Draft dated January 2021; Forthcoming in European Yearbook of International Economic Law

Digital Trade in the Australia – EU FTA: A Future-Forward Perspective

Neha Mishra*

Contents

1 Introduction 2
2 Significance of Digital Trade in Australia and the EU 4
3 Digital Trade Chapters in EU and Australian FTAs: A Comparative Assessment 6
3.1 Digital Trade Provisions in EU PTAs 6
3.2 Digital Trade Provisions in Australian PTAs 11
4 Digital Trade in Australia-EU FTA: Possibilities and Challenges 17
4.1 EU's Proposed Digital Chapter in the Australia – EU FTA 17
4.1.1 Scope and Applicability of the Digital Trade Chapter 17
4.1.2 Right to Regulate and Applicable Exceptions 18
4.1.3 Data Flows and Privacy 18
4.1.4 No-Prior Authorisation 20
4.1.5 Other Digital Trade Provisions 20
4.2 Placing the Australia – EU PTA in the Digital Trade Realm: A Future-Forward Approach 23
4.2.1 Data Protection and Privacy 23
4.2.2. Boosting the Growth of MSMEs 25
4.2.3 Experimenting with New Models of Cooperation 26
5 Conclusion 26
References 27

Abstract *This paper assesses the significance of the Digital Trade Chapter of the Australia – EU FTA and focuses on the disciplines necessary to boost digital trade. In the ongoing negotiations, the EU and Australia are likely to agree upon conventional digital trade disciplines (e.g., e-signatures, e-authentication, paperless trading, customs duties on electronic transmissions) as well as provisions on online consumer trust and spam, and more contemporary disciplines on source code disclosure and data localisation. These disciplines can undoubtedly contribute to boosting digital trade between Australia and the EU. However, data flows and data protection will remain a sticky issue in the ongoing negotiations, given the differences in data protection laws of the EU and Australia, and the EU's exceptionally defensive approach in data protection. Instead of bypassing such issues, the FTA negotiators should view the negotiations as an opportunity to build mutual consensus and foster cooperation in formulating standards and mechanisms for data transfer. Further, the negotiations*

* Lecturer, ANU College of Law

provide an opportunity for adopting deeper disciplines on digital trade facilitation that can nurture start-ups as well as experimenting with novel models for regulatory cooperation in nascent policy areas including AI ethics and open government data.

1 Introduction

The European Union ("EU") and Australia started negotiating a Free Trade Agreement ("FTA") on 18 June 2018.[1] Since then, both parties have completed nine rounds of negotiations, the last round being from 30 November to 11 December in 2020.[2] In 2019, the two-way trade between Australia and the EU was estimated to be a total of AUD 85 billion.[3] The EU is Australia's second largest trading partner and the largest source of foreign investment in Australia,[4] while Australia was the EU's 21st largest trading partner in 2019 in merchandise trade.[5] Both the EU and Australia share a "long-standing and fruitful bilateral relationship",[6] with a "shared commitment to the rule of law, global norms and free and open markets".[7] Further, Australia and the EU converge on "many global economic issues and cooperate to promote international prosperity in the World Trade Organization and G20".[8]

This paper focuses on the digital trade chapter in the *Australia – EU Free Trade Agreement* ("Australia – EU FTA"). Digital trade refers to all digitally enabled transactions facilitating the delivery of goods and services, irrespective of whether this occurs virtually or physically.[9] With the growing digitalisation of the economy, electronic commerce chapters (or digital trade chapters, as they have more recently been named) have become commonplace in Preferential Trade Agreements ("PTAs").[10] The first generation of electronic commerce chapters were developed at the turn of this century by the United States ("US") and then subsequently adopted by Singapore and Australia in several of their bilateral trade agreements.[11] Since then, the number of trade agreements containing provisions on electronic commerce have increased substantially.[12] Further, recent PTAs cover a much broader range of electronic commerce issues, and in greater depth, including rules in sensitive areas such as data flows and data localisation, source code disclosure/trade secret protection, and

[1] Department of Foreign Affairs and Trade ('DFAT'), Australia-European Union Free Trade Agreement, www.dfat.gov.au/trade/agreements/negotiations/aeufta/Pages/default#:~:text=Australia%20and%20the%20European%20Union,source%20of%20foreign%20investment1 (last accessed 12 December 2020).
[2] The reports of these negotiation rounds are posted by the DFAT and the European Commission ('EC'). See DFAT, A-EUFTA News, www.dfat.gov.au/trade/agreements/negotiations/aeufta/Pages/aeufta-news (last accessed 12 December 2020); EC, Commission Reports on Latest Negotiating Round with Australia, https://trade.ec.europa.eu/doclib/press/index.cfm?id=2151 (last accessed 14 December 2020).
[3] DFAT, above n 1.
[4] These statistics refer to EU27 and the United Kingdom. See DFAT, above n 1.
[5] EC, Client and Supplier Countries of the EU27 in Merchandise Trade (value %), https://trade.ec.europa.eu/doclib/docs/2006/september/tradoc_122530.pdf (last accessed 23 January 2021).
[6] See https://www.dfat.gov.au/geo/europe/european-union/Pages/european-union-brief (last accessed 23 January 2021).
[7] See https://www.dfat.gov.au/trade/agreements/negotiations/aeufta/Pages/default (last accessed 23 January 2021).
[8] DFAT, above n 1.
[9] This term encompasses B2B, B2C and C2C transaction, thus covering all forms of commercial transactions in the supply chain. The Organisation for Economic Cooperation and Development (OECD) has also developed a similar definition of "digital trade". See OECD, The Impact of Digitalisation on Trade, http://www.oecd.org/trade/topics/digital-trade/ (last accessed 23 January 2021).
[10] The term PTAs refers to all bilateral, regional, and megaregional trade agreements outside of the WTO. See generally Burri and Polanco (2020).
[11] Monteiro and Teh (2017), pp. 5-6.
[12] Burri and Polanco (2020), pp. 193-6.

framework for personal information protection.[13] The discussion in Section 3 on the evolution of Electronic Commerce chapters in Australian and EU FTAs also reflects this trend, although Electronic Commerce Chapters in EU FTAs have generally been narrower in scope compared to Australian FTAs.

Services trade, including in digital services, is an important component of the Australia-EU trade relations.[14] Further, several opportunities remain untapped for expanding digital trade between Australia and the EU.[15] Thus, a high-quality digital trade agreement between the EU and Australia can create several positive outcomes including: (i) enhancing economic opportunities for digital businesses in both the EU and Australia; (ii) reducing business uncertainty for Australian and European businesses in the digital sector; and (iii) creating greater interconnectivity between the two markets and reducing digital trade protectionism, including blatant data localisation measures.

This paper discusses how the digital trade chapter in the Australia – EU FTA can enable secure and open digital trade, as well as provides insights on the possible areas of agreement and disagreement between the parties on possible digital trade provisions. Section 2 discusses the overlapping policy preferences on digital trade between the EU and Australia. Section 3 compares the evolution of Electronic Commerce Chapters in Australian and EU PTAs. These two sections argue that although Australia and the EU share common ideas regarding the liberalisation of digital trade and reduction of digital protectionism, the Electronic Commerce Chapters in their PTA have historically diverged, particularly due to the EU's distinct regulatory approach in data privacy and digital regulation and tendency to focus on low hanging issues related to trade facilitation, consumer trust, and customs duties on electronic transmissions. However, with the growing importance of digital trade in the global economy, the EU appears to have embraced the need to address modern digital trade issues in its PTAs such as cross-border data flows, data localisation, and dealing with variable regulatory frameworks on data protection in different countries.[16] One such example is the recently concluded *EU – UK Trade Cooperation Agreement* ("EU-UK TCA") between the EU and the United Kingdom ("UK").

Against this background, Section 4 analyses the legal and policy implications of the text proposed by the EU on "digital trade"[17] in the Australia – EU FTA and suggests possible areas of improvement.[18] Based on past PTA practices of both countries, this section argues that the EU and Australia are likely to agree on several provisions pertaining to digital trade, especially in uncontroversial areas such as electronic signatures and authentication, paperless trading, customs duties on electronic transmissions, online consumer protection, spam, and frameworks for electronic transactions.[19] Further,

---

[13] *Ibid*.

[14] See https://www.dfat.gov.au/trade/agreements/negotiations/aeufta/Pages/summary-of-negotiating-aims-and-approach (last accessed 23 January 2021).

[15] Lee-Makiyama (2018) pp. 212, 214.

[16] See, e.g., European Parliament, Towards a Digital Trade Strategy, Doc no A8-0384/2017 (29 November 2017), https://www.europarl.europa.eu/doceo/document/A-8-2017-0384_EN.pdf (last accessed 23 January 2021).

[17] Unlike most of its previous PTAs, the EU uses the title "digital trade" for the relevant chapter, instead of electronic commerce. Some scholars believe digital trade signifies a broader scope of economic activities as compared to electronic commerce. See Burri (2016).

[18] EC, Draft Proposal for Australia – EU FTA (Digital Trade Chapter), http://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157570.pdf (last accessed 23 January 2021).

[19] See Report of the 7th round of negotiations for a Free Trade Agreement between the European Union and Australia, 4 – 15 May 2020, https://trade.ec.europa.eu/doclib/docs/2020/may/tradoc_158762.pdf (last accessed 23 January 2021).

agreement is also expected with regard to some modern-day digital trade provisions such as source code disclosure requirements and, potentially, prohibitions on protectionist data localisation requirements.

However, to significantly boost digital trade between the EU and Australia, the Australia – EU FTA must also address the potential obstacles to the transfer of data between the two regions. In that regard, the differences in data protection and privacy laws of the EU and Australia and the exceptionally defensive approach of the EU on privacy remains a compelling political and legal barrier. Rather than leaving this issue untouched, the paper suggests that the EU and Australia must use the FTA negotiations as a platform to jointly explore avenues for cooperation in data regulation, including facilitating data transfers for digital trade. Further, this paper suggests that the FTA negotiations provide an opportunity for both the parties to consider new disciplines that may facilitate digital start-ups including deeper digital trade facilitation mechanisms, as well as experiment with new models of regulatory cooperation on digital trade.

2 Significance of Digital Trade in Australia and the EU

Both Australia and the EU recognise the importance of digital trade in their economic growth.[20] This section identifies the common policy goals and priorities on digital trade of Australia and the EU and, thereafter, discusses the potential for growth of digital trade between the two parties.

Australia has, time and again, emphasised its ambition to maximise the economic benefits of digital trade and become a global leader in the digital economy.[21] Further, there is a greater acknowledgement within Australia that digitalisation of micro, small and medium sized enterprises ("MSMEs") will lead to greater economic welfare and improved digital inclusion.[22] In addition to the services industry,[23] Australia has also recognised the economic importance of digital technology in several traditional sectors such as agriculture, mining, and manufacturing.[24] The Australian government considers modern and comprehensive trade agreements an important tool to ensure international opportunities for Australian businesses in the digital sector, and a vital component of Australia's foreign cyber-policy.[25] Thus, in its "Summary of Negotiating Aims and Approach" for the Australia – EU FTA, the Australian government identified the following objective with regard to the Digital Trade Chapter:[26]

> We are seeking to establish ambitious digital trade commitments that strike a balance between facilitating modern trade and ensuring appropriate protections for consumers. High-quality rules on issues such as data flows and localisation will create a more certain and secure online environment and support increased growth of e-commerce between Australia and the EU.

