Towards an Asia-Pacific Digital Economy Governance Regime

Authors

Shiro Armstrong, Associate Professor, The Australian National University and Visiting Fellow, Research Institute of Economy, Trade and Industry.
Rebecca Sta Maria, Executive Director, APEC Secretariat, Singapore.
Tetsuya Watanabe, Vice President, Research Institute of Economy, Trade and Industry

Contributing specialists

Wendy Cutler, Vice President, Asia Society Policy Institute
Deborah Elms, Founder and Executive Director, Asian Trade Centre
Yiping Huang, Professor of Economics and Deputy Dean, National School of Development and Director, Institute of Digital Finance, Peking University
Bilahari Kausikan, Chairman, Middle East Institute, National University of Singapore
Peter Lovelock, Director, Technology Research Project Corporate
Joshua Meltzer, Senior Fellow, Global Economy and Development, Brookings Institution

April 2021

Suggested citation:
Armstrong, S., R Sta Maria and T. Watanabe, 2021, 'Towards an Asia-Pacific Digital Economy Governance Regime', Research Institute of Economy, Trade and Industry.

Corresponding authors: shiro.armstrong@anu.edu.au and watanabe-tetsuya@rieti.go.jp

Key recommendations

Middle powers can lead the creation of solutions to fragmentation of the international digital economy. Geopolitics are contributing to a digitally divided global economy with strategic rivalry between China and the United States, leading to digital decoupling and contributing to a more fragmented digital global economy. Middle powers like Australia and Japan are well positioned to find creative solutions and groupings that are inclusive. ASEAN could be central to progress in achieving an Asia-Pacific Digital Economy Governance Regime.

As a first step, multilateral rules in the digital economy must be designed to limit discrimination, promote transparency, openness, fairness and predictability and constrain protectionism among diverse and sovereign digital regimes. There are system differences between countries: there is diversity in systems of government, economies, digital maturity and readiness, approaches to data privacy and ownership, governance regimes and attitudes to international trade and investment. A multilateral digital governance regime allows governments to set their own policies and retain sovereignty while multilateral rules limit discrimination, promote transparency and predictability, and constrain governments from protectionist policies.

An Asia-Pacific Digital Governance Regime must encompass not just traditional trade issues but issues such as trusted data access, protection of privacy and security, competition policy and norms governing emerging technologies, including AI and fintech. An Asia-Pacific Digital Economy Governance Regime will have to comprehend a wider range of issues beyond traditional trade issues and existing agreements and initiatives including trusted access to data, protecting privacy and security, competition policy and formulating agreed norms to govern artificial intelligence and fintech.

Common rules and standards must be guided by forward-leaning multilateral principles, avoiding a lowest common denominator approach, by building trust across different sovereign systems through technical and economic cooperation. Developing a common set of rules and standards will need to be guided by multilateral principles and to build on sectoral approaches while avoiding a lowest common denominator approach. Different philosophies and values among countries can be bridged over time with technical and economic cooperation that builds trust and confidence.

APEC has a unique role to play in mobilizing governments, technical experts and business to promote economic cooperation on digital trade facilitation and progress on an Asia Pacific Digital Governance Regime. An economic cooperation process needs to involve multiple stakeholders, including governments, big tech companies, small and medium sized companies, entrepreneurs, investors, workers, consumers and technological experts. These groups can be mobilised in existing cooperation frameworks like APEC. An economic cooperation agenda should be developed around shared and common interests in areas such as digital trade facilitation in a mutually beneficial way with real and demonstrable gains.

An APEC or other regional initiative on Asia Pacific digital governance should be founded on open regionalism and interoperability with other regimes. International cooperation should adopt an open regionalism approach for a global perspective beyond the Asia-Pacific and create interoperability with other regimes.

Risk mitigation can be achieved through technical solutions and increased competition over time. Competition, technical solutions and agreed principles and rules can help manage and mitigate risk. Introducing more competition takes time and needs to be done with governance that identifies and reduces risk within and across borders; requiring international cooperation and experience sharing.

