SNG0005 – Emily Jones et al.

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

Digital trade is increasingly important for the UK economy: roughly 25% of all UK trade in services and goods was digitally delivered in 2019,[v] a percentage that has likely grown due to the pandemic. The UK-Singapore DEA is the first dedicated digital economy agreement signed by the UK,[vi] and has been widely advertised as 'the world's most comprehensive' agreement on the topic.[vii] The 49-page agreement is a actually an amendment to the UK-Singapore FTA that was signed in 2020, replacing the e-commerce section of that agreement entirely, and amending other sections in the areas of customs and trade facilitation and financial services (Art.2).

Alongside the DEA text, the UK and Singapore have entered into three Memoranda of Understanding, focussed on digital identities cooperation,[viii] digital trade facilitation,[ix] and cybersecurity cooperation.[x] The nature of these commitments, although non-binding, is reminiscent of the dynamic found in framework conventions - where the bulk of the substantive commitments are not agreed upon from the start. There is thus a risk that actual regulation will take place via MoUs, which are less accountable and provide less opportunities for public participation and Parliamentary oversight than formal treaties, such as free trade agreements.[xi] Due to the extensive scope of the digital provisions and the unusual structure of the agreement, it is important that the UK-Singapore DEA is properly scrutinised by Parliament.

In this note we examine the digital provisions in the UK-Singapore DEA, explain how they differ from previous UK trade agreements, and highlight possible public policy implications. We also discuss the content of the MOUs. Our headline findings are that:

- **The UK-Singapore DEA is the UK's most extensive agreement on digital trade so far**, and arguably the most extensive digital trade agreement in the world. It builds upon other recent agreements, notably the Australia-Singapore Digital Economy Agreement (2020) and the UK-Australia FTA (2022) (see Table 1). It includes novel provisions such as articles on Logistics (Art. 8.61-C), Lawtech cooperation (Art. 8.61-T), and Digital Inclusion (Art. 8.61-P) and is the first agreement to specifically mention the issue of decent work in the digital economy. It also goes further

than previous UK agreements in areas such as digital identities, e-invoicing, electronic authentication, online safety, competition policy, and digital standards and conformity assessment.

- The agreement has **implications for UK digital economy policy in a range of areas** including data protection, online safety, regulation of digital technologies such as AI and Internet of Things, digital identities, and cyber security. 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 UK-Singapore DEA strike an appropriate balance between different policy objectives such as enabling free flow of data and ensuring high levels of personal data protection, and promoting innovation while also ensuring ethical use of new technologies. In some areas there are concerns that commitments are too narrow and specific to ensure effective policymaking and may unduly restrict the government's future ability to regulate fast-moving technologies.
- The agreement focuses on promoting digital trade and the adoption of digital technologies in the UK and Singapore, through commitments by the UK and Singaporean governments to **refrain from imposing some forms of regulation in future** (such as data localisation) and by **promoting inter-operability** between regulatory frameworks. In some areas of digital economy regulation, the Parties agree to work towards **regulatory alignment and mutual recognition**, including in digital identities, e-authentication, and Internet of Things.
- Compared with previous UK agreements, the UK-Singapore DEA makes **modest steps forward in promoting consumer interests, labour protections and digital rights** although stops short of making strong and specific commitments in most cases. Notably the UK-Singapore DEA is the first trade agreement to mention the issue of labour protection in the digital economy. This is important as more than 4 million people work in the gig economy in the UK[xii] and there are widespread concerns about gig economy employment practices. It is the first UK agreement to include articles on online safety and promoting competition in the digital economy, to explicitly acknowledge some challenges associated with new technologies such as unintended bias in the use of AI, and to mention the use of data trusts as a mechanism for improving data sharing. However, the Parties stop short of making strong commitments in these areas, and in the area of open internet access, the commitments are weaker than previous UK agreements.
- Like previous agreements there are strong provisions on cross-border data flows. These are accompanied by a **small change in the legal drafting of the article on personal data protection** which may reduce the risk of downward pressure on UK standards on personal data protection. However, it is striking that the UK has not followed the EU's path in negotiating more robust protections for its personal data regime, and the UK will also need

to exercise caution that any data adequacy decision for Singapore does not undermine its own data adequacy with the EU.

- **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. However, **stakeholder engagement processes remain weak**. In the negotiation of the agreement the UK government had a specific mechanism for consulting with UK businesses - the Trade Advisory Group on telecoms and technology – but there was no analogous mechanism for consumer groups, digital rights groups, or labour organisations (instead they had to rely on more general consultative committees). The UK-Singapore DEA agreement creates a Digital Economy Dialogue with the express aim of promoting stakeholder engagement but the language is vague and although it 'may include participation from other interested stakeholders, such as researchers, academics, and industry' no mention is made of consumer groups, digital rights groups, or labour unions as potential participants.