---

[20] See generally https://www.dfat.gov.au/trade/services-and-digital-trade/Pages/e-commerce-and-digital-trade#:~:text=Digital%20trade%20is%20an%20increasingly,as%20further%20grow%20our%20economy (last accessed 23 January 2021); European Parliament, above n 16.

[21] See generally Australian Government (2018), p.7; Australian Trade and Investment Commission (2016); Parliament of the Commonwealth of Australia (2018); DFAT (2017); Meltzer (2018).

[22] See generally Parliament of the Commonwealth of Australia (2018).

[23] Australian Government (2018), pp.6-7.

[24] Australian Government (2018), pp.7-8; Meltzer (2018), p. iii.

[25] Along with cybersecurity, cybercrime, international security and cyberspace, internet governance and cooperation, human rights, and democracy online, technology for development, and cyber-affairs, digital trade is one of the pillars of Australian International Cyber Engagement Strategy. See DFAT (2017).

[26] See https://www.dfat.gov.au/trade/agreements/negotiations/aeufta/Pages/summary-of-negotiating-aims-and-approach (last accessed 23 January 2021).

This negotiating objective reflects Australia's commitment to promoting free and open markets for digital trade including liberalising data flows and eliminating data localisation measures. At the same time, the government acknowledges the significance of the right to regulate in important policy areas of the digital economy such as digital privacy, cybersecurity, cybercrimes, and online consumer protection.[27]

Like Australia, the EU has recognised the importance of digital trade for economic growth and especially for creating opportunities for MSMEs.[28] Historically, the EU has opted to include a minimal framework on e-commerce in its PTAs.[29] However, in recent years, the EU has indicated its preference to adopt more ambitious provisions on digital trade so as to create a level-playing field for e-commerce companies and eliminate unjustified data localisation requirements and other discriminatory measures.[30] This policy approach is also reflected in the relatively ambitious proposals advanced by the EU in the Joint Statement Initiative ("JSI") on Electronic Commerce of the World Trade Organization ("WTO").[31] Similarly, as detailed in Section 4, the text proposed by the EU for the digital trade chapter in the ongoing Australia – EU FTA negotiations is much more comprehensive than its previous PTAs.

Australia and the EU appear to have several overlapping interests and motivations with respect to negotiating the digital trade chapter in their bilateral FTA, despite their distinct regulatory frameworks on privacy and data protection. The Framework Agreement signed in 2017 by Australia and the EU indicate that both parties are committed to creating "an environment conductive to greater bilateral trade and investment".[32] Although this agreement does not include specific provisions on digital trade, it contains a provision on the protection of personal data, acknowledging the OECD Privacy Framework as a "relevant international standard" and the possibility of "exchange of information and expertise" and "cooperation between regulatory counterparts" on data protection-related issues.[33]

Further, Article 42 of the Framework Agreement broadly recognises the growing importance of ICT sector in facilitating economic development, the need for greater digital interconnectivity between Australia and the EU, and building a robust regulatory environment for digital consumers, including through regulatory cooperation in areas such as security, trust, and privacy. The Framework Agreement also contains provisions on cybercrime and cybersecurity, particularly emphasising the importance of cooperation in these areas[34] and identifying that the Budapest Convention on Cybercrime is the "global standard against cybercrime".[35] Finally, more broadly, the EU and Australia both support an open, secure, and free internet for the digital economy as well as advocate for the protection of human rights in an online environment.[36]

---

[27] DFAT, 2019 Progress Report, https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_progress_report.html (last accessed 23 January 2021).
[28] See generally European Parliament, above n 16.
[29] See Section 3.1.
[30] European Commission, Trade For All (2015), p. 12, 13. See also Towards a Digital Trade Strategy.
[31] WTO, Joint Statement on Electronic Commerce, WTO Doc WT/L/1056 (25 January 2019); WTO, Joint Statement on Electronic Commerce, WTO Doc WT/MIN(17)/60 (13 December 2017).
[32] Framework Agreement, Preamble.
[33] Framework Agreement, art. 40.
[34] Framework Agreement, art.11, art. 36.
[35] Framework Agreement, art. 36(3).
[36] European Parliament, above n 16, pp. 6, 8.; DFAT, Internet Governance and Cooperation, https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-

Several opportunities exist to generate mutually advantageous business opportunities for digital trade between Australia and the EU. For instance, the growing awareness of privacy and digital trust in Australia can incentivise the development of domestic robust and privacy-compliant digital technologies, which could find a market in the EU. Likewise, Australian consumers may be interested to purchase high-quality digital technologies from the EU. Further, investors in both the regions can find new opportunities for profitable ventures in emerging technologies such as Artificial Intelligence ("AI") and Internet of Things ("IoT"). These opportunities in the digital realm are well complemented by the fact that Australia and the EU share many underlying norms and values regarding the ethical use of emerging data- driven technologies such as AI.[37] Finally, being a leader in the Asia-Pacific including in technological research and development, Australia is an attractive base for European businesses to foray into the e-commerce sector in this region.

To date, Australia's trade in ICT goods and services has grown much faster with China, Korea and Japan as compared to the EU. [38] A notable difference is that Australia has already entered into bilateral trade and investment agreements with these countries (although, further research is necessary to establish the exact causal connection between these agreements and increasing trade flows). Therefore, several incentives exist for both Australia and the EU to negotiate a high-quality digital trade chapter in the Australia – EU FTA.

3 Digital Trade Chapters in EU and Australian FTAs: A Comparative Assessment

As of early 2020, the EU had signed 18 PTAs with electronic commerce provisions.[39] On 30 December 2020, the EU signed a trade agreement with the UK, containing a comprehensive chapter on digital trade. Australia has included electronic commerce chapters in 14 out of a total of 16 PTAs that are currently in force.[40] Electronic Commerce Chapters in Australian PTAs are usually more comprehensive, deeper and contain larger number of binding provisions than EU PTAs, which have generally been short and focused on consumer-related issues.[41] This section looks at the general structure, scope, and kinds of provisions in the Electronic Commerce Chapters in Australian and EU PTAs and draws broad comparisons. **Annex 1** contains a tabular comparison of electronic commerce provisions in EU PTAs and **Annex 2** contains a tabular comparison of electronic commerce provisions in Australian PTAs.

3.1 Digital Trade Provisions in EU PTAs

Electronic commerce provisions in EU PTAs are included either as a separate chapter[42] or as a part of the trade in services chapter.[43] The inclusion of these provisions in the trade in services chapter indicates the EU's underlying position that electronic commerce falls within the realm of trade in services. In majority of its PTAs, the EU

strategy/aices/chapters/part_5_internet_governance_and_cooperation.html (last visited 23 January 2021).

[37] EPIC consortium (2019).

[38] EPIC consortium (2019), p. 5.

[39] Willemyns (2020), p. 229.

[40] See https://www.dfat.gov.au/trade/services-and-digital-trade/Pages/e-commerce-and-digital-trade (last accessed 23 January 2021).

[41] Willemyns (2020), p. 228.

[42] See, e.g., EU-Canada Comprehensive Economic and Trade Agreement ("CETA"); EU-Mexico Globalised Agreement; EU-UK TCA.

[43] See, e.g., European Union–South Korea Free Trade Agreement ("EU-KR FTA"); EU-Singapore Free Trade Agreement ("EU-SG FTA").

has included a minimal framework on electronic commerce, with similarly worded provisions on: (i) ban on customs duties on electronic transmissions; (ii) online consumer trust and protection; (iii) regulatory cooperation on issues related to digital trade; (iv) no prior authorisation requirement for online services; and (v) electronic contracts, authentication, and signatures. Some recent PTAs also contain a provision on requirements for disclosure of source code.

EU PTAs generally recognise the importance of electronic commerce for economic growth. [44] However, several variations can be found in the preambular clauses of EU PTAs. For instance, the *EU-Canada Comprehensive Economic and Trade Agreement* ("CETA"), while setting out a broad objective of promoting electronic commerce, acknowledges that countries are not obligated to allow any form of delivery by electronic means, unless it is in accordance with the obligations of the PTA.[45] The Digital Trade Chapter in the *EU-Mexico Globalised Agreement* and the EU-UK TCA both contain a preambular provision, explicitly recognising that parties have a right to regulate to achieve "legitimate public policy objectives" including for "protection of public health, social services, public education, safety, environment or public morals, social or consumer protection, privacy and data protection, or the promotion and protection of cultural diversity".[46] The EU-UK TCA also states that the parties are not prevented from "adopting or maintaining" measures for public interest reasons contained in the general and security exception and the prudential carve-out.[47] The *EU-Singapore Free Trade Agreement* ("EU-SG FTA") recognises the importance of "the free flow of information on the internet".[48] In the *EU-Japan Economic Partnership Agreement* ("EU-Japan EPA"), the parties recognise the importance of technology neutrality in electronic commerce.[49]

Some EU PTAs clearly set out the scope and applicability of the Electronic Commerce Chapter. For instance, certain services have been excluded from the scope of the electronic commerce chapter in EU's bilateral trade agreements with Japan and Mexico: gambling and betting services, broadcasting services, audiovisual services, services of notaries or equivalent professions, and legal representation services.[50] The recent EU-UK TCA leaves out audiovisual services from the scope of the digital trade chapter.[51] In addition to these sectors, the *Mexico-EU Globalised Agreement* excludes government procurement.[52]

Some EU PTAs contain a provision on "no prior authorisation", requiring that parties must endeavour to not impose "prior authorisation or any other requirement having equivalent effect on the provision of services by electronic means".[53] This provision does not apply for authorisation schemes not specifically targeted at digital services and

[44] See, e.g., CETA, art. 16.2.1; EU-Vietnam Free Trade Agreement ("EU-VN FTA"), art. 8.50.
[45] See, e.g., CETA, art. 16.2.2.
[46] Mexico – EU Globalised Agreement, art. 1.2 (Chapter on Digital trade); EU-UK TCA, art. DIGIT.3. Similar provisions are also included in the EU-Singapore FTA, *EU-Japan Economic Partnership Agreement* ("EU-Japan EPA") and EU-Vietnam FTA.
[47] EU-UK TCA, art. DIGIT.4.
[48] EU-SG FTA, art. 8.57.3.
[49] EU-Japan EPA, art. 8.70.3.
[50] See, e.g., Japan – EU EPA, art. 8.70.5; *Mexico – EU Globalised Agreement*, art. 1.4 (Chapter on Digital Trade).
[51] EU-UK TCA, art. DIGIT.2.2.
[52] *Mexico – EU Globalised Agreement*, art. 1.4(f) (Chapter on Digital Trade).
[53] See, e.g., EU-Japan EPA, art. 8.75(1); *Mexico – EU Globalised Agreement*, art. 4.1 (Chapter on Digital Trade).

does not apply to telecommunication services.[54] This language was modified in the recent EU-UK TCA, where the relevant provision is framed in binding terms stating that a party "shall not require prior authorisation of the provision of a service by electronic means solely on the ground that the service is provided online".[55] This provision does not apply to telecommunications services, broadcasting services, gambling services, legal representation services or to the services of notaries or equivalent professions.[56]

Another common provision in many EU PTAs is on open internet access that requires parties to ensure that domestic laws do not restrict choices of services available to internet users, that they are able to connect to devices of their choice and have access to information on the network management practices of internet service providers.[57]

Another area commonly addressed in several EU PTAs is the recognition of the validity of electronic contracts and prohibition on parties from denying validity of electronic signatures or authentication methods on the sole basis that they are in an electronic form.[58] In order to facilitate electronic commerce, some provisions also encourage the use of interoperable standards for electronic signatures and authentication methods.[59] Under the EU-SG FTA, the parties further agree that they will "examine the feasibility of having a mutual recognition agreement on electronic signatures in the future".[60]

EU PTAs generally contain a provision on customs duties on electronic transmissions, although the language is not always identical. For instance, CETA restricts "customs duty, fee, or charge on a delivery transmitted by electronic means" but do not restrict any internal taxes or charges on electronic deliveries, provided it is otherwise consistent with the PTA.[61] The term language "delivery transmitted by electronic means" varies from Australian PTAs, which tend to follow US PTAs, in restricting "customs duties on electronic transmissions, including content transmitted electronically".[62] However, in some PTAs such as the EU-Japan EPA, the *EU-Vietnam Free Trade Agreement* ("EU-VN FTA"), the EU-SG FTA, the EU-UK TCA and the *EU-Mexico Globalised Agreement*, the provision simply prohibits "customs duties on electronic transmissions".[63] In one of its submissions under the WTO JSI, the EU proposal suggested language similar to Australian PTAs: "members shall not impose customs duties on electronic transmissions, which include the transmitted content".[64] This trend suggests increasing convergence between the EU and other countries.