Governance needs to ensure the digital economy is inclusive and narrows the digital divide within and between countries. To be credible and sustain broad support, digital governance should narrow the digital divide, promote digital inclusiveness and facilitate and bolster the participation of SMEs in international trade.

The Digital Economy

The digital economy is the new economy, underpinning productivity growth, development and prosperity globally. The COVID-19 pandemic accelerated the digitalisation of economies as societies adjusted to social distancing and rapid responses in healthcare, education and service delivery.

The sources of innovation and technological progress are increasingly diffuse. The United States accounted for 28.8 percent of global R&D expenditure in 2018 measured in purchasing power terms (down from 69 per cent in 1960), with China accounting for 23.1 per cent with Japan in third place with 8.5 per cent and Germany in fourth with 7 per cent. China overtook the United States in 2020 as the largest source of international patent applications with Japan third and Asia accounting for 52.4 percent of global patent applications.

In the absence of multilateral rules governing the digital economy, a patchwork of bilateral, regional and plurilateral agreements are setting some standards and rules that cover some aspects of digital trade. There is a global governance deficit that now needs urgent attention.

Geopolitics are also contributing to a digitally divided global economy. The strategic rivalry between China and the United States is leading to digital decoupling and contributing to a more fragmented digital global economy.

Digital protectionism is on the rise, fueled by the lack of multilateral rules and norms, interest in promoting home-grown companies, as well as geopolitical rivalry. Since much of the digital economy has more features of a public good, barriers are particularly detrimental for economic growth and development. A digitally divided global economy will affect supply chains, productivity, peoples' livelihoods, and reduce the growth potential of economies, including those at the technological frontier.

Governments are struggling to balance competing policy objectives, including privacy, intellectual property, consumer protection and competition policy. There is much that governments could learn from one another, particularly in developing and articulating frameworks that consider these disparate trade-offs. But the current trajectory is to have a plethora of inconsistent policy frameworks across jurisdictions.

This paper sets out the issues, reviews the state of play and suggests ways forward towards an **Asia-Pacific Digital Economy Governance Regime**. The Asia-Pacific includes China, the United States, and countries that are proactively engaged in rule-making. East Asia is the most data rich region in the world. There are shared global interests and common challenges as well as huge potential productivity and growth gains from agreeing to principles and rules by which to govern the digital economy and engaging in dialogue and cooperation for confidence and trust building. A patchwork of inconsistent and disparate policies and regulations across the region risks losing the biggest productivity boost in recent history.

How is digital different?

Physical distance almost no longer matters for international commerce and exchange. Information sharing and the cost of transporting digital goods and services is virtually zero.

Data is non-rival so the same data can be used by many companies simultaneously and there are increasing returns, potentially compounding the benefits from mutually beneficial exchange across the global economy, with implications for property rights over data.

Digital platforms like messaging apps, social networking and search are usually dominated by a few major companies because they exhibit economies of scale, network effects (where their value is derived from the number of users) and are often free for consumers and scalable at very low cost. Many platforms are two-sided markets and that has implications for governance and competition policy within and between countries.

Data is already dominating the old economy, for example, with intangibles now making up 84 percent of the S&P, up from around 10 percent just 20 years ago. Without setting the rules now, more and more of the global economy will face increasing protectionism as data continues to spread.

A key principle for approaching the governance of the digital economy across borders is to start with the free flow of data, only allowing exemptions when they can be justified by agreed and transparent criteria. That is similar to trade in goods, where clear and agreed criteria for domestic health and quarantine exemptions and some trade remedies are allowed. Exemptions or carve-outs for security, privacy and other domestic imperatives should be areas for dialogue, cooperation and confidence building leading to agreement over time. Security of data can facilitate new economy markets, but there is little consensus on what rules should govern data access and trading of data. This paper sets out ways to mitigate risks and facilitate agreement.

