AUT0055 – Emily Jones et al

Digital Trade Provisions in the AUS-UK FTA

Emily Jones,[i] Danilo Garrido Alves,[ii] Beatriz Kira,[iii] and Rutendo Tavengerwei[iv]

We are submitting evidence in our capacity as researchers at the Blavatnik School of Government, University of Oxford. The Blavatnik School of Government is committed to improving the quality of government and public policymaking worldwide.

Introduction

In December 2021, the UK and Australia signed a free trade agreement (hereafter AUS-UK FTA), which is now being scrutinised prior to ratification. The UK and Australia are both seeking to position themselves as world leaders in digital trade and the UK government stated that the new agreement is 'setting new global standards in digital' with 'cutting-edge agreements in areas where Britain is a world leader, including in digital and tech'.[v]

Digital trade is increasingly important for the UK economy: roughly 25% of all UK trade in services and goods was digitally delivered in 2019,[vi] a percentage that has likely grown due to the pandemic. Digital trade also corresponds to a significant proportion of trade between the UK and Australia – in 2019, the UK exported £4.3 billion worth of services to Australia digitally, over 50% of all services between the two countries.[vii] The AUS-UK FTA is the first from-scratch free trade agreement that the UK government has negotiated since it exited from the European Union. As such it important not only because it will govern future trade relations between the UK and Australia but because it sets a precedent for the UK's future trade negotiations.

In this note we examine the digital provisions in the AUS-UK FTA, explain how they differ from previous UK trade agreements, and highlight possible public policy implications.[viii] Our headline findings are that:

- The provisions on digital trade are more extensive than previous UK trade agreements and include new or substantially revised provisions, including on digital identities, digital transferable records, e-invoicing, data innovation, paperless trading, and regulatory cooperation, as well as a chapter dedicated to innovation (see Table 1). These provisions draw extensively on the Australia-Singapore Digital Economy Agreement (2020), although in some areas the AUS-UK FTA is less ambitious than the Australia-Singapore DEA, notably on online harms and competition.
- In general, the digital trade commitments aim at 'binding' existing practices and increasing cooperation rather than requiring changes to current regulations or policies. Nonetheless, the commitments condition

what the UK will be able to do in future and have substantial implications for important areas of UK digital policy that are still evolving, including data protection, online harms, regulation of AI, digital identities, financial regulation, and cyber security. In the area of data regulation, questions remain as to the compatibility of the UK's commitments with its existing regime for personal data protection. Given that the UK's data protection regime is based on the EU's GDPR, it is striking that it has not followed the EU's path in negotiating more robust protections for its personal data regime.

- Careful analysis and evaluation of the provisions is important for ensuring consistency between the text of the treaty and areas of existing or proposed domestic policy, to ensure that commitments in the FTA strike an appropriate balance between different policy objectives (such as the promotion of AI and data protection), and do not unduly restrict the government's future ability to regulate fast-moving technologies. As we explain below, in some areas there are concerns that commitments are too narrow and specific to ensure effective policymaking.
- The agreement places substantial emphasis on enhancing government-to-government cooperation in the digital economy, which is important given the rapid evolution of digital technologies and the challenges governments face in developing policy that promotes innovation while also ensuring ethical use of data and new technologies and safeguarding digital rights of citizens.
- The UK has created a Digital Regulation Cooperation Forum to improve coordination across government which brings together the Competition and Markets Authority, Information Commissioner's Office, the Office of Communications, and the Financial Conduct Authority. It is unclear from public documents the extent to which this Forum has advised on the details of digital trade provisions in the AUS-UK FTA.
- Comparing the final text with the policy positions of key interest groups suggests that the provisions on digital trade generally align with requests articulate by major UK business groups. In some areas the agreement makes modest steps forward in promoting consumer interests and digital rights but does not go as far as consumer and digital rights groups would like. The agreement makes no mention of strengthening gig-economy labour protections, which is striking as more than 4 million people work in the gig economy in the UK[ix] and there are widespread concerns about gig economy employment practices. This is an area in which the UK and trading partners could look to innovate in future. Although the government has a specific mechanism for consulting with UK businesses on digital trade - the Trade Advisory Group on telecoms and technology – there is no analogous mechanism for consumer groups, digital rights groups, or labour organisations.