Several EU PTAs recognise the importance of data protection for ensuring consumer trust,[65] emphasising that "the development of electronic commerce must be fully

[54] See, e.g., EU-Japan EPA, art. 8.75(2); Mexico – EU Globalised Agreement, art. 4.2 (Chapter on Digital Trade).
[55] EU-UK TCA, art. DIGIT.9.1.
[56] EU-UK TCA, art. DIGIT.9.2.
[57] *Mexico – EU Globalised Agreement*, art. 10 (Chapter on Digital Trade). However, this provision is not binding as the language used is "shall endeavour to ensure".
[58] See, e.g., *Mexico – EU Globalised Agreement*, arts. 5, 6 (Chapter on Digital Trade); EU-Japan EPA, arts. 8.76, 8.77.
[59] See, e.g., *Mexico – EU Globalised Agreement*, art. 6.4 (Chapter on Digital Trade).
[60] EU-Singapore FTA, art. 8.60.1.
[61] See, e.g., CETA, art. 16.3.
[62] See, e.g., USMCA, art. 16.3.1; SADEA, art. 5.
[63] See, e.g., EU-JAPAN EPA, art. 8.72; EU-SG FTA, art. 8.78; Mexico – EU Globalised Agreement, art. 3 (Chapter on Digital Trade); EU -VN FTA, art. 8.51; EU-UK TCA, art. DIGIT.8.
[64] Joint Statement on Electronic Commerce. EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce, INF/ECOM/22, 26 April 2019, Para 2.5
[65] See, e.g., CETA art. 16.4.

compatible with international standards of data protection".[66] In fact, the EU-CARIFORUM FTA contains an entire chapter on personal data protection, setting out the common interest of the parties to protect privacy rights of individuals and maintaining effective data protective regimes consistent with international standards.[67] This chapter further sets out the baseline requirements of a data protection framework including specifying principles including purpose limitation, transparency in data collection and processing, security-by-design, and data access and rectification.[68] The chapter also sets out requirements pertaining to processing sensitive data with additional safeguards[69] and onward data transfers i.e. personal data can only be transferred to those countries with an adequate privacy framework.[70]

Other EU PTAs contain a more basic provision on personal information protection. For instance, Article 16.4 of the CETA states:

> Each Party should adopt or maintain laws, regulations or administrative measures for the protection of personal information of users engaged in electronic commerce and, when doing so, shall take into due consideration international standards of data protection of relevant international organisations of which both Parties are a member.

The EU-UK TCA contains a provision recognising the unqualified right of the parties to maintain measures for personal data protection and privacy, including pertaining to cross-border data transfers provided that these are measures of "general application".[71]

EU PTAs also usually contain a high-level provision on online consumer protection, whereby parties recognise the importance of consumer trust, agreeing to adopt a framework for online consumer protection to prohibit fraudulent and deceptive commercial practices, and acknowledging the importance of inter-state cooperation on consumer protection issues.[72] Another provision relevant to consumer trust common to many EU PTAs is the requirement for parties to adopt a regulatory framework for unsolicited commercial electronic messages or spam.[73]

Some recent EU PTAs include a provision prohibiting the "transfer of, or access to, source code of software owned by a juridical or natural person of the other Party".[74] This provision is inspired from the megaregional trade agreement, *Comprehensive and Progressive Trans-Pacific Partnership Agreement* ("CPTPP"), as discussed in the next section.[75] In order to balance commercial interests (i.e. protecting proprietary interests of companies) and public interests (e.g., protecting citizens against algorithmic discrimination), the restrictions on source code disclosure are qualified by different exceptions. For instance, the *Mexico-EU Globalised Agreement* provides a carve-out

---

[66] EU-SG FTA, art. 8.57.4; EU-Korea FTA, art. 8.57.4; EU-CARIFORUM FTA, art. 119.2. See also EU-Japan EPA, art. 8.78.3.
[67] EU CARIFORUM FTA, art. 197
[68] EU CARIFORUM FTA, art. 199(a).
[69] EU CARIFORUM FTA, art. 199(a).
[70] EU CARIFORUM FTA, art. 199(a).
[71] EU-UK TCA, art. DIGIT.7. The term 'general application' refers to 'conditions formulated in objective terms that apply horizontally to an unidentified number of economic operators and thus cover a range of situations and cases'. See EU-UK TCA, art. DIGIT.7, n.34.
[72] See, e.g., *Mexico – EU Globalised Agreement*, art. 7 (Chapter on Digital Trade); EU-Japan EPA, art. 8.78.
[73] See, e.g., *Mexico – EU Globalised Agreement*, art. 8 (Chapter on Digital Trade); EU-Japan EPA, art. 8.79.
[74] See, e.g., EU-Japan EPA, art. 8.73; *Mexico – EU Globalised Agreement*, art. 9 (Chapter on Digital Trade)
[75] CPTPP, art. 14.17.

where disclosure of source code is necessary to achieve a legitimate public policy objective (e.g. in accordance with general, security exceptions or prudential carve-outs),[76] or if required by a judicial body to remedy a violation of competition law and enforcement of intellectual property law.[77] The obligations on the disclosure of source code also do not apply "in the context of a public procurement transaction or a freely negotiated contract".[78] Further, any restrictions on the disclosure of source code does not "affect the right of a Party to take any action or not disclose any information that it considers necessary for the protection of its essential security interests relating to the procurement of arms, ammunition or war materials, or to procurement indispensable for national security or for national defence purposes".[79] In the EU-Japan EPA, the prohibition on source code disclosure does not apply to "the transfer of or granting of access to source code in commercially negotiated contracts, or the voluntary transfer of or granting of access to source code, for instance in the context of government procurement"[80] and does not affect application of competition or intellectual property law.[81] Further, this agreement explicitly recognises that parties can adopt any measure consistent with the general and security exceptions.[82]

EU PTAs often contain a high-level provision to enhance cooperation and dialogues on electronic commerce between trade partners. Under the CETA, the EU-VN FTA, the EU-CARIFORUM FTA and the EU-SG FTA, the scope of such dialogues on electronic commerce extends to the recognition of electronic signatures, liability of intermediaries for transmission or storage of information, spam, online consumer protection, and personal information protection.[83] Under *the Mexico-EU Globalised Agreement*, the parties agree on cooperating on a broad range of areas such as electronic trust and authentication methods, treatment of direct marketing communications, addressing MSME concerns in e-commerce, cybersecurity issues, and online consumer protection.[84] In addition to several of the above issues, the EU-Korea FTA also includes cooperation between the parties on paperless trading.[85] The EU-Japan EPA contains a unique provision on stakeholder engagement, requiring parties to convene dialogues with their domestic civil society in a representative manner.[86]

The EU-UK TCA is the first EU PTA to contain a binding provision on cross-border data flows. This provision prohibits parties from restricting cross-border flows by: (i) requiring the use of local computing facilities or network elements, including those that are domestically approved or certified; (ii) imposing local storage or processing requirements for data; and (iii) subjecting cross-border transfer of data to local storage requirements or use of local computing facilities or network elements.[87] However, the PTA also requires the implementation of this provision will be reviewed within three years of the agreement coming into force. The EU-Japan EPA and the Mexico-EU Globalised Agreement contain a review clause on cross-border data flows that allow the

[76] *Mexico – EU Globalised Agreement*, art. 9.2 (a) (Chapter on Digital Trade).
[77] *Mexico – EU Globalised Agreement*, art. 9.3 (Chapter on Digital Trade).
[78] *Mexico – EU Globalised Agreement*, art. 9.2 (b) (Chapter on Digital Trade).
[79] *Mexico – EU Globalised Agreement*, art. 9.2 (c) (Chapter on Digital Trade).
[80] EU-Japan EPA, art. 8.73.1.
[81] EU-Japan EPA, art. 8.73.2.
[82] EU-Japan EPA, art. 8.73.3.
[83] CETA, art. 16.6; EU-CARIFORUM FTA, art. 120; EU-Singapore FTA, art. 8.61 EU -VN FTA, art. 8.52.
[84] *Mexico – EU Globalised Agreement*, art .11 (Chapter on Digital Trade).
[85] EU-KOREA FTA, art. 7.49(e).
[86] EU-Japan EPA, art. 16.16.
[87] EU-UK TCA, art. DIGIT.6.

parties to assess the need for inclusion of provisions on the free flow of data into this Agreement after three years after the PTA enters into force.[88]

A unique requirement in EU PTAs is a provision setting out the scope of computer and related services. Computer and related services are defined quite broadly in several EU PTAs to include services providing:[89]

> …(a) consulting, strategy, analysis, planning, specification, design, development, installation, implementation, integration, testing, debugging, updating, support, technical assistance or management of or for computers or computer systems;
>
> (b) computer programs plus consulting, strategy, analysis, planning, specification, design, development, installation, implementation, integration, testing, debugging, updating, adaptation, maintenance, support, technical assistance, management or use of or for computer programs;
>
> (c) data processing, data storage, data hosting or database services;
>
> (d) maintenance and repair services for office machinery and equipment, including computers; or
>
> (e) training services for staff of clients, related to computer programs, computers or computer systems, and not elsewhere classified.