Security of all nations is enhanced when countries cooperate in setting rules where each sees benefit from being close to the technology frontier, rather than attempting to push some countries away from it. Winners take all network effects will likely continue to create strong incentives to build domestic champions but they will be in a more competitive international environment under an open and transparent international regime with agreed principles and rules.

Bottom-up rule-making

Existing initiatives and agreements have sought to create rules and understanding between smaller groupings of countries. By their very nature they are all limited in membership and coverage of issues but do set standards and potential language for application to future agreements and start to put some of the scaffolding together for a regional and global architecture of digital agreements.

A list of key regional agreements and coverage of issues can be found in the attached Table.

The following principles should guide future cooperation in creating a Digital Economy Governance Regime:

- Adopt initiatives and standards where bigger groupings can make progress, such as in the **APEC Cross Border Privacy Rules** (CBPR).

- Build confidence and cooperation multilaterally with agreed principles through vehicles like the **Data Free Flow with Trust (DFFT)** from the Osaka Track, which had 24 countries including the United States and China sign on to the Osaka Declaration on Digital Economy.

- Design agreements to expand membership of arrangements like the Chile, New Zealand and Singapore **Digital Economy Partnership Agreement (DEPA)** and mega regional agreements, the Comprehensive and Progressive Agreement for Trans Pacific Partnership (**CPTPP**) and Regional Comprehensive Economic Partnership (**RCEP**), towards open plurilateral agreements that can be multilateralised like the **WTO E-Commerce agreement**.

Bilateral and regional agreements can compete to set standards but the rule-making ideally needs to be consolidated to avoid a digitally divided global economy. Forums like APEC that are non-binding cooperative groupings can help make progress on principles and bring larger groups of countries together.

Existing agreements work to further digital trade and have been concerned with keeping cross border data flows open, facilitating digital trade, building government-to-government, business and consumer trust, protecting personal information, and with some cooperation on fintech, small and medium sized enterprises and cyber security. A *Digital Economy Governance Regime* will include digital economy issues beyond negotiated digital trade agreements.

Many agreements have security ‘carve-outs’ that exempt members from the free flow of data, and data localisation commitments. These exemptions are often broad and can severely weaken commitments. For example, RCEP Articles 12.14 and 12.15 make clear that provisions for data localisation and free flow of data are exempt from

> “*any measure that it considers necessary for the protection of its essential security interests. Such measures shall not be disputed by other Parties*”.

Managing and mitigating risk

Security exemptions in digital agreements are the most contentious and difficult area to resolve. The security carve-outs leave large gaps in existing agreements that need to be resolved over time to avoid a fractured architecture of the global digital economy. The risks are serious and real with malicious use of private data by state and non-state actors, cyber attack and disruption. These risks need to be and can be dealt with in the following ways.

Competition can mitigate risk of malicious use of private data by transferring the security or other risk to private enterprise. Agreed multilateral rules and principles on domestic regulation to strengthen competition, reduce barriers to entry and expansion, and address competition challenges in the digital space can help shift risks from societies and consumers to private enterprises, changing incentives and behaviour. Introducing more competition takes time and needs to be done with governance that identifies and reduces risk within and across borders; requiring international cooperation and experience sharing.

- ★ **Platforms** that rely on large numbers of users and network effects will be punished by users and lose market share quickly if they breach the trust of consumers, provided the market is competitive and switching costs are not prohibitive. Platforms in any country have an incentive to protect the data of their users with cyber security and transparent terms and conditions that maintain the trust of users. That incentive can be enhanced with appropriate governance. With more competition, more transparency and more alternative platforms, the disincentive to lose the trust of users is higher.

- ★ **Hardware bottlenecks and choke points** can be alleviated by competition. Concentration of production and supply of semiconductors, strategic materials and information and communications technology are all risks that can be alleviated or even avoided by increased competition. Avoiding vertical integration of production and allowing competition, including from foreign companies, in each stage of production will increase alternative suppliers and shift risk to private enterprises.

- ★ **Increased competition, including between China and the United States**, under agreed multilateral rules instead of bans for strategic, security or protectionist reasons will increase innovation, productivity and reduce risks borne by governments and societies. Agreed principles and rules can lead to competition that leads to measures to outperform other countries instead of undermining them.