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

A series of provisions in the UK-Singapore DEA 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 8.59); to try an implement '**paperless trade**' whereby all customs and other trade compliance paperwork can be completed digitally (Art 8.61-B); to ensure that **contracts made by electronic means** have equivalent effect to their paper counterparts and to facilitate the use of **digital transferable records** (Art. 8.60); to facilitate the use of **e-authentication and electronic trust services** (Art 8.61) 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; to promote compatibility between their regulatory regimes for **digital identities** (Art 8.61-S); to promote interoperability between their respective **e-invoicing systems**, and promote this internationally (Art 8.61-A); to support cross-border **e-payments** by promoting adoption of international standards, interoperability, and encouraging innovation and competition (Art 8.54-A); and to implement a single window enabling traders to submit documentation or information required for the exportation, importation and transit of goods through a single entry point (Art 6.13).

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 to existing practice. 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 previous UK agreements (Table 1). The agreement contains a novel article on **logistics** (Art 8.61-C) although it aims to 'share best practice and general information' rather than making specific policy commitments. In the UK-Singapore DEA the parties will share information on last-mile deliveries, including 'on-demand and dynamic routing solutions; the use of electric, remote controlled and autonomous vehicles; facilitating the availability of cross-border options for the delivery of goods, such as parcel lockers; and new delivery and business models for logistics' (Art 8.61-C). The aim is to make last-mile delivery cheaper and more efficient. To reduce costs, logistics companies have been experimenting with last-mile delivery by autonomous drones and delivery to parcel lockers, Singapore is rolling out a national network of parcel lockers that will be open to all logistics companies and e-commerce platforms[xiii], while both the UK and Singapore have been running trials of delivery drones. It is noteworthy that the focus of the article is on efficiency and makes no mention of wider public policy objectives such as addressing pollution and congestion, the privacy implications of drones, or working conditions in the logistics sector.

In other areas of trade facilitation, commitments on **digital transferable records** are slightly stronger than the commitments found previous agreements, with parties committing to 'endeavour to establish a legal framework governing electronic transferable records consistent with the UNCITRAL Model Law on Electronic Transferable Records 2017' (Art. 8.60). The provision is in line with requests from UK businesses which expect substantial efficiency gains, including for SMEs and recent draft legislation in the UK.[xiv] On **electronic authentication**, the Parties 'shall encourage the use of interoperable electronic authentication and work towards the mutual recognition of electronic authentication and electronic digital signatures' rather than simply 'recognise the benefits of working towards mutual recognition' (Art 8.61). Wording is also slightly stronger in **digital identities** with more details on how the Parties may cooperate to promote compatibility and interoperability (Art 8.61-S), and in e-invoicing where the text incorporates language found in the Australia-Singapore DEA and explicitly mentions Peppol 'each Party shall take into account international frameworks when developing measures related to electronic invoicing, such as Peppol' (Art 8.61-A).

The MOU on digital trade facilitation goes into more detail in these areas and sets out three projects to be carried by the UK and Singapore: (i) a pilot project for **electronic transferable records** to transfer simulated transferable electronic bills of lading; (ii) a project on **e-invoicing** information exchanges and capacity building, aimed at learning and exploring the benefits of using common standards (e.g. Peppol) for e-invoicing; and (iii) an e-invoicing pilot project between companies/organisations with cross-border transactions, aimed at demonstrating

the benefits of e-invoicing to encourage adoption of common standards (e.g. Peppol) by companies in both Participants' territories.

In the UK-Singapore DEA text, the UK has made its most ambitious commitment on **digital identities**, going beyond what it had agreed in the UK-Australia FTA to also include a commitment to facilitate the development of 'comparable protection of digital identities under each Party's respective legal frameworks, or the recognition of their legal effects, whether accorded autonomously or by agreement' (Art. 8.61-S.2(b)).

Table 1: Comparison of UK-Singapore DEA provisions on digital trade with other recent agreements

Provision	UK-SG (2022)	UK-NZ (2022)	UK-AUS (2021)	UK-JPN (2020)	AUS-SG (2020)	CPTPP (2018)
Issue 1: Trade Facilitation						
Customs duties (e-transmissions)	✓	✓	✓	✓	✓	✓
Paperless trade	✓	✓	✓	-	✓	(✓)
Electronic contracts	✓	✓	✓	✓	-	-
Electronic transferable records	✓	✓	✓	-	✓	-
E-authentication and trust services	✓	✓	✓	✓	✓	✓
Digital identities	✓	✓	✓	-	✓	-
E-invoicing systems	✓	✓	✓	-	✓	-
E-payments	✓	-	✓	-	✓	(✓)
Logistics	✓	-	-	-	-	-
Issue 2: Cross-border data flows						
Free flow of data & data localisation	✓	✓	✓	✓	✓	✓
Personal information protection	✓	✓	✓	✓	✓	✓
Financial data (free flow & localisation)	✓	✓	✓	✓	(✓)	-
Open government data	✓	✓	✓	(✓)	✓	✓
Data innovation	✓	✓	✓	-	✓	-
Issue 3: Innovation and regulation of new technologies						
Source code disclosure	✓	-	✓	✓	✓	✓
Standards & conformity assessment	✓	-	-	-	(✓)	-
Cryptography	✓	✓	✓	✓	✓	-
AI and emerging technologies	✓	✓	✓	(✓)	✓	-
Strategic Innovation Dialogue	-	-	✓	-	-	-
Fintech and Regtech	(✓)	-	(✓)	-	✓	-
Lawtech	✓	-	-	-	-	-
Issue 4: Regulation of digital platforms						