Issue 1: Trade facilitation (customs duties, e-signatures, e-contracts, e-authentication, e-payments, paperless trading)

A series of provisions in the AUS-UK agreement aim to make it easier for all types of business to leverage digitalisation to facilitate their cross-border transactions. Parties commit not to impose **customs duties on electronic transmissions** (Art 14.3); to try an implement '**paperless trade**' whereby all customs and other trade compliance paperwork can be completed digitally (Art 14.8); to ensure that **contracts made by electronic means** have equivalent effect to their paper counterparts (Art 14.5); to facilitate the use of **digital transferable records** (Art 14.4); facilitate the use of **e-authentication and electronic trust services** (Art 14.6) by ensuring that electronic forms of signature have equivalent legal effect to their paper counterparts, ensuring parties to a transaction are free to decide the form of authentication (subject to a limited exception), and promoting interoperability of e-authentication methods; promote compatibility between their regulatory regimes for **digital identities** (Art 14.7); promote interoperability between their respective **e-invoicing systems**, and to promote this internationally (Art 14.9); and support cross-border **e-payments** by promoting adoption of international standards, interoperability, and encouraging innovation and competition (Art 9.16).

In general, the commitments 'bind' existing practice (e.g. in the area of customs duties) and promote cooperation rather than oblige either Party to make significant changes. The provisions generally reflect the requests of UK businesses keen to ensure they can conduct cross-border business transactions without needing to use paper documents, and ensure interoperability so that they can use the same forms of electronic processes in different jurisdictions (e.g. e-signatures, digital identities).

The provisions on digital trade facilitation are more extensive than the CPTPP and UK-Japan FTA, building from text found in the Australia-Singapore DEA (Table 1). Commitments on paperless trade and e-invoicing, were not found in the UK-Japan FTA. There is explicit recognition of the importance of enabling businesses to use digital transferable records, and the Parties make a soft commitment to 'endeavour to take into account' the relevant UNICTRAL Model Law (2017) in developing domestic policy. The provision is similar to one in Australia-Singapore DEA and is in line with requests from UK businesses which expect substantial efficiency gains, including for SMEs.[x]

Table 1: Comparison of AUS-UK FTA provisions on digital trade with other recent agreements

Provision	AUS-	AUS-Sing	UK-Japan	CPTPP
Issue 1: Trade Facilitation				
Customs duties on electronic	ü	ü	ü	ü
Paperless trade	ü	ü	-	(ü)

Electronic contracts	ü	-	ü	-
Electronic transferable	ü	ü	-	-
E-authentication and trust	ü	ü	ü	ü
Digital identities	ü	ü	-	-
E-invoicing systems	ü	ü	-	-
Issue 2: Cross-border data flows				
Free flow of data & data	ü	ü	ü	ü
Personal information	ü	ü	ü	ü
Financial data - free flow	ü	ü	ü	ü
Financial data – localisation	ü	(ü)	ü	-
Open government data	ü	ü	(ü)	ü
Data innovation	ü	ü	-	-
Issue 3: Innovation and regulation of new technologies				
Algorithms and source code	ü	ü	ü	ü
Cryptography	ü	ü	ü	-
AI and emerging	ü	ü	(ü)	-
Strategic Innovation	ü	(ü)	-	-
Issue 4: Regulation of digital platforms				
ISP liability (copyright)	ü	ü	ü	ü
Open internet access	(ü)	ü	ü	(ü)
Competition in digital	-	ü	-	-
Issue 5: Online consumer protection				
Online consumer protection	ü	ü	ü	ü
Spam	ü	ü	ü	ü
Online harms	-	ü	ü	ü
Issue 6: Cybersecurity				
Cybersecurity	ü	ü	-	(ü)

Notes: ü = provision is present; (ü) provision is present but less specific; - = no provision.