Domestic laws are important for protecting against data misuse or privacy breaches by foreign and domestic actors. Clear, consistent and enforceable domestic laws around privacy and market integrity requirements and compliance testing with serious penalties are an important protection against cyber risk. Domestic laws can be the source of trust as well as barriers to trade.

The report Asymmetric Competition: A Strategy for China & Technology by a group of influential American tech and foreign policy leaders sets out a framework for evaluating and managing risk (China Strategy Group, 2020)[1].

A. **Acceptance of dependency** of a foreign owned platform or technology.
B. **Specific concessions negotiated** between countries.
C. **Specific technical requirements** in areas such as data storage, data privacy, open standards, code audits and encryption.
D. **Proactively enable technology** to mitigate future risks.
E. **Ban** as a last resort.

The US China Strategy Group (2020) argues:

> *Banning would represent a failure to have acted swiftly in years prior with options B, C, or D at an earlier stage. While it may be necessary in some cases, this should be seen as a last resort and with a clear articulation of why the risks inherent in the platform are not remediable through negotiation, legislation, or technology.*

An *Asia-Pacific Digital Economy Governance Regime* could install a process of dialogue, cooperation and confidence building so that the global digital economy can realise more competition and countries can agree to multilateral rules and norms that involve options A, B, C and D, and agree to avoid bans (option E).

Negotiated conditions to avoid option E will likely include requirements for disclosure and transparency, technical requirements, data localisation, open standards, open source and code audits. Banning hardware or platforms from other countries leads to less competition, retaliation and a concentration of production and supply risks globally. Cyber risk matters regardless of ownership of data assets and banning ownership is often the wrong option.

Data protection is a key priority to build trust: how it is protected, used, audited and accessed by governments. Trust measures will be an enabler for data flows. The issues include:

- Data privacy, use (access and re-access) and sharing
- Cyber security
- Data localisation
- Source code, algorithm and cryptography (proprietary information) protections

Increased global competition and multilaterally negotiated concessions, rules, technical requirements and agreed enabling technology standards can be the basis for confidently allowing foreign companies to own data assets and provide digital services. Domestic regulation can and should be supplier-blind.

[1] The report targets China and is concerned with maintaining US technology leadership but its framework for managing risk can be generalised to include, for example, conditions for American owned technology companies operating in other countries.

From regional to global digital economy governance

There are **system differences** between countries: there is diversity in systems of government, economies, approaches to data privacy and ownership, governance regimes and attitudes to international trade and investment. These differences are not confined to those between China and the United States. With a multilateral digital governance regime governments can set their own policies and retain sovereignty, but just like in the WTO, **multilateral rules** can limit discrimination, promote transparency and predictability, and constrain governments from protectionist policies that result in a prisoner's dilemma outcome with everyone worse off.

Strategic competition between China and the United States has led to a myriad of restrictions, resulting in some degree of technological decoupling. Other countries are increasingly having to make choices between Chinese or US technology, limiting their economic and strategic policy space. An Asia-Pacific Digital Economy Governance Regime can gradually turn strategic competition into market competition that reduces risks and encourages productivity enhancing innovation.

Bundling issues together may help to tackle fundamental differences and allow for policy trade-offs between different interests. State-related cyber security issues should be part of a broader dialogue and confidence-building, to be discussed alongside positive-sum mutually beneficial digital trade and digital economy cooperation between countries. Engaging in mixed-interest exercises by bundling positive sum with zero- or negative-sum issues may help to restrain adverse actions.

Adopting an **open regionalism** approach will mean an Asia-Pacific Digital Economy Governance Regime will have a global perspective beyond the Asia-Pacific that includes interoperability with other regimes. An open regionalism approach that involves regional economic cooperation and integration without discrimination against economies outside the region will be inclusive of other countries and regions, including proactive cooperation with India and South Asia.