Further, these PTAs recognise the "important distinction between the enabling service such as web-hosting or application hosting and the content or core service that is being delivered electronically such as banking, and that in such cases the content or core service is not covered by CPC 84".[90]

With regard to inscribing committees in various service sectors in their schedules, the EU has generally preferred positive listing in its PTAs, whereby the EU explicitly lists the various sectors in which it undertakes commitments on market access and national treatment.[91] This approach has served the EU well in protecting emerging service sectors from unplanned liberalisation.[92] However, while negotiating CETA with Canada, the EU agreed to provide a more liberalising approach of providing negative list for services,[93] whereby the parties only list those sectors/sub-sectors where they wish to make reservations for market access and national treatment obligations. The negative list consisted of Annex I (reservations with regard to existing measures) and Annex II (reserving possible future measures). The EU also considered a hybrid approach for inscribing commitments in service sectors in the stalled Trade in Services Agreement, consisting of a positive list for market access and negative list for national treatment.[94]

3.2 Digital Trade Provisions in Australian PTAs

The extent and depth of provisions in most Australian FTAs is much more comprehensive and liberalising than Electronic Commerce Chapters in EU FTAs. Many of Australia's recent PTAs closely follows the language contained in the megaregional

---

[88] EU-Japan EPA, art. 8.81; *Mexico – EU Globalised Agreement*, art. XX (Chapter on Digital Trade).
[89] See, e.g., EU-KR FTA, art. 7.25.3; EU-SG FTA, art. 8.21.3; EU-VN FTA art. 8.22.3; EU-UK TCA, art. DIGIT.7; EU-CARIFORUM FTA, art. 188.
[90] EU-KR FTA, art. 7.25.4; EU-SG FTA, art. 8.21.4; EU-VN FTA art. 8.22.4.
[91] See generally EC, Services and investment in EU trade deals Using "positive" and "negative" lists, April 2017, http://trade.ec.europa.eu/doclib/docs/2016/april/tradoc_154427.pdf (last accessed 23 January 2021).
[92] Elms (2017), p. 47.
[93] Elijah (2017), p. 60.
[94] EC, above n 91.

CPTPP. Significant deviations are observed in certain agreements such as the *China – Australia FTA* ("ChAFTA"), where the Electronic Commerce Chapter does not contain provisions on data localisation or cross-border data flows and is also not subject to dispute settlement. Further, certain PTAs pre-dating the CPTPP are not as comprehensive as the recent Australian PTAs such as those with Peru (*Peru – Australia Free Trade Agreement* or "PAFTA"), Hong Kong (*Hong Kong – Australia Free Trade Agreement* or "HK-AFTA"), Singapore (*Singapore – Australia Digital Economy Agreement* or "SADEA"), and Indonesia (*Indonesia – Australia Economic Partnership Agreement* or "IAEPA").

Preambular provisions in Australian PTAs usually recognise the economic opportunities provided by electronic commerce and the importance of consumer confidence in electronic commerce,[95] but do not typically recognise the right to regulate in the digital context which is common to many EU PTAs. The scope of application of Electronic Commerce Chapter in Australian PTAs applies to measures adopted or maintained by a party that affect trade by electronic means.[96] This language is usually not included in most EU PTAs. Some Australian PTAs exclude government procurement and government data (including data collected and processed on behalf of the government) from scope of the Electronic Commerce Chapter.[97] Further, financial service providers are typically excluded from the Electronic Commerce Chapter in Australia's PTAs.[98]

Unlike any of EU PTAs, some Australian PTAs contain a provision on non-discrimination of digital products prohibiting a party from providing less favourable treatment to digital products of the other party, subject to the non-conforming measures agreed to between the parties and consistent with the provisions on intellectual property.[99] Under the *Japan – Australia Economic Partnership Agreement* ("JAEPA"), this obligation also does not apply in the case of government procurement, state subsidies and services supplied by the government. [100] Under the PAFTA, SADEA and CPTPP, this obligation also does not apply to broadcasting services.[101]

Like the EU PTAs, most Australian PTAs contain provisions on electronic signatures and electronic authentication, requiring parties to recognise the validity of electronic signatures and ensuring secure methods for electronic authentication, including encouraging the use of interoperable standards.[102] Some Australian PTAs also encourage parties to "work toward the mutual recognition of electronic signatures issued or recognised by either Party".[103]

Many Australian PTAs also provide that parties must adopt a domestic framework for electronic transactions consistent with international standards such as UNCITRAL

[95] See, e.g., HK-AFTA, art. 11.1.1; IAEPA, art. 13.2.1; PAFTA, art. 13.2.1; CPTPP, art. 14.2.1; ChAFTA, art. 12.1 (only recognising the economic growth and opportunities provided by e-commerce and the importance of avoiding barriers to e-commerce); JAEPA, art. 13.1 (also recognises the principle of technology neutrality in e-commerce, similar to the Japan-EU EPA).
[96] See, e.g., CPTPP, art. 14.2.2; HK-AFTA, art. 11.1.2; IAEPA, art.13.2.2; PAFTA, art. 13.2.2; SADEA, art. 2.1.
[97] See, e.g., CPTPP, art. 14.2.3; HK-AFTA, art.11.1.3; IAEPA, art. 13.2.3, art 13.2.4; PAFTA, art. 13.2.3; KAFTA, art. 15.1; SADEA, art. 2.2.
[98] See, e.g., HK-AFTA, art. 11.2 (Definition of covered persons); CPTPP, art. 14.1 (Definition of covered persons).
[99] See, e.g., JAEPA, art.13.4; PAFTA, art. 13.4; CPTPP, art. 14.4; SADEA, art. 6.
[100] See, e.g., JAEPA, art. 13.4.
[101] PAFTA, art. 13.4.4; CPTPP, art. 14.4.4; SADEA, art. 6.4
[102] See, e.g., HK-AFTA, art.11.3; IAEPA, art. 13.5; See also ChAFTA, art.12.6; JAEPA, art.13.6; PAFTA, art. 13.6; CPTPP, art. 14.6; SADEA, art. 9.
[103] JAEPA, art. 13.6.4.

Model Law on Electronic Commerce 1996 or the United Nations Convention on the Use of Electronic Communications in International Contracts.[104] The ChAFTA only references the UNCITRAL Model Law and adds other relevant international standards may be taken into account in devising domestic legal frameworks on electronic transactions.[105] The recently signed SADEA recognises international principles for transfer of electronic records such as the UNCITRAL Model Law on Electronic Transferable Records.[106] Further, certain Australian PTAs require that parties must endeavour to avoid "any unnecessary regulatory burdens on electronic transactions" and "facilitate input by interested persons in the development of its legal framework for electronic transactions".[107] Similar provisions are not found in EU PTAs.

EU PTAs do not typically contain a provision on paperless trading. In contrast, most Australian PTAs contain at least a hortatory provision on paperless trading requiring parties to endeavour to: (i) provide trade administration documents in electronic forum; (ii) accept electronic submission of trade administration of documents, to the extent legally and practically feasible.[108] Under the ChAFTA, the provision on accepting electronic version of trade administration documents is legally binding on the parties.[109] Under the recent SADEA, Australia has agreed to more onerous provisions on paperless trading such as making electronic versions of all trade administration documents available and accepting electronic submissions of trade administration documents.[110]

Australian PTAs generally prohibit imposition of customs duties on electronic transmissions, although the language somewhat varies across PTAs. Some PTAs prohibit customs duties on "electronic transmissions, including content transmitted electronically" but do not prohibit parties from imposing internal taxes, fees or charges on content transmitted electronically.[111] Other PTAs simply state that parties will not impose customs duties on electronic transmissions.[112] Under the ChAFTA, Australia and China agree to not maintain its practice of imposing customs duties on electronic transmissions consistent with the WTO moratorium under the Work Programme on Electronic Commerce.[113] This means that if WTO parties do not renew the moratorium, then China will not be bound by the provision anymore.[114] The language on customs duties on electronic transmissions in Australian PTAs diverges from EU PTAs, although, as explained earlier in Section 3.1, some convergence can now be observed.

Similar to EU PTAs, Australian PTAs contain high-level provisions on online consumer protection and spam. The most common provision on online consumer protection requires parties to adopt legal framework to protect consumers from "fraudulent and deceptive commercial practices" in electronic commerce and recognises the importance

[104] See, e.g., HK-AFTA, art. 11.4.1; IAEPA, art. 13.9.1; PAFTA, art. 13.5.1; CPTPP, art. 14.5.1; KAFTA, art. 15.4.1; SADEA, art. 8.2.
[105] ChAFTA, art. 12.5.1.
[106] SADEA, art. 8.4.
[107] See, e.g., HK-AFTA, art.11.4.2; IAEPA, art. 13.9.2; PAFTA, art. 13.5.2; CPTPP, art .14.5.2. See also ChAFTA, art. 12.5.2 (language is slightly different).
[108] See, e.g., HK-AFTA, art. 11.10; IAEPA, art.13.4; JAEPA, art. 13.9; PAFTA, art. 13.9.
[109] ChAFTA, art. 12.9.1.
[110] SADEA, art. 12.1, art. 12.2. In addition, it has agreed on other provisions including single electronic window and developing data exchange systems for trade administration documents.
[111] See, e.g., CPTPP, art. 14.3; HK-AFTA, art. 11.6; PAFTA, art. 13.3; SADEA, art. 5.
[112] See, e.g., JAEPA, art. 13.3; KAFTA, art. 15.3.
[113] ChAFTA, art. 12.3.1.
[114] ChAFTA, art. 12.3.2.

of cooperation on online consumer protection.[115] However, some other provisions on online consumer protection are weaker in nature, where the PTA parties only recognise the importance of online consumer protection for electronic commerce (i.e. providing "protection that is at least equivalent to that provided for consumers using other forms of commerce"), without any binding obligations.[116] Similarly, for spam, the relevant provision in Australian PTAs requires parties to adopt or maintain measures for regulating spam such as facilitating the ability of recipients to prevent reception of spam and providing consent mechanisms for spam.[117]

Australian PTAs recognise the importance of personal information protection for electronic commerce but diverge from EU PTAs in significant ways: (i) they are usually not as detailed and comprehensive (see e.g., EU-CARIFORUM FTA, discussed in the previous section); and (ii) they do not provide an unqualified right for parties to adopt data protection laws i.e., such provisions must be inconsistent with trade obligations contained in the agreement, including for cross-border data transfers. Following the CPTPP,[118] several of Australia's other recent PTAs contain a provision requiring all parties to "adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce".[119] The provision does not prescribe any standards or benchmarks for the legal framework but imposes a general requirement that parties "take into account principles or guidelines of relevant international bodies".[120] The CPTPP provides a further clarification in a footnote as to what constitutes framework for personal information protection:

> For greater certainty, a Party may comply with the obligation in this paragraph by adopting or maintaining measures such as a comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy.[121]

This provision paves the path for parties to adopt their own version of a privacy law without having to comply with any specific international standards. However, this footnote has been omitted in most Australian PTAs including the HK-AFTA, PAFTA and IAEPA. This footnote was however retained in the recent SADEA.[122] Following a similar provision in the *United States – Mexico – Canada Agreement* ("USMCA"),[123] the SADEA added APEC Cross-Border Privacy Rules System ("CBPR") and the OECD Privacy Guidelines as examples of relevant international guidelines on data protection.[124]

---

[115] See, e.g., HK-AFTA, art.11.5; IAEPA, art. 13.6; PAFTA, art. 13.7; CPTPP, art .14.7. See also SADEA, art. 15.
[116] See, e.g., JAEPA, art. 13.7; ChAFTA, art. 12.7.
[117] See, e.g., HK-AFTA, art.11.11; IAEPA, art. 13.8; PAFTA, art. 13.13; CPTPP, art. 14.14; KAFTA, art. 15.9; SADEA, art. 19.
[118] CPTPP, art.14.8.2.
[119] See, e.g., HK-AFTA, art.11.9.2; IAEPA, art. 13.7.2; PAFTA, art. 13.8.1. See also JAEPA, art. 13.8; KAFTA, art. 15.8. The language in ChAFTA, art. 12.8.2 is slightly different ("In the development of data protection standards, each Party shall, to the extent possible, take into account international standards and the criteria of relevant international organisations".)
[120] See, e.g., HK-AFTA, art. 11.9.2; IAEPA, art. 13.7.2; PAFTA, art. 13.8.2.
[121] CPTPP, art. 14.8.2, n 6.
[122] SADEA, art. 17.2, n.11.
[123] USMCA, art. 19.8.2.
[124] SADEA, art. 17.2.