The UK has made a commitment on digital identities for the first time, and the provision is similar to the Australia-Singapore DEA, with the Parties committing to 'pursue the development of mechanisms to promote compatibility between their respective digital identity regimes' (Art 14.7). However, unlike the DEA, they do not aspire to comparable protection under each other's legal frameworks. This seems prudent given that the early stage of UK policymaking

on digital identities. Consumers and digital rights groups have expressed concerns about the design of digital identities and while Australia has an established digital identities regime, the UK is only now trialling one.[xi]

Issue 2: Cross-border data flows (including privacy, data localisation, open government data, data innovation, financial data)

Cross-border data flows are vital for integrated supply chains and cross-border provision of digital products and services but there are also concerns that allowing data to flow freely may undermine policy objectives such as personal data protection and financial stability. In the AUS-UK text the Parties make a strongly worded commitment **not to 'prohibit or restrict' cross-border flows, including personal information,** if the activity is for the conduct of the business of a covered person, (Art 14.10) and **not to require the localisation of data** (Art 14.11). Both provisions include an exception under which parties may introduce non-compliant measures, but any such measure has to meet a 4-step test: it must be designed to (i) achieve a 'legitimate public policy objective', (ii) not be applied 'in a manner which would constitute a means of arbitrary or unjustifiable discrimination, (iii) not be applied so as to be 'a disguised restriction on trade', and (iv) not impose restrictions 'greater than are required to achieve the objective'.

The AUS-UK text also recognises the importance of **personal information protection** (Art 14.12). The Parties make no specific commitments on the nature of personal data protection and simply commit to implement domestic legal frameworks that protect personal data. Importantly, Art 14.12 explicitly notes that the obligation can be met via a variety of approaches, including the enforcement of voluntary undertakings by enterprises (an approach that is widely viewed as providing lower levels of protection and being less trade-restrictive than the UK GDPR). This approach is very similar to the CPTPP, UK-Japan, and DEA (although unlike the DEA the AUS-UK text stops short of explicitly endorsing the APEC Cross-Border Privacy Rules).

It is important to note that the EU has not made a commitment analogous to Art 14.10 in any of its trade agreements.[xii] As EU privacy scholars have noted, the EU GDPR may not meet the necessity test found in the WTO's general exceptions because other protection frameworks exist for personal data – such as the 2015 APEC Privacy Framework – that are arguably less trade-restrictive.[xiii] Other experts similarly argue that the EU GDPR is unlikely to meet the type of 4-step test found in the CPTPP (which is replicated in the AUS-UK FTA).[xiv] Given that the UK's Data Protection Act of 2018 is based on the EU's GDPR, it is striking that the UK has agreed to the 4-step test.

Moreover, the article on personal data protection found in recent EU agreements is very different to that in the AUS-UK text. In the EU-UK TCA for instance, the EU insisted on a very strongly worded provision aimed at protecting the GDPR which states that 'nothing in this Agreement shall prevent a Party from adopting

or maintaining measures on the protection of personal data and privacy, including with respect to cross-border data transfers' provided that specific instruments [e.g. standard contractual clauses] are provided that enable transfers 'under conditions of general application for the protection of the data transferred' (Art 202). This carve-out is intended to help protect the EU from challenge and thereby ensure it retains a high level of autonomy in crafting its personal data protection regime. Again, it is striking that the UK has not replicated the EU approach and negotiated more robust protections for the UK GDPR.[xv]

Consumer and digital rights groups have raised concerns that the type of commitments found in Articles 14.10 and 14.12 of the AUS-UK FTA could lead to a weakening of UK data protection standards over time. The logic underpinning this argument is that by explicitly recognising voluntary undertakings and agreeing to promote compatibility between regimes (Art. 14.12) the UK is essentially treating lower standards as equivalent.[xvi] Coupled with the 4-step test (Art. 14.10) the UK arguably becomes vulnerable to potential challenges by trading partners on the basis that the UK GDPR imposes measures 'greater than are required to achieve the objective'. The concern is that the UK may lower its standards of protection in response to a challenge (or the threat of a challenge). While a possibility, it is hard to assess how likely this is to play out in practice.

