covered investment* will include the wide asset-based definition of investment in the Investment chapter, such as enterprises, shares, intellectual property rights, rights under contracts and licenses.
* *Financial institutions*, public entities and financial service suppliers as defined in the financial services annex are excluded from coverage, as are investors in a financial institution or in a financial service supplier. However, the annex will still apply to financial data and various kinds of e-finance and is likely to be equally problematic.

Financial services rules in the TPPA (for example, on non-discrimination, cross-border trade, new financial services and treatment of certain information) apply to measures affecting the supply of financial services, which includes the ‘provision and transfer of financial information, and financial data processing and related software by suppliers of other financial services’.

TPPA also has Annex 11-B. Section B, which guarantees the right of financial firms to transfer data out of the source country for processing as an ordinary part of their business. Governments can have measures to protect data privacy and confidentiality, and require regulatory approval (for prudential reasons) of the recipients of that information – but there is a potentially circular proviso that those measures can’t be used as a means of avoiding this commitment or obligation! It is unclear whether some similar provision is in RCEP. If it is, it could become a major headache for financial regulators.

***Other RCEP Rules***

A number of rules are carried over from the TPPA, although almost all of them have variations.

***Use and location of computing facilities (Art 15)***

* A covered person cannot be required to use or locate computing facilities, such as servers, in a Party’s territory as a condition of doing business there. The core obligation is the same as the TPPA but, as noted earlier, the exceptions are broader.
* Like the TPPA, RCEP allows the adoption of inconsistent measures to achieve a ‘legitimate public policy objective’. However, RCEP makes the decision on whether the measure is necessary self-judging. Whether the public policy objective is ‘legitimate’ could still be challenged.
* The TPPA also requires the measure to be least burdensome to achieve the objective, whereas RCEP leaves the nature of the measure completely to the parties.
* The measure must not be applied in a manner that would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade, both of which could be problematic in relation to a requirement to use local servers.
* Although several aspects of the provision could be challenged, it is important to remember that the chapter currently has no enforcement mechanism.
* In addition, a Party can adopt any measure it considers necessary to protect its ‘essential security interests’ and this explicitly ‘shall not be disputed by other Parties’.
* Finally, the local server rule does not apply to measures that a Party has preserved the right to use in the services and investment chapters. This is complicated, for several reasons. First, those protections *only* apply to the extent there is cross-over between the e-commerce rules and the rules in those chapters that the protections apply to (eg non-discrimination). Because different negotiators are responsible for each chapter, it is quite likely that they have not considered the possible crossover between chapters. Second, a previous leak showed that Parties are using different kinds of schedules to note these protections, and they are required to transition from a positive list, where they set out what is subject to the rules, to a negative list that says what is not protected. Those lists are technically very difficult and there is high risk of error or unforeseen consequences. They also have to be negotiated and agreed among the Parties.
* The LDCs have 5 years’ grace to comply, with a possible 3-year extension. Vietnam has 5 years to comply.

***Cross-border transfer of information by electronic means (Art 16)***

* The general effect of this provision is similar to the TPPA, but with a shift from an active to a passive obligation. The TPPA imposed a positive duty to *allow* a ‘covered person’ to transfer of information, including personal information, across the border for its business. RCEP says a Party shall not *prevent* such transfers.
* The inbuilt exception is identical to Article 15 on local computing facilities. The same cross-reference to reservations in the services and investment chapter also applies.
* The LDCs have 5 years grace to comply, with a possible 3-year extension. Vietnam has 5 years to comply.

***Paperless trading (Art 6)***

* This is a soft ‘endeavour’ obligation to promote the use of, and accept, paperless trading, with the LDCs having 5 years’ grace to comply.

***Electronic authentication (Art 7)***

* A legal signature cannot be rejected solely because it is in electronic form. A Party’s laws and regulations can provide a different rule for specified circumstances. Cambodia and Lao PDR have 5 years to comply.
* Private parties to transactions must be allowed to decide what authentication technologies they want to use and to show these meet states’ domestic laws with respect to authentication. Governments can set performance and/or and certification requirements for a particular category of electronic transactions in their laws or regulations. This rule would prevent RCEP governments from requiring certain levels of cybersecurity etc, such as two-factor authentication for online banking or encryption of credit card details, unless the government has treated them as a special category.

***Consumer protection (Art 8)***

* The RCEP wording is even weaker than the equivalent TPPA provision. It merely requires the Parties to have consumer protection measures, defined as narrowly as providing ‘*protection for* *consumers using electronic commerce against fraudulent and misleading practices that cause harm or potential harm to such consumers’*, without setting any minimum threshold. They have to publish information on the consumer protection they provide.
* The TPPA has no minimum standard either, but at least it requires the adoption of consumer protection laws to *proscribe* fraudulent and deceptive commercial activities that cause harm or potential harm to consumers engaged in *online activities’*.
* The LDCs have a 5-year grace period to comply.