The provision on personal information protection in many Australian PTAs also encourages the development of mutual recognition mechanisms between parties[125] and adoption of non-discriminatory practices in protecting e-commerce users from privacy violations.[126] Parties are also legally bound to publish information regarding their personal information protection laws such as how individuals can pursue remedies and compliance requirements for businesses handling personal data.[127] In the recent SADEA, Australia and Singapore recognised that the APEC CBPR was a "valid mechanism to facilitate cross-border information transfers while protecting personal information".[128]

Unlike the EU, Australia has consistently adopted an open position on cross-border data flows and data localisation. The language used in most Australian PTAs is similar to the CPTPP provisions,[129] where parties are required to allow cross-border transfer of information for electronic commerce, including personal information.[130] Similarly, as regards data localisation, the relevant provision prevents parties from requiring covered businesses[131] to use local computing facilities as a condition for conducting business within the country.[132] However, parties can only adopt or maintain measures which restrict cross-border data transfers or require local data localisation to achieve a "legitimate public policy objective". Further, such measures must not be "applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination, or a disguised restriction on trade".[133] In the IAEPA, in addition to the above, parties have agreed that they are not prohibited from adopting or maintaining any measures "necessary for the protection of its essential security interests".[134]

Unlike most other Australian PTAs where data transfers for financial services is covered in the Financial Services Chapter, the HK-AFTA and the SADEA contain provisions for cross-border data transfers and data localisation for financial services in the Electronic Commerce Chapter. The relevant provision in these two agreements imposes a general prohibition on restricting cross-border data transfer necessary for financial services or requiring financial service providers to use local computing facilities.[135] However, the prohibition on data localisation is subject to the requirement that financial regulators must have "immediate, direct, complete and ongoing access to information processed or stored on computing facilities that the covered financial person uses or locates outside the Area of the Party".[136] Further, if a financial service provider is unable to provide data access to financial regulators, it must be given a "reasonable opportunity to remediate a lack of access to information", "to the extent practicable", before governments impose data localisation requirements.[137] Finally, parties can adopt or maintain any measures pertaining to financial services to achieve a "legitimate public policy objective", provided that it is not "applied in a manner which would constitute a

[125] See, e.g., HK-AFTA, art. 11.9.5; IAEPA, art. 13.7.4; PAFTA, art. 13.8.5; CPTPP, art. 14.8.5.
[126] See, e.g., HK-AFTA, art. 11.9.3; IAEPA, art. 13.7.3; PAFTA, art. 13.8.4; CPTPP, art. 14.8.4.
[127] See, e.g., HK-AFTA, art. 11.9.4; IAEPA, art. 13.10.2.
[128] SADEA, art. 17.8.
[129] CPTPP art 14.11, art. 14.13.
[130] See, e.g., HK-AFTA, art. 11.7.2; IAEPA, art. 13.11.2; PAFTA, art. 13.11.2; SADEA, art. 23.
[131] The definition of covered persons in these PTAs excludes financial service providers.
[132] See, e.g., HK-AFTA, art. 11.8.2; IAEPA, art. 13.12.2; PAFTA, art. 13.12.2.
[133] See, e.g., HK-AFTA, art. 11.7.3, art. 11.8.3; IAEPA, art. 13.11.3(a), art. 13.12.3(a); PAFTA, art.13.11.3, art. 13.12.3.
[134] See, e.g., IAEPA, art. 13.11.3(b), art.13.12.3(b).
[135] HK-AFTA, art.11.15.1; art. 11.15.2; SADEA, art. 25.2.
[136] HK-AFTA, art. 11.15.2.
[137] HK-AFTA, art. 11.15.3. See also HK-AFTA, art. 11.15.4; SADEA, art. 25.3.

means of arbitrary or unjustifiable discrimination" or is "a disguised restriction on trade".[138]

Similar to some recent EU PTAs as discussed above in Section 3.1, recent Australian PTAs also contain prohibitions on the forced disclosure of source code that broadly follow the language of the provision of the CPTPP.[139] The relevant provision prohibits parties from requiring that companies transfer or provide access to source code of software to regulators "as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory".[140] This provision applies to "mass-market software or products containing such software" but excludes "software used for critical infrastructure".[141] This provision is not applicable to "commercially negotiated contracts" which require for the "provision of source code",[142] or in circumstances, where a party may "requir[e] the modification of source code of software necessary for that software to comply with laws or regulations which are not inconsistent with this Agreement".[143] Further, some PTAs specify that the prohibition on disclosure of source code does not prevent companies from licensing their software on a "free and open source basis".[144] The prohibition on involuntary disclosure of source code does not apply to provision of source code for "patent applications", "granted patents", including "in relation to patent disputes", provided that there are "safeguards against unauthorised disclosure under the law or practice of a Party".[145] Additionally, the IAEPA does not prohibit the parties from adopting or maintaining any source code disclosure requirements if "it considers" the measure "necessary for the protection of its essential security interests".[146]

Following the CPTPP,[147] recent Australian PTAs such as the PAFTA and SADEA contain a high-level provision recognising the benefits for consumers of open access to the internet and digital services (subject to "reasonable network management" by the internet service provider) as well as the importance of consumers being able to use devices of their choices to connect to the internet and access information regarding the network management practice of their internet service supplier.[148]

Like the EU PTAs, most Australian PTAs contain a high-level provision encouraging cooperation between the parties on various issues pertaining to e-commerce including sharing of information, best practices and experiences in those relevant area including personal information protection, online consumer protection, spam, security, electronic authentication, international cooperation initiatives, and self-regulatory models in electronic commerce, and capacity building for computer security incident response.[149]

In addition to conventional digital trade issues, the SADEA, modelled on the lines of the *Digital Economy Partnership Agreement* ("DEPA") between Singapore, Chile, and

[138] HK-AFTA, art.11.15.5.
[139] See CPTPP art. 14.17.
[140] See, e.g., HK-AFTA, art. 11.12.1; IAEPA, art. 13.13.1; PAFTA, art. 13.16.1.
[141] See, e.g., HK-AFTA, art.11.12.2; IAEPA, art. 13.13.2; PAFTA, art. 13.16.2.
[142] See, e.g., HK-AFTA, art. 11.12.3(a); IAEPA, art. 13.13.3(a); PAFTA, art. 13.16.3(a)
[143] See, e.g., HK-AFTA, art. 11.12.3(b); IAEPA, art. 13.13.3(b); PAFTA, art. 13.16.3(b).
[144] See, e.g., HK-AFTA, art .11.12.3(c); SADEA, art. 28.3.
[145] See, e.g., HK-AFTA, art. 11.12.4; IAEPA, art. 13.13.4; PAFTA, art. 13.16.4.
[146] IAEPA, art.13.13.5.
[147] CPTPP, art. 14.10.
[148] PAFTA, art. 13.10; SADEA, art. 20.
[149] See, e.g, HK-AFTA, art. 11.13; IAEPA, art. 13.3; CPTPP, art. 14.15 and art. 14.16; ChAFTA, art. 12.10. See also JAEPA, art. 13.10; PAFTA, art.13.14, art. 13.15 (cooperation on cybersecurity). See further SADEA, art. 16 (cooperation on competition policy), art. 33, art. 32(fintech and regtech cooperation)

New Zealand, covers several new areas which have conventionally been left out of Electronic Commerce Chapter in PTAs. Some of these new areas include electronic invoicing,[150] electronic payments,[151] express shipments,[152] online safety,[153] data innovation,[154] open government data,[155] and artificial intelligence.[156]

4 Digital Trade in Australia-EU FTA: Possibilities and Challenges

At the outset of the negotiations, the EU released a draft text proposal for the Digital Trade Chapter[157] in the Australia – EU FTA.[158] The draft proposal is far more comprehensive than most of EU PTAs, discussed in Section 3.1 above. This section analyses this draft EU proposal, taking into account the past PTA practices of Australia and the EU, including the reports from the ongoing negotiations, as well as the significance of digital trade provisions in strengthening the economic relationship between Australia and the EU. It then suggests certain areas for improvement and dialogues to adopt a future-forward approach in negotiating the digital trade chapter in the Australia – EU FTA.

4.1 EU's Proposed Digital Chapter in the Australia – EU FTA

4.1.1 Scope and Applicability of the Digital Trade Chapter

The proposed chapter applies to any measure "affecting trade enabled by electronic means" and only excludes audiovisual services.[159] Trade enabled by electronic means would refer to any economic activity enabled by the internet, irrespective of whether it involves physical or virtual products and services; it would also include intermediate forms of digital trade, such as B2B transactions, instead of only B2C transactions, which has traditionally been associated with e-commerce. Most Electronic Commerce Chapters in Australian PTAs apply to trade "affected" by rather than "enabled" by electronic means; while the term "affected" theoretically appears to have a broader application, both the terms in practice are likely to have a very similar scope of application. The exclusion of "audiovisual services" from the ambit of digital trade chapter is unlikely to be highly contentious between Australia and the EU, given Australian sensitivity towards audiovisual services.[160] The EU proposal interestingly

[150] SADEA, art. 10.
[151] SADEA, art. 11.
[152] SADEA, art. 13
[153] SADEA, art. 18.
[154] SADEA, art. 26.
[155] SADEA, art. 27.
[156] SADEA, art. 31.
[157] The proposal suggests the chapter title as 'Digital Trade' and not electronic commerce. Some experts believe that the use of 'digital trade' as a chapter title acknowledges the broader scope and applicability of these provisions to economic transactions in the digital economy. See Anupam Chander, The Coming North American Digital Trade Zone, 9 October 2018, https://www.cfr.org/blog/coming-north-american-digital-trade-zone (arguing the same in the context of the USMCA, which is the first PTA to adopt this chapter title).
[158] Identical text proposed for ongoing negotiations between New Zealand and the EU. See https://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157581.pdf (last accessed 23 January 2021).
[159] EU proposal, Digital Trade Chapter, Australia – EU FTA, art. 1. This exclusion is because the European Commission does not have the capacity to negotiate on audiovisual services but individual members. See Lee-Makiyama (2018), p. 219.
[160] For e.g., in CPTPP, Australia included a NCM for the audiovisual sector with respect to its applicable obligations on national treatment, MFN, market access, performance requirements and local presence contained in the investment and trade in services chapter. CPTPP, Annex of Australia, https://www.mfat.govt.nz/assets/Trade-agreements/TPP/Annexes-ENGLISH/Annex-II.-Australia.pdf,

does not contain any exclusions for government procurement or financial services, which is common to many PTAs, especially to which Australia has been a party.