In tandem with the FTA, the UK is considering whether to grant Australia data adequacy. Australia has not received an adequacy decision from the EU or UK to date, so transfers of personal data occur mainly through standard contractual clauses, which can be cumbersome and costly, especially for small businesses. If the UK grants adequacy and the EU does not, the UK will need to be careful not to undermine its own adequacy decisions from the EU (which permits free flow of data between the UK and EU) through inadvertent onward transfers of EU data.[xvii]

Like many trade agreements, the digital trade chapter does not cover financial services suppliers (Art 14.1) and provisions for **cross-border flows of financial data** are found in the financial services chapter. The Parties make a general commitment to allow data to flow (Art 9.12.2) and stipulate the conditions under which a Party may require localisation of financial data (Art 9.12.3-5), subject to a general exception for prudential regulation (Art 9.3), a specific exception that covers 'public entities in pursuit of monetary policies and related credit policies, or exchange rate policies' (Art 9.4), as well as a national treatment obligation (Art 9.5). Striking the balance between enabling financial data to flow freely (a demand from businesses, including the UK financial services sector[xviii]) and ensuring regulators have sufficient access to data for regulation and supervision has been a controversial issue in trade agreements. While the provisions in the AUS-UK FTA are similar to the UK-Japan FTA, it is notable that they place more conditions on regulators than the CPTPP text (where there is no commitment prohibiting data localisation for financial data)

and the USMCA text (where the conditions for requiring localisation of financial data are less exacting, see USMCA 17.18).

Although for different reasons, UK technology companies and digital rights groups have been advocating for **open government data.** Technology companies particularly promote the access to large data sets, noting that they are vital to the development of the UK's AI sector. Digital rights groups advocate for commitments by government to make data shareable and re-usable to promote transparency and accountability, and allow citizens an opportunity to engage with their own governance. The AUS-UK agreement contains a provision on open government data (Art 14.13) which is very similar to that found in the Australia-Singapore DEA, the UK-EU TCA and USMCA. The Parties recognise the importance of open government data but stop short of making strong commitments, agreeing to strive towards ensuring that whenever government information is made public, it be up-to-date and easy to access and is 'appropriately anonymised'. Some experts argue that large AI firms with the capacity to collect open data and to correlate it with the 'closed data' they hold benefit disproportionately from such initiatives, and argue that trade agreements should help make privately held data made more accessible to governments, businesses, and citizens. The AUS-UK FTA and other recent agreements are silent on this.[xix]

The AUS-UK FTA also has a provision on **data innovation** (Art 14.14) which is adapted from the Australia-Singapore DEA and promotes the use of regulatory sandboxes to facilitate data innovation. The UK Information Commissioner's Office has an established sandbox approach, so this provision is in line with existing practice.[xx] Regulatory sandboxes enable a direct testing environment for innovative products, services or business models, pursuant to a specific testing plan, which usually includes some degree of regulatory lenience combined with certain safeguards. While sandboxes can spur innovation and facilitate the entry of new products to the market, they also pose risks. Some scholars and consumer groups raise concerns that sandboxes may contribute to a 'race-to-the-bottom' in data protection standards as governments seek to attract start-ups and investors, particularly if their design allows the disapplication of substantial regulatory standards and safeguards.[xxi]

Issue 3: Innovation and regulation of new technologies – protection of algorithm and source code, cryptography, AI and emerging technologies

For technology firms, the protection of proprietary **algorithms and source code** through intellectual property rights has become vital to maintaining their competitive edge. At the same time, as the use of technologies powered by algorithms, such as artificial intelligence, become more widespread, so have public policy concerns with the risks that could be associated with them, including discrimination and lack of fairness and accountability. While technology firms have advocated for provisions in trade agreements that prohibit governments from requiring disclosure of algorithms and source code except

under very specific circumstances, consumers and digital rights groups have expressed concerns that this may impede effective regulation.

The AUS-UK text includes a provision on source code (Art. 14.18) banning Parties from requiring transfer of or access to source code and software as a condition of doing business, subject to a limited exception which provides for specific types of government body to 'preserve and make available' source code for 'an investigation, inspection, examination, enforcement action, or judicial or administrative proceeding'. While the text is very similar to previous agreements, it provides slightly more leeway than the Australia-Singapore DEA as it provides for more government bodies to require disclosure (conformity assessment bodies and independent tribunals) which would enable screening of products *before* they enter the market (as new EU legislation proposes for high-risk AI products) as well as for specific forms of *ex poste* disclosure found in this and other agreements.[xxii] Importantly, the safeguarding exception in the AUS-UK FTA gives authorities actual *access* to the source code, rather than following the CPTPP and DEA approach that merely provides for the possibility of requiring the *modification* of source code for law enforcement purposes.