With strategic competition between China and the United States, and geopolitics making it difficult for rule-making among all Asia-Pacific countries, middle powers like Australia and Japan are well positioned to promote creative solutions and groupings that are inclusive. ASEAN centrality could be important in achieving an Asia-Pacific Digital Economy Governance Regime given its consensus driven approach and open regionalism nature.

Cooperation agenda for an Asia-Pacific Digital Economy

An Asia-Pacific Digital Economy Governance Regime will have to comprehend a wider range of issues beyond traditional trade issues and existing agreements and initiatives (see attached Table). There are shared interests that suggest dialogue and cooperation which can build confidence and trust. Government access to data, censorship, surveillance and privacy violations are issues that cut across many countries with different systems of government. And regulating different aspects of big tech companies is a common challenge between countries. Agreed norms to govern the development of artificial intelligence and fintech will be important to maintain confidence for consumers and avoid unintended consequences.

The digital economy is fast becoming pervasive across every economy and just like all other domestic regulation, much of the regulation of it cannot easily be negotiated in international agreements. But digital commerce knows no borders and regulatory coherence or alignment and best practice regulation and governance can help facilitate better domestic outcomes and a deeper and more efficient international digital economy.

There is a need to set international standards and agreed principles to help guide domestic regulation and regional cooperation. Non-binding and voluntary international cooperation and collaboration on sensitive issues can help to build trust and avoid policy reversals and unintended consequences that may bring retaliation.

A cooperation agenda around technical cooperation, capacity building and experience sharing can help build confidence and trust, and over time forge consensus. Collaborative work in areas such as trade facilitation in the digital space is a mutually beneficial way forward with real and demonstrable gains.

Technical cooperation, capacity building and experience sharing can:

- Help find technical solutions to sensitive issues
- Bring together officials, business, consumer groups and specialists from different backgrounds to approach issues holistically
- Understand where carve-outs in the name of security are being used for protectionism
- Help governments balance privacy, intellectual property, consumer protection and competition policy with innovation
- Help find ways to manage disruption from innovation
- Build confidence and trust between different actors and between countries

Lifting restrictions to foreign participation will require dialogue, cooperation and confidence- and trust-building. Regulatory harmonisation and rule-making can help open markets and increase competition. Measuring restrictions to digital trade can help identify areas for liberalisation and reform. Priorities include:

- Opening up fintech to international cooperation
- Prohibiting customs duties on digital transactions
- Commitment to avoid restrictions on cross-border data flows
- Commitment to non-discrimination

Regulatory coherence between markets can help bridge and minimise digital divides. Developing digital infrastructure and creating international regulatory coherence in digital trade protocols will promote e-commerce but also enhance visibility across supply chains and help identify vulnerabilities. Regional data privacy standards, tax and other incentives to share data will encourage the use of digital supply networks. e-invoicing and e-payments systems should be aligned with international frameworks.

Regulatory coherence or harmonisation can increase interoperability and introduce more competition in platforms and competition along the supply chain, avoiding hardware bottlenecks and choke points for semiconductors and strategic materials. DFFT includes measures to increase interoperability that encourages innovation, fosters competition and increases consumer choice between countries.

Best practice regulation and governance of new technology and the digital economy is rapidly evolving. There is significant scope for mutually beneficial cooperation to share experience, skills and intelligence on how to protect personal information, reduce barriers to digital trade and govern the digital economy. Trust in platforms, service providers and technologies (such as autonomous vehicles), as well as trust in legal frameworks and regulation will be crucial to realising the growth potential of the digital economy. Issues such as shifting ownership and control of data to consumers and competition policy for two-sided markets can be advanced through experience sharing and cooperation.

Domestic policy can be guided by best practice to introduce competition, avoid regulations that stifle innovation and narrow the digital divide. Areas such as immigration policy, attracting skilled workers and education systems have less scope for international cooperation but areas such as R&D and intellectual property policies that do not impede joint research would benefit from experience sharing and international dialogue. For sustainable transformation and international collaboration governments will have to show how an Asia-Pacific Digital Economy Governance Regime will benefit consumers and society.