4.1.2 Right to Regulate and Applicable Exceptions

The proposed text sets out an independent provision on the right to regulate, encompassing a broad number of "legitimate public policy objectives":[161]

> The Parties reaffirm the right to regulate within their territories to achieve legitimate policy objectives, such as the protection of public health, social services, public education, safety, the environment including climate change, public morals, social or consumer protection, privacy and data protection, or the promotion and protection of cultural diversity.

This provision will presumably inform how the exceptions may be read in the agreement, which is currently in a draft form in the proposed text, indicating that the EU desires to include the general exceptions, the security exception and the prudential carve-out (in the context of financial services) (which may later be moved to a separate chapter applicable to the entire FTA).[162] Read together, these two provisions highlight the importance accorded by the EU to protecting the right to regulate the digital sector. Further, in the Electronic Commerce Chapters of other recent EU FTAs, some elements of the general exceptions have been slightly modified, for instance, the sub-clause allowing measures "necessary to protect public security or public morals or to maintain public order".[163] Given that both Australia and the EU accord high importance to regulating the digital sector and share common values on internet and digital services regulation, such a provision is unlikely to be pose difficulties during negotiation, although Australian negotiators may aim to align this wording with their existing PTAs.

4.1.3 Data Flows and Privacy

The next section of the proposed EU text deals with data flows and personal data protection. As is already evident from the reports of the first eight round of negotiations between the EU and Australia, these provisions will be the most complicated to negotiate. Article 5(1) of the proposed text sets out a strict prohibition on unjustified data localisation measures, reflecting EU's digital trade policy and identical to the language contained in the EU-UK TCA (discussed above in Section 3.1):

> The Parties are committed to ensuring cross-border data flows to facilitate trade in the digital economy. To that end, cross-border data flows shall not be restricted between the Parties by:
>
> (a) requiring the use of computing facilities or network elements in the Party's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of the Party;
>
> (b) requiring the localisation of data in the Party's territory for storage or processing;
>
> (c) prohibiting storage or processing in the territory of the other Party;
>
> (d) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Party's territory or upon localisation requirements in the Party's territory

p.9. Similarly, in the GATS, Australia included audio-visual services in its MFN list and also not undertaken any commitments in the GATS Schedule.

[161] EU proposal, Digital Trade Chapter, Australia – EU FTA, art. 2.

[162] EU proposal, Digital Trade Chapter, Australia – EU FTA, art. 3.

[163] See, e.g., EU-VN FTA, art. 8.53(a).

This provision is a horizontal clause applicable to all sectors and covering both personal and non-personal data. Further, the scope of this provision appears broad as it prohibits different forms of data localisation such as forced local storage and processing requirements (arguably, including data mirroring requirements), forced use of local servers and other computing facilities including local technologies and overseas data storage and processing, and prohibits imposing conditions on cross-border data flows to use local "computing facilities" or "network elements" (arguably, including different forms of local content or performance requirements). The terms computing facilities and network elements are undefined but appear to be broad. A useful reference is the definition of computing facilities in the CPTPP: "computer servers and storage devices for processing or storing information for commercial use".[164] Similarly, network elements can refer to any networking infrastructure related to the internet. Similar to the EU-UK TCA, the EU proposes to review and assess the functioning of this provision three years after the agreement comes into force.[165] This caution is not surprising given that this is one of the early attempts by the EU to adopt a binding prohibition on data localisation.[166]

Predictably, the proposed EU text provides a broad provision on privacy, acknowledging that right to privacy is a "fundamental right" and is a precondition to facilitate digital "trust". Further, the proposed provision provides an unlimited scope for each party to adopt a privacy framework as they deem fit, including safeguards for cross-border data transfers, irrespective of the obligations contained in the FTA:

> 1. Each Party recognises that the protection of personal data and privacy is a fundamental right and that high standards in this regard contribute to trust in the digital economy and to the development of trade.
>
> 2. Each Party may adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data. Nothing in this agreement shall affect the protection of personal data and privacy afforded by the Parties' respective safeguards.
>
> 3. Each Party shall inform the other Party about any safeguard it adopts or maintains according to paragraph 2.
>
> 4. For the purposes of this agreement, 'personal data' means any information relating to an identified or identifiable natural person.

The EU and Australia have adopted a different approach in data protection in their respective PTAs.[167] The EU has consistently refused to include any provisions that could subject its privacy laws to trade obligations.[168] This approach is also reflected in the above provision proposed by the EU, intended to provide a blanket exemption for existing regulatory barriers for cross-border data flows under the GDPR. In contrast, Australia has generally taken a more liberal approach with respect to provisions on data protection in their PTAs. As discussed in Section 3.2, majority of Australian PTAs include a provision requiring parties to adopt a basic framework for protection of

[164] CPTPP, art. 14.1.
[165] EU proposal, Digital Trade Chapter, Australia – EU FTA, art. 5.2
[166] See Section 3.1 above.
[167] See Sections 3.1 and 3.2 above.
[168] See e.g., European Parliament, above n 16, p. 8 (See also Para 7: "Recalls that nothing in trade agreements shall prevent the EU and its Member States from maintaining, improving and applying its data protection rules").

personal information. However, Australian PTAs do not include a carve out for domestic privacy law, implying that any measures in domestic privacy laws must be consistent with the obligations contained in the PTA or otherwise be justifiable under the exceptions available under the PTA.

This provision will probably be the most difficult area for negotiation. The provision proposed by the EU does not alleviate the concerns of Australian businesses that use or monitor personal data of EU residents and depend on data transfers out of the EU. Therefore, the Australian negotiators are likely to push back against the adoption of the provision in the current form.

4.1.4 No-Prior Authorisation

Similar to the language adopted the EU-UK TCA (discussed in Section 3.1), the proposed text for the Australia – EU FTA also includes a provision on "no prior authorisation":

> 1. A Party shall not require prior authorisation solely on the ground that a service is provided online, or adopt or maintain any other requirement having an equivalent effect.
>
> 2. Paragraph 1 does not apply to telecommunications services, broadcasting services, gambling services, or legal representation services, nor to services of notaries or equivalent professions to the extent that they involve a direct and specific connection with the exercise of public authority.[169]

This provision effectively means that a party cannot subject online service providers to authorisation or equivalent requirements solely on the grounds that they offer online services. The aim of the provision appears to be discouragement of authorisation or equivalent procedures aimed specifically at online services.[170] However, as Streinz argues, the dichotomy between online and offline services is diluted in the current digital world and, hence, the relevance of this provision appears less clear today.[171]

4.1.5 Other Digital Trade Provisions

The remainder of the proposed Digital Trade Chapter includes provisions typical to many modern digital trade/electronic commerce chapters in PTAs: (i) prohibition on customs duties on electronic transmissions; (ii) electronic contracts, signatures, and authentication; (iii) prohibition on forced disclosure of source code; (iv) requirement to adopt a framework on online consumer protection; (v) protection against spam; (vi) regulatory cooperation on digital trade.

The EU proposes banning any customs duties on electronic transmissions.[172] Electronic transmissions relates to the "supply of services",[173] reflecting EU's approach of treating all trade in digitally encoded products as trade in services; therefore, this provision does not apply to customs duties applied on goods delivered via electronic commerce. The EU and the US have been involved in a long-standing divide at the WTO, whether digital products constitute goods or services or both.[174] It remains unclear from the wording of the proposed provision if electronic transmissions refer only to transmissions or also to

[169] EU proposal, Digital Trade Chapter, Australia – EU FTA, art. 8.
[170] No prior authorisation requirements was also a part of the E-commerce Directive in the EU.
[171] Thomas Streinz, Tweet (20 January 2021) https://twitter.com/t_streinz/status/1351848132729065473 (last accessed 23 Janaury 2021).
[172] EU proposal, Digital Trade Chapter, Australia – EU FTA, art. 7(2).
[173] EU proposal, Digital Trade Chapter, Australia – EU FTA, art. 7(1).
[174] This topic has also been subject to extensive debate in the WTO, where the EU and the US have taken opposite sides. For more discussion, see Willemyns (2020), p. 233.

the content transmitted,[175] although the EU has taken a liberal approach on this issue in recent PTAs, as previously discussed in Section 3.1.

The proposed text includes a headnote for reservations, listing the services included under "computer and related services",[176] which would also inform the interpretation of the scope of EU's commitments under the Australia – EU FTA. The EU has proposed the adoption of the same schema for listing non-conforming measures as the CETA, consisting of Annex I and Annex II, [177] as discussed previously in Section 3.1.

Following the trend in several recent PTAs,[178] the EU has also proposed a provision prohibiting the forced disclosure of source code: [179]

> 1. A Party shall not require the transfer of, or access to, the source code of software owned by a natural or juridical person of the other Party.
>
> 2. For greater certainty:
>
> (a) the general exception, security exception and prudential carve-out can apply to measures of a Party adopted or maintained in the context of a certification procedure; (b) paragraph 1 does not apply to the voluntary transfer of or granting of access to source code on a commercial basis by a natural or juridical person of the other Party, for instance in the context of a public procurement transaction or a freely negotiated contract.
>
> 3. Nothing in this Article shall affect: (a) requirements by a court, administrative tribunal or competition authority to remedy a violation of competition law; (b) intellectual property rights and their protection and enforcement; and (c) the right of a Party to take measures in accordance with Article [security and general exceptions of the Public Procurement Title].

The proposed text does not contain a definition of source code, but source code ordinarily refers to the instructions written by the computer in programming language. Notably, this provision does not include algorithms (for instance, unlike the USMCA). As discussed in Section 3.2, several Australian PTAs include a provision on source code disclosure and the EU has recently also agreed upon similar provisions in its PTAs.

The EU has proposed various provisions to facilitate electronic commerce such as removing obstacles for parties to conclude a contract by electronic means;[180]

---

[175] However, note EU's proposal to JSI discussed above.

[176] This headnote reads:

> 1. Any of the following services shall be considered as computer and related services, regardless of whether they are delivered via a network, including the Internet: (a) consulting, adaptation, strategy, analysis, planning, specification, design, development, installation, implementation, integration, testing, debugging, updating, support, technical assistance or management of or for computers or computer systems; (b) computer programmes defined as the sets of instructions required to make computers work and communicate (in and of themselves), as well as consulting, strategy, analysis, planning, specification, design, development, installation, implementation, integration, testing, debugging, updating, adaptation, maintenance, support, technical assistance, management or use of or for computer programmes; (c) data processing, data storage, data hosting or database services; (d) maintenance and repair services for office machinery and equipment, including computers; and (e) training services for staff of clients, related to computer programmes, computers or computer systems, and not elsewhere classified.
>
> 2. For greater certainty, services enabled by computer and related services, other than those listed in paragraph 1, shall not be regarded as computer and related services in themselves.

[177] EU proposal, Investment Liberalisation and Trade in Services, Australia – EU FTA, art. 2.7.1.

[178] For a general discussion, see Mishra (2021), pp. 41-46.

[179] EU proposal, Digital Trade Chapter, Australia – EU FTA, art. 11.