Future-proofing the carveouts to make space for all the areas of compliance and lawfulness where source code disclosure may be needed is difficult. The AUS-UK text is closer aligned with experts' recommendations for source code exceptions.[xxiii] However, considering the fast-paced nature of innovation in this sector, it is unclear whether the carveouts in the agreement will be sufficient to allow policymakers to fully mitigate existing and potential risks that could emerge from the widespread use of algorithms, and whether consumers and citizens will have means to understand how their data is collected and processed by algorithms outside the scope of judicial or administrative proceedings. Trade unions have also advocated for more algorithmic and source code transparency in trade agreements, especially in light of the growing use of AI in the hiring, management, and dismissal of workers.[xxiv]

On the use of **cryptography** for information and communication services the language found in the AUS-UK text (Art. 14.19) is similar to the provisions included in other UK agreements. Like in the UK-Japan and the DEA, the AUS-UK agreement prohibits parties from adopting regulation that requires access to a particular cryptography technology or access key, with exceptions to networks controlled by the government bodies (including central banks), for the supervision and investigation of financial markets, and for law enforcement purposes. These provisions are important to ensure the integrity and security of encrypted services, and to prevent unlawful interception and electronic surveillance, upholding individuals' right to privacy. There are concerns from the technical community, however, that exceptional access to encrypted communications by law enforcement, such as included in the caveat of the article, might be unfeasible in practice and would create systemic vulnerabilities for users and consumers, for example creating backdoors that could be explored by ill-intentioned agents.[xxv]

The AUS-UK FTA includes a **chapter on innovation** (Chapter 20) which aims to promote trade and economic growth by fostering innovation and draws on similar provisions in the Australia-Singapore DEA. It includes a commitment to cooperate in **AI and emerging technologies** (Art 20.4), promoting activities that encourage the development and adoption of emerging technologies, and facilitating trade in related products and services. It creates a '**Strategic Innovation Dialogue**' between the Parties (Art 20.5) which, seemingly inspired by the DEA's 'Digital Economy Dialogue' (Art 35), will involve the creation of a Joint Committee. Notably, cooperation is focused on promoting innovation and while issues of effective regulation and responsible use of technologies are mentioned, the remit of the Dialogue does not explicitly mention the promotion of digital rights, which limits its relevance for consumer and labour groups. In future trade negotiations the UK could look to strengthen such dialogue initiative to fosters cooperation in the promotion of the digital rights of consumers and citizens, including cooperation in important areas like digital competition and online harms.

The AUS-UK deal further includes provisions on **Fintech** and **Regtech**[xxvi] focusing on promoting trade in these fast-growing areas in which UK companies are globally competitive. The Parties endeavour to "collaborate to improve opportunities for each Party's RegTech enterprises, including through their respective trade promotion agencies and regulators, and in relevant international fora" (Art 14.21). While the commitments are similar to what was agreed by Australia and Singapore in their DEA, the AUS-UK FTA is slightly less ambitious as the it does not have specific headings on Fintech and RegTech (making commitments under articles on "emerging issues" (Art 9C.8) and "cooperation" (Art14.21) respectively) and the commitment is that Parties shall *endeavour* to collaborate, while in the DEA they state they shall *encourage collaboration* (Art 32).

Issue 4: Regulation of platforms (including ISP liability, open internet access, competition in digital markets)

Nations around the world have been drafting and adopting rules on **internet liability**, regulating in what circumstances internet companies are legally responsible for harmful or illegal content shared on their platforms, including for breaches of copyright. UK technology companies have been advocating for the adoption of safe harbours and rules that limit or except them from liability for the content they host or transmit, calling on the UK to adopt provisions analogous to those found in the USMCA, where liability provisions are based on the controversial s.230 of the US Communications Decency Act (CDA).[xxvii] Meanwhile domestic policymakers in many countries have been discussing new rules requiring companies to take more responsibility for content they host (e.g.

the UK Online Safety Bill). In terms of general intermediary liability the AUS-UK adopts a more cautious approach with regards to general liability rules, refraining from including the prescriptive and generous safe harbour regime adopted in the USMCA (Art 19.17.2) that was modelled on section 230 of the US CDA.