The APEC economic cooperation agenda can be activated, better supported, and mobilised for technical cooperation and capacity building. Regional cooperation should pursue an open regionalism approach that is not at the expense of non-members.

Further reading

China Strategy Group (2020) *Asymmetric Competition: A Strategy for China & Technology, Actionable Insights for American Leadership*.

Triole, Jean (2017) *Economics for the Common Good*, Princeton University Press, Princeton and Oxford. (Chapter 14).

Ferracane, Martina, Hosuk, Lee-Makiyama and Erik van der Marel (2018) *Digital Trade Restrictiveness Index*, European Center for International Political Economy (ECIPE).

De Brouwer, Gordon (2019) *Bringing Security and Economics Together in the National Interest*, paper presented to the RIETI-ANU Symposium, Asian Integration and the Global Economy: Economics of geopolitics. https://www.rieti.go.jp/jp/events/19112101/pdf/s-1_brouwer_paper.pdf

Elms, Deborah (2020) *Digital trade in the Asia-Pacific: Issues for 2021 and beyond*, Hinrich Foundation.

Table of Digital Trade Agreements and Issue Coverage

	DEA, DEPA	CPTPP, USMCA, US-J	RCEP, DFFT	WTO E-Commerce
Keeps cross-border data flows open	- Affirm prior commitments on limiting data localisation requirements as a condition of doing business in jurisdictions party to the agreement (no party shall prevent another form measures to achieve a legitimate public policy objective as long as it's not arbitrary/unjustifiable); - Affirm prior commitments on limiting restrictions on cross-border data flows for conduct of business (no party shall prevent another form measures to achieve a legitimate public policy objective as long as it's not arbitrary/unjustifiable) - DEA and DEPA participants have agreed to these measures on cross-border data flows in other agreements, including CPTPP	- No data localisation requirements as a condition of doing business (under *location of computing facilities*; but no party shall prevent another from adopting or maintaining measures to achieve a legitimate public policy objective as long as it's not arbitrary/unjustifiable discrimination); - **Commitment to not impede any party to providing cloud computing and data storage services to other parties in CPTPP**; - No restrictions on cross-border transfers of information by electronic means for conduct of business (but similar to above, no party shall prevent another form measures to achieve a legitimate public policy objective as long as it's not arbitrary/unjustifiable); - *No party can be prohibited from access to any information the disclosure of which it determines to be contrary to its essential security interests AND no party can restrict the maintenance or restoration of international peace or security, or the protection of its own essential security interests*	- No data localisation requirements as a condition of doing business (Cambodia, Laos, Myanmar and Vietnam are exempt AND *each party may have its own measures on the use or location of computing facilities, including requirements that seek to ensure the security and confidentiality of communications* AND includes arbitrary/unjustifiable provisions on policies that might restrict locations of computing facilities AND parties that put in place restrictions decide themselves if they are legitimate or not); - No restrictions on cross-border data flows for conduct of business (with similar exceptions to above) - **DFFT looks at differences in data transfer mechanisms (i.e. how regulatory regimes impact how data is transferred across borders in different jurisdictions, including: no regulations, ex-post regulations, adequacy determinations, case-by-case assessments)**	- Discussions on data flows, localisation requirements, source code protections