[180] EU proposal, Digital Trade Chapter, Australia – EU FTA, art. 9(1).

recognising electronic authentication methods and ensuring that their underlying performance standards are "objective, transparent and non-discriminatory";[181] and ensuring that parties provide effective protection to consumers against spam.[182] In the draft text, the EU has also included a provision on online consumer trust, requiring parties to adopt measures to prohibit fraudulent and deceptive commercial practices, promote fair commercial practices, reduce information asymmetry between consumers and e-commerce businesses, and provide adequate rights and remedies to aggrieved consumers.[183] As discussed in Section 3, these kinds of provisions are common to both EU and Australian PTAs, although the exact wording varies across the PTAs. These issues appear to be low hanging fruit and likely to be agreed upon by both sides during the Australia – EU FTA negotiations, as also indicated by available reports.[184]

Like many of its previous FTAs, the EU has proposed a provision on regulatory cooperation in areas such as electronic trust and authentication methods, spam, online consumer protection and other matters relevant to digital trade.[185] This provision however does not include cybersecurity cooperation, which seems surprising given that cybersecurity cooperation was included in the Framework Agreement and is not atypical of EU FTAs.[186] Further, the EU appears to exclude mechanisms for regulatory cooperation on privacy and data protection issues:

> For greater certainty, this provision shall not apply to a Party's rules and safeguards for the protection of personal data and privacy, including on cross-border transfers of personal data.

The above provision appears undesirable because it reduces the possibility for Australia and the EU to seek mechanisms for achieving interoperability between their privacy frameworks to facilitate cross-border flows of personal data. Given the importance of data-driven trade for the both the parties, this provision seems over-cautious and defensive, especially since the proposed chapter already contains strong provisions on data protection (Article 6) and right to regulate (Article 2).

Reports also indicate that Australia and the EU have agreed on a provision on open government data.[187] While the proposed text is not available, both the SADEA[188] and the EU-UK TCA[189] contain a non-binding provision on open government data, which although not identical, is similarly worded. The key objective is recognising that "facilitating public access to and use of government information contributes to stimulating economic and social benefit, competitiveness, productivity improvements and innovation".[190] Further, parties are encouraged to provide public data in a user-friendly and accessible manner, consistent with principles of data protection.[191] Given that this is a high-level and non-binding provision, to which Australia and the EU have

[181] EU proposal, Digital Trade Chapter, Australia – EU FTA, art. 10.
[182] EU proposal, Digital Trade Chapter, Australia – EU FTA, art. 13.
[183] EU proposal, Digital Trade Chapter, Australia – EU FTA, art.13(1).
[184] See, e.g., Report of the 6th round of negotiations for a Free Trade Agreement between the European Union and Australia**,** 10-14 February 2020, https://trade.ec.europa.eu/doclib/docs/2020/february/tradoc_158656.pdf (last accessed 23 January 2021).
[185] EU proposal, Digital Trade Chapter, Australia – EU FTA, art. 14(1); art. 13(2).
[186] See, e.g., Japan -EU EPA, art. 8.80(2)(c).
[187] Report of the 8th round of negotiations for a trade agreement between the European Union and Australia, September 2020,https://trade.ec.europa.eu/doclib/docs/2020/october/tradoc_158976.pdf (last accessed 23 January 2021).
[188] SADEA, art. 27
[189] EU-UK TCA, art. DIGI.15.
[190] SADEA, art. 27.2; EU-UK TCA, art. DIGI.15.1.
[191] SADEA art. 27.3; EU_UK TCA, art. DIGI.15.2.

agreed with other trading partners, it is quite likely that the final provision will be similarly worded as the EU-UK TCA. Further, reports also suggest that parties have agreed on provisions on paperless trading and open internet access. These provisions are likely to be modelled very similar to the existing provision in some recent PTAs.

Over-all, several of the digital trade provisions currently being considered to be included in the Australia – EU FTA will create an open and robust environment for digital trade and enhance opportunities for digital trade between the two regions. Further, disciplines on electronic transactions, e-signatures, paperless trading, and online consumer protection will be important in creating security and predictability in digital trade as well as reduce transaction costs for businesses. The inclusion of modern-day digital trade provisions such as disciplines on source code disclosure requirements and prohibition on data localisation are also welcome changes. In that regard, the Australia – EU FTA is likely to achieve a stronger balance between provisions requiring the free flow of data and other regulatory pre-requisites for enabling data flows such as privacy protection and consumer trust as compared to the CPTPP.[192] The EU has also demonstrated its willingness to consider including disciplines on broader digital economy issues such as open government data. While several of these developments are positive, the General Data Protection Regulation ("GDPR") disciplines on cross-border data transfers will be a major barrier for Australian businesses intending to conduct business in the EU. These challenges are addressed in the next section.

4.2 Placing the Australia – EU PTA in the Digital Trade Realm: A Future-Forward Approach

The previous section identifies various provisions likely to be included in the Australia – EU PTA and their potential impact on digital trade between the parties. While the EU and Australia appear to be moving forward on several areas of digital trade in their trade negotiations, this section identifies three areas critical to strengthen their digital trade links: (i) identifying and agreeing upon relevant cooperation mechanisms and standards for data transfers and arriving at a consensus regarding how their respective data protection frameworks could be made interoperable; (ii) adopting new trade disciplines that can enable innovation by MSMEs, especially taking advantage of digitalisation; and (iii) experimenting with new forms of institutional cooperation in digital trade, including participation in parallel mechanisms at the OECD, G20, WTO and internet multistakeholder institutions. Of these three areas, an agreement on cross-border data transfers and data protection appears to be the most challenging.

4.2.1 Data Protection and Privacy

The biggest impediment that Australian businesses are likely to face while conducting digital trade with the EU is the incompatibility of their respective regulatory frameworks on data protection.[193] While a detailed discussion is outside the scope of this paper, the GDPR and the Privacy Act in Australia have several notable differences. First, the GDPR is much broader in scope and applies to all businesses that offer services in the EU or even monitor the behaviour of EU residents.[194] In contrast, the Privacy Act generally applies to specified entities with a turnover of more than 3 million AUD with

[192] See generally Mishra (2017).
[193] Lee-Makiyama (2018), p. 214.
[194] GDPR, art. 3.

the exception of those trading in personal information or providing health services.[195] Thus, even a sole Australian entrepreneur intending to offer digital services in the EU must comply with the GDPR. Further, the GDPR classifies a broader range of information as personally identifiable information, including tracking cookies. In the ongoing negotiations, the EU and Australia are working toward a common definition of personal data.[196] This is likely to be a challenging task given the different definition of personal data in the EU and Australian law.

Second, the GDPR provides individuals with broader scope of rights compared to the Australian data protection law such as the right to data portability, right to be forgotten and right not be subjected to automated decision-making, thereby increasing compliance burden for any business handling personal data of Europeans.

Most importantly, while Australia has adopted an accountability-based mechanism for cross-border data transfers,[197] the EU has adopted a prescriptive mechanism, whereby, data can only be transferred to countries that have obtained a positive adequacy finding (Australia has not obtained a positive adequacy finding, to date) or if the business can offer appropriate safeguards (e.g., Standard Contractual Clauses).[198] As the latter option entail huge compliance costs, most MSMEs in Australia are unlikely to be able to exercise that option.[199]

Adequacy findings require long bilateral negotiations. The EC considers several factors in adequacy negotiations pertaining to the foreign country including their data privacy/protection framework, respect for rule of law, international commitments to data protection, and the strength of their economic and political relationship with the European Union.[200] Although New Zealand has obtained a positive adequacy finding, it remains unclear if Australia will be able to achieve this in the future. Experts have pointed out how this may cause business uncertainty in the future, given that New Zealand entities offering their services in the EU will be unable to operate through their Australian subsidiaries.[201]

Given the importance of digital interconnectivity for digital trade between the EU and Australia, the EU must use the ongoing FTA negotiations with Australia as a platform to explore new mechanisms to enable cross-border data transfers between the two regions. The CPTPP and several Australian PTAs already contain a provision that encourages parties to explore mutual recognition mechanisms for their privacy frameworks, as discussed previously in Section 3.2. A similar provision must be considered in the context of Australia – EU FTA. Several experts have also indicated the advantages of including language in PTAs to foster interoperability among privacy regimes.[202] For instance, as Australia already endorses the APEC CBPR, the EU can

[195] Office of the Australian Information Commissioner, Australian Privacy Principles Guidelines, https://www.oaic.gov.au/assets/privacy/app-guidelines/app-guidelines-july-2019.pdf (last accessed 23 January 2021).
[196] Report of the 8th round of negotiations for a trade agreement between the European Union and Australia, September 2020,https://trade.ec.europa.eu/doclib/docs/2020/october/tradoc_158976.pdf (last accessed 23 January 2021).
[197] The only restriction in Australian law is the cross-border transfer of e-health records. See Personally Controlled Electronic Health Records Act 2012 (Cth), s. 77.
[198] See GDPR, Chapter 5.
[199] Submission of the Australian Business in Europe, 27 June 2019, p.4-5, https://www.dfat.gov.au/sites/default/files/australian-business-in-europe-eufta-submission.pdf (last accessed 23 January 2021).
[200] GDPR, art. 45(2).
[201] Lee-Makiyama (2018), p. 214.
[202] Meltzer (2018), p. ix.

explore possible compatibility between the mechanisms available under the GDPR and the CBPR certification mechanism. Further, as was the case while negotiating the Japan-EU EPA, the EU and Australia must consider engaging in parallel dialogues regarding negotiation of adequacy arrangements with Australia in the near future.

4.2.2. Boosting the Growth of MSMEs

The proposed digital trade chapter in the Australia – EU FTA currently does not contain any provisions tailored towards facilitating the growth of MSMEs. In that regard, provisions on electronic payments and e-invoicing found in the SADEA and DEPA and the provision on logistics in the DEPA provide a good foundation for enabling MSMEs struggling to integrate in the global e-commerce markets due to the uncertainties in the global e-commerce framework. Such provisions are particularly instrumental for both the EU and Australia due to the high possibility of dynamic innovation by digital start-ups in these countries.

The provision on logistics in the DEPA states:

> 1. The Parties recognise the importance of efficient cross border logistics which would help lower the cost and improve the speed and reliability of supply chains.
>
> 2. The Parties shall endeavour to share best practices and general information regarding the logistics sector, including but not limited to the following:
>
> (a) Last mile deliveries, including on-demand and dynamic routing solutions;
>
> (b) The use of electric, remote controlled and autonomous vehicles;
>
> (c) Facilitating the availability of cross-border options for the delivery of goods, such as federated lockers;
>
> (d) New delivery and business models on logistics.

Although it is not legally binding, a similar provision could facilitate greater cooperation between the EU and Australia to share best practices and help small companies navigate the problems around small-value shipments and managing demands in real-time.[203] Another useful example is the provision on electronic invoicing in the SADEA, which facilitates cross-border interoperability of their electronic invoicing frameworks and collaboration on initiatives that facilitate the adoption of electronic invoicing by domestic companies.[204] As both Australia and the EU are digitally developed with high regulatory expertise, such a provision appears feasible for both the parties to implement meaningfully.

Another useful example that the negotiators of the Australia – EU FTA can consider is the provision on electronic payments in the SADEA.[205] Some of the key features of this provision are: (i) requiring parties to be transparent about their laws and regulations on electronic payment services; (ii) encouraging the adoption of international standards for data exchange and messaging in electronic payment systems; (iii) encouraging regulatory sandboxes in the fintech sector; (iv) possibility of greater interoperability and competition by facilitating open platforms and architectures in electronic payment systems; and (v) recognising the importance of a proportionate risk-based approach in regulating electronic payment systems. A provision containing such high-level principles on electronic payments, albeit largely soft in nature, can still be critical in the growth of fintech start-ups providing services in both Australia and the EU.