In terms of liability related to intellectual property rules, the AUS-UK text the Parties agree to establish and maintain a system to limit the liability and the remedies available against internet companies *at least* for copyright violations as part of the IP chapter (Art 15.88). Provisions on intermediary liability for copyright infringement were already included in the UK-Japan agreement; however, the language in the AUS-UK deal is more detailed and goes slightly beyond the UK-Japan agreement in two-ways, first by committing parties to *the establishment of a system* to limit liability rather than a general commitment to take appropriate measures, and second by opening a window to shield platforms from liability for other types of content, beyond copyright and other intellectual property. At the same time, the AUS-UK deal is not as prescriptive with regards to the model of intermediary liability for copyright violations such as the CPTPP (Art 18.82) and the USMCA (Art 20.88), deals that mirror US domestic legislation (DCMA s. 512) and require parties to establish safe harbours for internet platforms and to adopt a 'notice and take down' mechanism.

Consumer organisations in the UK are concerned that proposed legislation to place greater responsibilities on online platforms for the safety and accuracy of their content could be undermined through commitments made in trade negotiations, leading to weaker protection for British consumers.[xxviii] At the same time, there are concerns that legal mechanisms to limit liability might create incentives for companies to remove more content than required and undermine freedom of speech online.[xxix]

The language on the AUS-UK deal regarding **open internet access** (Art 14.15) provides weaker commitments than previous UK treaties, and indeed replicates the timid language of the CPTPP (Art 14.10). While in the UK-Japan agreement (Art 8.78) and the TCA (Art 170) the government has committed to ensure non-discriminatory access to the internet, consistent with network neutrality principles, in AUS-UK the relevant provision merely *recognises the benefits* for consumers of having access to internet services and applications in a non-discriminatory way, incorporating the same watered-down wording that was agreed in the CPTPP. This goes against calls from UK consumer organisations[xxx] and means that the UK missed the opportunity to get a stronger commitment from Australia on network neutrality, commitments that are central to protect an open and innovative internet, prevent network managers from censoring, filtering or charging more for specific contents.

The provisions in the AUS-UK regarding competition policy are less ambitious that of the DEA, and include more traditional trade provisions related to levelling the playing field and providing technical cooperation, with no explicit mentions

to the specific challenges of promoting **competition in digital markets**. In contrast, the DEA has expressed specific competition concerns related to digital markets, explicitly mentioning the benefits of parties "sharing their experiences in enforcing competition law and in developing and implementing competition policies to address the challenges that arise from the digital economy" (art. 16 DEA). While it is true that the commitments in the DEA related to digital competition are mostly focused on sharing best practices, providing training and technical cooperation, the agreement does express a desire to cooperate in the enforcement of competition in digital markets, "including through notification, consultation and the exchange of information" (art. 16 para. 2, DEA). This acknowledgment that digital markets bring new concerns related to fostering competition reflects efforts from competition authorities and regulators in many jurisdictions, who have been discussing ways to update and complement the conventional competition law toolkit. While domestically the UK Competition and Markets Authority (CMA) has published studies showing the need to rethink competition in these markets and the UK Digital Markets Taskforce has proposed a new pro-competitive regulatory framework, commitments in UK trade agreements are yet to reflect this new approach to digital competition.[xxxi]

Issue 5: Online consumer protection

The rapid shift to business online has made it a necessity for policymakers to ensure that digital marketplaces are safe, and that consumer trust is promoted, particularly when consumers engage in cross-border digital transactions. In the AUS-UK provision on **online consumer protection** (Art.14.16), the Parties commit to maintaining laws that prohibit misleading and deceptive commercial activities, to fostering cooperation between their respective consumer protection agencies, and facilitating access to redress including for consumers from one Party transacting with suppliers from the other. The provision is very similar to that in the Australia-Singapore DEA and provides slightly stronger wording than UK-Japan and CPTPP, as it explicitly recognises the need to provide access to redress for cross-border transactions. It is however not as broad as the DEPA which provides explicit language both on what is considered to be 'fraudulent, misleading or deceptive conduct' prior and during a transaction, as well as the nature of consumer protection laws to be adopted at the delivery stage of goods (Art. 4 – Art. 5 DEPA).