***Online personal information protection (Art 9)***

* The ‘privacy’ provision is also weak and slightly different from the TPPA. Parties must have a legal framework that ‘*ensures* the protection of personal information of the users of electronic commerce’. Personal information is defined as ‘any information, including data, about an identified or identifiable individual’. The TPPA only requires the law to *provide* for protection of personal information and refers to an identifiable *natural person*.
* There is no minimum standard, although a Party must (TPPA said should) ‘take into account’ international standards, guidelines, etc of relevant international bodies.
* As with the TPPA, Parties can comply by adopting a comprehensive personal privacy law or sector-specific laws, or by providing for enforcement of contractual obligations that enterprises adopt.
* They must publish information on the protection they provide (TPPA said should), and encourage enterprises to publish their policies online.
* The RCEP has dropped the TPPA’s rhetorical recognition of the ‘economic and social benefits of protecting personal information’ and the ‘encouragement’ for Parties to promote compatibility between their different legal approaches.
* The LDCs have a 5-year grace period to comply.

***Unsolicited electronic messages* (spam) (*Art 10*)**

* Parties must adopt measures on spam, but these may be limited to particular modes of delivery, such as email, rather than the more lucrative forms, such as unsolicited advertising or targeted messaging.
* The content the measures must contain is weak: suppliers of spam must be required either to ‘facilitate’ recipients stopping the messages, or require their consent, or ‘otherwise provide for minimisation’ of spam, with unspecified ‘recourse’ against suppliers who fail to comply.
* The LDCs have a 5-year grace period to comply, and Brunei has a 3-year transition.

***Domestic regulatory frameworks (Art 11)***

* Parties must maintain a legal framework to govern electronic transactions that ‘takes into account’ the relevant UNCITRAL, UN or other international conventions and model laws on electronic commerce.
* Cambodia has a 5 year grace period.
* Parties must also ‘endeavour’ to avoid ‘any unnecessary regulatory burden on electronic transactions’. Even though the Party must only ‘endeavour’, it still has a positive obligation to do so. This is a version of the disciplines on domestic regulation of services that require light handed approaches to regulation and which many developing countries have resisted in the WTO.

***Customs duties on electronic transmissions*** ***(Art 12)***

* As noted above, the RCEP maintains the currentWTO moratorium on customs duties. However, electronic transmissions are not defined. That leaves it unclear whether the moratorium applies to all material transmitted electronically, including content, as the US has claimed, or does not apply to electronically-transmitted goods and services, as Indonesia confirmed with the WTO Secretary General (WT/MIN(17)/68, 20 December 2017).
* Unlike the TPPA, the moratorium is not made permanent. If there is a new outcome from the 1998 WTO Work Programme on Electronic Commerce (which might be a permanent ban, a longer term, or to let the moratorium lapse), it is left to each RCEP Party to decide whether to adjust its approach to reflect that new position.

***Transparency (Art 13)***

* Parties must make their general measures that comply with this chapter available publicly, at least on the Internet – although only ‘as promptly as possible’ and ‘where feasible’. They must also respond as promptly as possible to requests from another Party for specific information about those measures.

***Cybersecurity (Art 14****)*

* As with the TPPA,there is a reference to the issue of cybersecurity, but no obligation to do anything about it.

***Obligations in other chapters (Art 3.5****)*

* The e-commerce chapter makes it clear that the Parties’ obligations, and related exceptions, in the trade in services and investment chapters still apply. Those chapters are more problematic than the e-commerce chapter, for several reasons.
* The trade in services rules apply to ‘measures affecting the supply’ of services a Party. Many of the measures referred to in the e-commerce chapter might arguably fall under that description, where a Party has committed the relevant service in its schedule (for a positive list) or not explicitly protected it (under a negative list approach). Covered services include ‘computer and related services’, including data processing and storage, as well as sectoral services, such as legal, financial, advertising, retailing and tourism services, whether they are provided in-country or across the border.
* The services chapter is also likely to include a rule that governments cannot require a cross-border service supplier to have a local presence in the country, although that can be subject to a reservation in a country’s schedule.
* Those services obligations will presumably be enforceable through state-state dispute settlement.
* Measures that allegedly breach investor protections, such as non-discrimination, fair and equitable treatment, or direct or indirect expropriation, could also be subject to state-state and investor state dispute settlement.

1. # Professor Jane Kelsey, Faculty of Law, The University of Auckland, New Zealand, 11 February 2020. This analysis refers to the final un-scrubbed text of the Electronic Commerce chapter of the Regional Comprehensive Economic Partnership, accessible at https://bilaterals.org/?rcep-e-commerce-chapter-text-41085 [↑](#footnote-ref-1)