Facilitates digital trade	- Confirms the prohibition of customs duties on e-commerce (this is a **binding commitment** under DEA and DEPA); - Affirm prior commitments on non-discriminatory treatment of digital products (includes carve out for IP protections where this may not apply if there is any inconsistency with the rights and obligations related to IP); - DEPA requires e-invoicing and e-payments alignment with international frameworks for better interoperability (**DEA supports alignment of e-payments with ISO system**); - Promote paperless trading and alignment of authentication and e-signature protocols with international standards (**DEA develops e-certification protocols for agricultural goods trade**); - Underscore importance of open access to the internet for e-commerce	- Prohibits customs duties on e-commerce; - Ensures non-discriminatory treatment of digital products (includes carve out for IP protections where this may not apply if there is any inconsistency with the rights and obligations related to IP); - Promotes paperless trading and encourages **interoperable electronic authentication** and recognises legal validity of e-signatures; - Underscores importance of open access to the internet for e-commerce - Electronic transactions are governed under a legal framework built around the *UNCITRAL Model Law on Electronic Commerce 1996* in the USMCA and US-J agreements;	- Prohibits customs duties on e-commerce; - Promotes paperless trading and encourages **interoperable electronic authentication** and recognises legal validity of e-signatures; - **DFFT considers the need for greater interoperability in legal frameworks, regulatory standards** (possibly towards binding treaties) to facilitate digital trade	- Moratorium on Customs Duties on Electronic Transmissions - Discussions on standard setting for e-signatures, authentication
Builds government-government, business and consumer trust	- DEPA has a modular design which emphasises building consensus around principles among current and future members. Future members do not need to accede to all modules and can instead pick up individual modules of their choosing. - Affirm the importance of and prior commitments related to prohibitions on access to and the transfer of source code as a condition for import, distribution, sale or use of software (regulatory authorities can request code as long as it doesn't negatively impact the source code's status as a trade secret **DEA explicitly extends these protections to SMEs**); - Prohibit forced transfer of technology, production processes or other proprietary information as a condition of conducting business; - DEPA underscores the importance of 'rich and accessible public domain'[2]; - Toward digital ID interoperability and a safe online environment, includes protections around unsolicited communications i.e. spam (DEPA does not have provisions on or consider online safety); - Encourage open access to government data for enhancing and generating business and research opportunities; - Include transparency chapter/module and encourages timely notification when a party adopts parts the agreement, or changes domestic regulations related to matters set out in the agreement, and gives sufficient time for the other party to respond (**DEPA also encourages open administrative**	- Prohibits access to, transfer of source code as a condition for import, distribution, sale or use of software (regulatory authorities can request code as long as it doesn't negatively impact the source code's status as a trade secret); - Prohibits forced transfer of technology, production processes or other proprietary information as a condition of conducting business (source code protections do not cover software used for critical infrastructure i.e. a party can request access to, transfer etc of source code used in critical infrastructure), an important security carve out - Includes protections around unsolicited communications; - Opens up access to government data for enhancing and generating business and research opportunities	- **Identifies issues related to source code transfers as a matter open for further dialogue**; - Includes online consumer protections, related to fraud and harm; - Includes protections around unsolicited communications; - See note on encouraging dialogue below	- Discussions advanced on building consumer trust through limitations on Spam/unsolicited communications