In relation to **spam** (Art 14.17), the Parties follow the same approach as the UK-Japan, CPTPP and Australia-Singapore DEA. This approach is weaker than that followed by the EU as it drops the requirement for prior consent (whereby a consumer must opt-in to receive commercial messages). Parties are however still obligated to adopt laws that enable recipients to opt out of unsolicited messages. The AUS-UK text provides slightly stronger consumer protection than the DEA as it introduces the requirement that "Each Party shall ensure that commercial electronic messages are clearly identifiable as such, clearly disclose

on whose behalf they are made, and contain the necessary information to enable recipients to request cessation free of charge and at any time" (Art 14.17.2). Unlike the Australia-Singapore DEA, no mention is made of the Parties cooperating to address online harms (c.f. DEA Art. 18), despite support from UK consumer organisations.[xxxii]

Issue 6: Cybersecurity

Cyber-attacks are an increasing source of risk in the global economy, are costly for businesses, and undermine trust in the digital economy. In the AUS-UK agreement the Parties agree to strengthen collaboration and domestic capabilities in cyber-defence and encourage businesses to adopt risk-based approaches based on open and transparent **cybersecurity** standards (Art 14.20). This provision is in line with the UK's wider agenda to strengthen international cooperation in cybersecurity, and with the new AUS-UK Cyber and Critical Technology Partnership,[xxxiii] and reflects consensus in global policy debates around risk-based approaches. The provision, modelled on the USMCA, is the strongest and most specific commitment the UK has made in a trade agreement and is broader than provisions in the CPTPP and DEA.

---

[i] Associate Professor, Blavatnik School of Government, University of Oxford
[ii] DPhil Candidate, Faculty of Law, and Research Officer, Blavatnik School of Government, University of Oxford
[iii] Senior Research Associate, Blavatnik School of Government, University of Oxford
[iv] DPhil Candidate, Faculty of Law, and Research Officer, Blavatnik School of Government, University of Oxford
[v] UK Department for International Trade, 'UK and Australia Sign World-Class Trade Deal' (*GOV.UK*, 16 December 2021) <https://www.gov.uk/government/news/uk-and-australia-sign-world-class-trade-deal> accessed 25 January 2022.
[vi] UK Department for International Trade, 'Impact Assessment of the Free Trade Agreement between the United Kingdom of Great Britain and Northern Ireland and Australia' (2021) 21.
[vii] ibid.
[viii] Note that the chapter on digital trade does not apply to audio-visual services, financial services suppliers, or non-conforming measures listed under Chapter 8 (cross-border trade in services) and Chapter 13 (Investment) and only partially applies to government procurement and information held by or on behalf of the Parties (Art 14.1 and Art 14.2).
[ix] TUC, 'Gig Economy Workforce in England and Wales Has Almost Tripled in Last Five Years' (5 November 2021) <https://www.tuc.org.uk/news/gig-economy-workforce-england-and-wales-has-almost-tripled-last-five-years-new-tuc-research> accessed 25 January 2022.
[x] ICC(UK)and Coriolis (2021) CREATING A MODERN DIGITAL TRADE ECOSYSTEM The economic case to reform UK law and align to the UNCITRAL Model Law on Electronic Transferrable Records (MLETR) https://cdn.shopify.com/s/files/1/2992/1976/files/ICCUK-Coriolis-MLETR-Alignment-UK_Business_Case.pdf?v=1619683679
[xi] UK Government, 'UK Digital Identity & Attributes Trust Framework: Updated Version' (*GOV.UK*, 8 September 2021) <https://www.gov.uk/government/publications/uk-digital-identity-attributes-trust-framework-updated-version> accessed 24 January 2022.
[xii] Note that the UK-EU TCA contains a commitment not to impose localisation requirements (Article 201) but it includes no general commitment not to prohibit or restrict cross-border flows.
[xiii] Svetlana Yakovleva and Kristina Irion, 'Pitching Trade against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade' (2020) 10 International Data Privacy Law 201.
[xiv] Graham Greenleaf, 'Will Asia-Pacific Trade Agreements Collide with EU Adequacy and Asian Laws?' [2020] SSRN Electronic Journal <https://www.ssrn.com/abstract=3753215> accessed 11 March 2022.
[xv] See discussion in Emily Jones and others, 'The UK and Digital Trade: Which Way Forward?' (Blavatnik School of Government 2021) <https://www.bsg.ox.ac.uk/research/publications/uk-and-digital-trade-which-way-forward> accessed 19 February 2021.
[xvi] Mira Burri, 'The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation' (2017) 51 UCDL Rev. 65, 116.
[xvii] Zach Meyers and Camino Mortera-Martinez, 'The Three Deaths of EU-UK Data Adequacy' (*Centre for European Reform*, 15 November 2021) <https://www.cer.eu/insights/three-deaths-eu-uk-data-adequacy> accessed 25 January 2022. See also Graham Greenleaf, 'Asia-Pacific Free Trade Deals Clash with GDPR and Convention 108' (Social Science

Research Network 2018) SSRN Scholarly Paper ID 3352288 <https://papers.ssrn.com/abstract=3352288> accessed 5 February 2021.