---

[203] See generally Mitchell and Mishra (2020).
[204] SADEA, art. 10.
[205] SADEA, art. 11.

4.2.3 Experimenting with New Models of Cooperation

As explained previously in Section 2, the EU and Australia share several common economic interests pertaining to the digital economy. The Australia – EU FTA can be critical in fostering sustainable cooperation between the two parties on relevant areas in digital trade. While some issues such as data transfer mechanisms may appear intractable in the short run, continued dialogues on these issues can help both parties to reach a practical solution to manage their regulatory differences on data protection.

In that regard, similar to some EU FTAs,[206] setting up a committee on electronic commerce with representatives from both parties will be helpful to not only monitor the implementation of the existing digital trade rules in the FTA but also explore new avenues where high-level disciplines may be beneficial. While the relevant FTA committee cannot and should not prescribe substantive norms and standards on these issues, it can facilitate transparent, informal dialogues and a common understanding between the parties on some of these issues including a consensus on the relevant international standard for data protection, cybersecurity, and AI regulation.

The DEPA and SADEA provide various examples where parties have agreed to engage in regulatory dialogues such as AI frameworks, data innovation, fintech/regtech, and digital competition policy. Such disciplines will also be relevant for digitally advanced countries in the EU to develop greater regulatory cooperation with their Australian counterparts. In turn, such cooperation can translate into meaningful policy advocacy and action in other international fora such as the WTO (e.g., JSI negotiations), G20 (e.g., facilitating the data free flow with trust framework) and the OECD (e.g., reforms on digital taxes). Similarly, the EU and Australia could develop a common position in the ICT standardisation debates in various internet multistakeholder and private standard-setting organisations.

Sectoral regulators in Australia and Singapore have currently signed several memoranda of understanding in areas such as electronic invoicing, data protection, fintech and regtech, and data innovation to exchange best practices, share information and potentially, develop a common position on specific issues.[207] Such an approach could also be replicated under the Australia – EU FTA. In the long run, novel cooperation mechanisms between like-minded partners will be critical in building greater transnational consensus and facilitating international regulatory cooperation in digital trade. The Australia – EU FTA provides an opportunity to explore and experiment with such mechanisms, which must not be lost.

5 Conclusion

The Australia – EU FTA lays an important foundation for strengthening the economic relationship between the EU and Australia. The Digital Trade Chapter in this FTA can contribute to this relationship, given the immense potential for increasing digital trade between the EU and Australia. This mutual economic interest is well complemented by the shared values of the EU and Australia regarding the development of data-driven technologies and internet governance.

Historically, Australia and the EU have adopted different approaches in their Electronic Commerce Chapters in PTAs. While Australia has adopted more comprehensive

[206] See, e.g., EU-KR FTA, art 7.3.

[207] See DFAT, Australia-Singapore Digital Economy Agreement, https://www.dfat.gov.au/trade/services-and-digital-trade/Pages/australia-and-singapore-digital-economy-agreement (last accessed 23 January 2021).

electronic commerce chapters with deeper commitments, the EU has stuck to a more bare-bones framework focusing largely on consumer trust and electronic transactions-related issues. However, in recent years, greater convergence can be observed in their PTA practices, with the EU agreeing upon provisions on source code disclosure requirements and data localisation in its recent FTAs. Based on these developments, it appears that the Australia – EU FTA will contain several digital trade disciplines including e-signatures, e-authentication, paperless trading, customs duties on electronic transmissions, online consumer trust and spam, trade disciplines on source code disclosure, and data localisation. Public reports also indicate that both parties are considering new areas such as open government data. However, the framing of the provisions on transborder data flows and data protection is likely to be a sticky issue for the parties. The EU's draft proposal indicates its preference to provide a blanket exemption for its GDPR disciplines on cross-border data flows. This approach is however not suited to Australian business interests and does not align with their past FTA practice.

Instead of bypassing such tricky issues, the negotiators of the Australia -EU FTA must see the negotiations as a meaningful opportunity to deliberate upon more ambitious digital trade disciplines that are mutually beneficial and essential to create new digital trade opportunities, especially for MSMEs in their respective economies. In that regard, the negotiators should remain mindful that the negotiations offer an opportunity to build mutual consensus and foster cooperation in data regulation, including data transfer mechanisms and standards. Further, the FTA negotiations provide an opportunity to consider deeper disciplines on digital trade facilitation that can nurture digital start-ups and experiment with novel models for regulatory cooperation to facilitate trade in emerging technologies such as AI and fintech.

References

Australian Government (2018) Australia's tech future: delivering a strong, safe and inclusive digital economy

Australian Trade and Investment Commission (2016) Investment opportunities in digital technologies in Australia

Burri M, Polanco R (2020) Digital trade in preferential trade agreements. Journal of International Economic Law 23(1): 187- 220

Burri M (2016) Designing future-oriented multilateral rules for digital trade. In: Sauvé P, Roy M (eds.), Research handbook on trade in services, Edward Elgar (online), pp 331-356

DFAT (2017) Australia's international cyber engagement strategy

Elijah A (2017) Is the CETA a Road Map for Australia and the EU? In: Elijah A et al (eds), Australia, the European Union and the new trade agenda, ANU Press, Canberra, pp 55-74

Elms D (2017) Understanding the EU–Singapore Free Trade Agreement. In: Elijah A et al (eds) Australia, the European Union and the new trade agenda, ANU Press, Canberra, pp 35-54

EPIC consortium (2019) Getting AI Right: Australian-Europe collaboration potential to maximise AI. EPIC Project policy brief #4

Lee-Makiyama H (2018) E-commerce and digital trade. In: Drake-Brockman J, Messerlin P (eds) Potential benefits of an Australia-EU Free Trade Agreement: key issues and options. University of Adelaide Press, Adelaide, pp 211-224

Meltzer JP (2018) Digital Australia: an economic and trade agenda. Global Economy and Development Working Paper 118, Brookings

Mishra N (2021) International trade law meets data ethics: a brave new world. New York Journal of International Law and Politics (Forthcoming, 2021)

Mishra, N (2017) The role of the Trans-Pacific Partnership Agreement in the internet ecosystem: uneasy liaison or synergistic alliance? Journal of International Economic Law 20(1): 31–60

Mitchell, AD, Mishra, N (2020) Digital trade integration in preferential trade agreements. ARTNeT Working Paper Series No. 191, Asia-Pacific Research and Training Network on Trade

Monteiro JA, Teh R (2017) Provisions on electronic commerce in regional trade agreements. WTO Working Paper ERSD-2017-11, World Trade Organization

Parliament of the Commonwealth of Australia (2018), Trade and the digital economy. Joint Standing Committee on Trade and Investment Growth

Willemyns I (2020) Agreement forthcoming? A comparison of EU, US, and Chinese RTAs in times of plurilateral e-commerce negotiations. Journal of International Economic Law 23(1): 221-244

	CETA	EU-Mexico Globalised Agreement	EU-KR FTA	EU-SG FTA	EU-VN FTA	Japan-EU EPA	EU-CARIFORUM FTA	EU-UK TCA
Objective and purpose: Economic growth, boosting trade opportunities	✓	✓	✓	✓	✓	✓	✓	✓
Specific recognition of right to regulate	×	✓	×	✓	✓	✓	×	✓
Specific scope or exclusions	×	✓	✓	✓	✓	✓	×	✓
Non-discrimination of digital products	×	×	×	×	×	×	×	×
Customs duties on electronic transmissions	✓	✓	×	✓	×	✓	×	✓
Online consumer protection	✓	✓	×	×	×	✓	×	✓
Framework for protection of personal information	✓	×	×	×	×	×	✓	✓
Cybersecurity-dedicated provision	×	×	×	×	×	×	×	×
Data Localisation	×	×	×	×	×	×	×	✓
Cross-border transfer of information	×	×	×	×	×	×	×	✓
Domestic regulation in e-commerce	×	×	×	×	×	✓	×	×
No prior authorisation requirement	×	✓	×	×	×	✓	×	✓
Open Internet Access	×	✓	×	×	×	✓	×	×
Electronic signatures and authentication	✓	✓	×	×	×	✓	×	✓
Spam	✓	✓	×	×	×	✓	×	✓
Involuntary disclosure of source code	×	✓	×	×	×	✓	×	✓
Transparency in e-commerce	✓	×	×	×	×	✓	×	×
Definition of computer services	×	×	✓	✓	✓	×	✓	✓
Dialogues/cooperation on e-commerce	✓	✓	✓	✓	✓	✓	✓	✓
Paperless trading	×	×	✓	×	×	×	×	×
Open Government Data	×	×	×	×	×	×	×	✓
Separate Chapter	✓	✓	×	×	×	×	✓	✓

Annex 1: Comparison of Electronic Commerce Chapters in EU PTAs

	CPTPP	ChAFTA	HK-AFTA	IAEPA	KAFTA	PAFTA	JAEPA	SADEA
Objective and purpose - Economic growth, boosting trade opportunities etc.	✓	✓	✓	✓	✓	✓	✓	✓
Specific recognition of right to regulate in Section/Chapter on Electronic Commerce	×	×	×	×	×	×	×	×
Specific scope or exclusions from Electronic Commerce Chapter	✓	×	✓	×	×	✓	×	✓
Non-discrimination of digital products	✓	×	×	×	×	✓	✓	✓
Customs duties on electronic transmissions	✓	✓	✓	×	✓	✓	✓	✓
Online consumer protection	✓	✓	✓	✓	✓	✓	✓	✓
Protection of personal information	✓	✓	✓	✓	✓	✓	✓	✓
Cybersecurity-dedicated provision	✓	×	×	×	×	✓	×	✓
Data Localisation	✓	×	✓	✓	×	✓	×	✓
Cross-border transfer of information	✓	×	✓	✓	×	✓	×	✓
Domestic regulation in e-commerce	×	×	×	×	✓	×	✓	✓
Open Internet Access	✓	×	×	×	×	✓	×	✓
Electronic signatures and authentication	✓	✓	✓	✓	✓	✓	✓	✓
Spam	✓	×	✓	✓	✓	✓	×	✓
Involuntary disclosure of source code	✓	×	✓	✓	×	✓	×	✓

Transparency in e-commerce	×	✓	×	✓	×	×	×	✓
Definition of computer services	×	×	×	×	×	×	×	×
Dialogues/cooperation on e-commerce	✓	✓	✓	✓	×	✓	✓	✓
Paperless trading	✓	✓	✓	✓	✓	✓	✓	✓
Domestic electronic transactions framework	✓	✓	✓	✓	✓	×	×	✓
Logistics, express shipments	×	×	×	×	×	×	×	✓
Electronic invoicing	×	×	×	×	×	×	×	✓
E-Payments	×	×	×	×	×	×	×	✓
Digital Identities	×	×	×	×	×	×	×	✓
Artificial Intelligence	×	×	×	×	×	×	×	✓
Open Government Data	×	×	×	×	×	×	×	✓
Data Innovation	×	×	×	×	×	×	×	✓
Separate Chapter	✓	✓	✓	✓	✓	✓	✓	✓

Annex 2: Comparison of Electronic Commerce Chapters in Australian FTAs