[2] https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement-depa/depa-modules/#bookmark6

	proceedings, and impartial and independent review or appeal mechanisms)			
Includes mechanisms to operationalise agreement	- DEPA is open to new members on a module-specific basis; - Intention to foster greater government-government cooperation at all levels of the agreement; - **DEA includes government-government MoU's that aim to build cooperation at departmental level** (these are absent from DEPA); - Encourages stakeholder engagement **(DEA makes clear intention to hold a Digital Economy Dialogue involving government and non-government stakeholders, DEPA includes provision to set up separate memoranda if needed and establishes a joint committee to consider implementation and operation of the agreement**); - Encourage sharing of best-practice procedures, policies and intelligence sharing at government-government level (**at government departmental level for DEA**)	- Intention to foster greater government-government cooperation at all levels of the agreement; - Encourages sharing of best-practice procedures, policies and intelligence sharing at government-government level (and encourage private sector development of *methods of self-regulation that foster e-commerce*);	- See note on encouraging dialogue below	- Discussions on digital infrastructure gaps/digital divide
Prioritises personal information protection	- Encourage the adoption or maintenance of a legal framework that protects personal information and suggests considering APEC's CBPR system on privacy when developing these legal frameworks (**DEPA mirrors APEC's CBPR framework, underscores importance of collection limitations, data quality, purpose specifications, use limitations etc on personal information**); - **DEA includes MoU between the Office of the Australian Information Commissioner and the Personal Data Protection Commission of Singapore, for cooperation on sharing best practice for protecting personal information** (DEPA makes clear intention to mutually recognise parties' data protection trustmarks to facilitate cross-border information transfers and protect personal information) - DEA assures domestic privacy laws apply to personal data when transferred overseas (e.g. Australian Privacy Act 1988 applies to	- Encourages the adoption or maintenance of a legal framework that protects personal information, and may be congruent with existing international frameworks (countries without a legal framework protecting personal data—Brunei Darussalam and Viet Nam—are not required to apply the personal information protection article before they implement relevant legal protections). Note that **USMCA recommends taking account of APEC's CBPR system and the OECD privacy guidelines for legal framework development** and recognises that the ***APEC CBPR system is a valid mechanism to facilitate cross-border information transfers while protecting personal informatio***n; - Parties should publish information on how to pursue remedies on personal information breaches	- Encourages the adoption or maintenance of a legal framework that protects personal information, and parties should take account of existing international frameworks on protecting personal information (Cambodia, Lao and Myanmar are exempt); - Parties should publish information on how to pursue remedies on personal information breaches	- Discussions on online consumer protection
Addresses cybersecurity risks	- Commitment to and recognition of the importance of strengthening domestic cybersecurity response capacity; - Aim to cooperate on cybersecurity workforce development, mutual recognition of qualifications	- Commitment to and recognition of the importance of strengthening domestic cybersecurity response capacity (**USMCA encourages parties to promote a risk-based approach to managing cyber security over *prescriptive regulations***); - Underscores importance of cooperation on cyber security through the work of national computer emergency response teams	- Encourages building relevant domestic cybersecurity authorities and the exchange of best-practices	
Sets out areas for cooperation on new and emerging technologies, and other areas	- Explore opportunities to collaborate on FinTech development **(DEA includes RegTech collaboration too**); - DEPA and DEA include a module/chapter on cooperation on competition policy but the risks that well designed competition policy could mitigate are not made clear in either agreement; - DEPA modules are comprehensive and set out what principles on governing the digital economy can and should inform future regional or multilateral rules/agreements; - Aim to cooperate on talent development and cultivation of shared ethical standards on Artificial Intelligence; - **DEA includes provision on deepening cooperation on submarine cable installation, maintenance and repair**; - Emphasis on SME cooperation (**DEPA intention to convene Digital SME dialogue**); - **DEPA promotes digital inclusion; rural internet connectivity, women's economic participation, indigenous access to technology**; - **DEPA puts strong emphasis on building *the wider trust environment in the digital economy*; and underscores the importance of fostering business and consumer trust through online consumer protection, spam prohibitions;** - **DEA Australia–Singapore Digital Standards Report for cooperation on digital standards** - DEPA's modular design and emphasis on building consensus around non-binding principles it has not attracted new members since its inception (except interest shown by Canada)	- Commitment to assist SMEs to overcome obstacles in using e-commerce (**USMCA recognises the importance of promoting interactive computing services, particularly for SMEs, as vital to digital trade growth**); - **Internet platforms—i.e. social media platforms—that host third-party content aren't liable for harm related to the content they carry under USMCA** (uncertain whether the same applies in US–J or in CPTPP)[3]	- Recognition of the usefulness of further dialogue on e-commerce, including on source-code protections, location of computing services in financial services, cross-border data flows, and current and emerging issues	

3 https://www.nortonrosefulbright.com/en/knowledge/publications/c68efe38/usmca---impact-on-digital-trade

Key: DEA = Australia-Singapore Digital Economy Agreement; DEPA = New Zealand–Singapore–Chile Digital Economy Partnership Agreement; CPTPP = Comprehensive and Progressive Trans-Pacific Partnership; USMCA = United States-Mexico-Canada Agreement; US-J = US-Japan Digital Trade Agreement; RCEP = Regional Comprehensive Economic Partnership; DFFT = Data Free Flow with Trust.