[xviii] City of London Corporation, 'Memorandum submitted to House of Commons International Trade Committee Inquiry into Digital and Data' (2021) <https://committees.parliament.uk/writtenevidence/22657/pdf/> accessed 25 January 2022

[xix] Thomas Streinz, 'International Economic Law's Regulation of Data as a Resource for the Artificial Intelligence Economy' in Shin-yi Peng, Ching-Fu Lin and Thomas Streinz (eds), *Artificial Intelligence and International Economic Law* (1st edn, Cambridge University Press 2021) <https://www.cambridge.org/core/product/identifier/9781108954006%23CN-bp-9/type/book_part> accessed 15 February 2022.

[xx] https://ico.org.uk/for-organisations/regulatory-sandbox/

[xxi] For a useful discussion see https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652752/IPOL_STU(2020)652752_EN.pdf

[xxii] This type of *ex ante* disclosure for regulatory purposes allows for conformity assessment bodies and regulators to have access to the source code outside the scope of judicial or administrative investigations. See Cosmina Dorobantu, Florian Ostmann and Christina Hitrova, 'Source Code Disclosure: A Primer for Trade Negotiators' in Ingo Borchert and Alan Winters (eds), *Addressing Impediments to Digital Trade* (CEPR Press 2021) <https://www.turing.ac.uk/research/publications/source-code-disclosure-primer-trade-negotiators>.

[xxiii] See ibid. p. 128.

[xxiv] Valerio De Stefano, '"Negotiating the Algorithm": Automation, Artificial Intelligence, and Labor Protection Automation, Artificial Intelligence, & Labor Law' (2019) 41 Comparative Labor Law & Policy Journal 15.

[xxv] James Ball, 'Encryption: The Key to Your Privacy' (*Which? News*, 21 October 2020) <https://www.which.co.uk/news/2020/10/encryption-the-key-to-your-privacy/> accessed 25 January 2022; Harold Abelson and others, 'Keys under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications' [2015] Journal of Cybersecurity <https://academic.oup.com/cybersecurity/article-lookup/doi/10.1093/cybsec/tyv009> accessed 25 January 2022.

[xxvi] FinTech refers to the use of technology to enhance or automate financial services and processes while RegTech aims to help firms to close the gap between compliance and efficiency through technology and automation

[xxvii] David MacCabe and Anna Swanson, 'U.S. Using Trade Deals to Shield Tech Giants From Foreign Regulators' *The New York Times* (7 October 2019) <https://www.nytimes.com/2019/10/07/business/tech-shield-trade-deals.html> accessed 24 January 2022; techUK, 'A Blueprint for UK Digital Trade' (2021) 55.

[xxviii] Which?, 'Digital Trade: Opportunities and Risks in Future Trade Deals' (2020) 11.

[xxix] EDRi, 'Trade Agreements and Digital Rights' <https://edri.org/files/tradelab_eu_trade_and_digitalrights.pdf> accessed 24 January 2022.

[xxx] Which?, 'Are the UK's Trade Deals Reflecting Consumer Priorities?' (2021) 33.

[xxxi] See CMA, 'A New Pro-Competition Regime for Digital Markets: Advice of the Digital Markets Taskforce' (Competition and Markets Authority 2020) <https://assets.publishing.service.gov.uk/media/5fce7567e90e07562f98286c/Digital_Taskforce_-_Advice.pdf>.

[xxxii] Which? (n 29) 29.

[xxxiii] UK Government, 'Cyber and Critical Technology Partnership with Australia: Foreign Secretary's Statement' (*GOV.UK*, 20 January 2022) <https://www.gov.uk/government/news/foreign-secretary-statement-cyber-and-critical-technology-partnership-with-australia> accessed 24 January 2022.