ISP liability (copyright)	✓*	✓	✓	✓	✓	✓
Open internet access	(✓)	✓	(✓)	✓	✓	(✓)
Competition in digital markets	(✓)	(✓)	-	-	(✓)	-
Issue 5: Online consumer protection						
Online consumer protection	✓	(✓)	✓	✓	✓	✓
Spam	✓	✓	✓	✓	✓	✓
Online harms	(✓)	-	-	-	✓	-
Issue 6: Cybersecurity						
Cybersecurity	✓	✓	✓	-	✓	(✓)
Issue 7: Labour						
Labour protections	(✓)	-	-	-	-	-
Issue 8: Stakeholder engagement, SMEs and Digital Inclusion						
Stakeholder engagement	(✓)	-	(✓)	-	(✓)	-
SMEs	✓	(✓)	(✓)	-	✓	-
Digital inclusion	✓	-	-	-	-	-

Notes: ü = provision is present; (ü) = provision is present but less specific; - = no provision; ü* = present in the UK-Singapore FTA and not removed by the UK-Singapore DEA

This aspiration to comparable protection under each other's legal frameworks can also be found in the Australia-Singapore DEA (Art. 29). The accompanying MOU on digital identities sets out collaboration in more detail, and *inter alia* will 'develop a roadmap to enable the interoperability, mutual recognition and use of digital identities between the Participants', and the roadmap is to be completed over the next 12 months.[xv] This seems premature given that the early stage of UK policymaking on digital identities: while Singapore has an established digital identities regime, the UK has only been trialling one and the Government is yet to table legislation.[xvi]

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. Like in UK-Australia, in the UK-Singapore DEA 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 8.61-F) and **not to require the localisation of data** (Art 8.61-G). 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 UK-Singapore DEA also recognises the importance of **personal information protection** (Art 8.61-E). The Parties make more specific commitments than in previous UK agreements on the nature of domestic legislation, and 'agree that the key principles for its legal framework, which take into account the principles of relevant international bodies, shall include: limitation on collection; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability' (Art 8.61-E.3). Although Art 8.16-E explicitly notes that the obligation can be met via a variety of approaches, unlike previous UK and other recent digital trade agreements it does *no*t include mention of 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).

These innovations are to be welcomed as they reduce the risks of downward pressure on UK's data protection standards. In previous agreements the UK has explicitly recognised voluntary undertakings as sufficient for meeting data protection obligations and agreed to promote compatibility between regimes.[xvii] Coupled with the 4-step test (Art. 8.61-F) this arguably rendered the UK vulnerable to potential challenges by trading partners on the basis that the UK GDPR imposes measures 'greater than are required to achieve the objective' (step iv in the test).

While the revised drafting wording reduces the vulnerability of the UK data protection regime to challenge, it does not go nearly as far as the EU. It is important to note that the EU has not made a commitment analogous to Art 8.61-F in any of its trade agreements.[xviii] 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.[xix] Other experts similarly argue that the EU GDPR is unlikely to meet the type of 4-step test found in the CPTPP and UK-Singapore DEA.[xx] 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 UK-Singapore DEA. In the EU-UK TCA for instance, the EU insisted on a very strongly worded carve-out 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.[xxi]

In tandem with the FTA, the UK has announced that Singapore is a 'top priority' for a **data adequacy** partnership.[xxii] Singapore's national data protection laws are less stringent than the EU GDPR in key areas and Singapore has not received an adequacy decision from the EU or UK to date.[xxiii] As a result, 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.[xxiv]

In relation to financial data, the UK-Singapore DEA includes a specific article on **financial information** (Art. 8.54). The Parties make a general commitment to allow financial data to flow (Art 8.54(1)) and stipulate the conditions under which a Party may require localisation of financial data (Art 8.54(3)). Striking the balance between enabling financial data to flow freely (a demand from businesses, including the UK financial services sector[xxv]) 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 UK-Singapore DEA are similar to the UK-Australia and UK-Japan FTAs, 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 UK-Singapore DEA contains a provision on open government information (Art 8.61-H) which is very similar to that found in the UK-Australia FTA, 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'.

The UK-Singapore DEA also has an article on **data innovation** (Art 8.61-I) which is similar to articles in the UK-Australia FTA and 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.[xxvi] 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.[xxvii]

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 open government data initiatives and argue that trade agreements should help make privately held data made more accessible to governments, businesses, and citizens.[xxviii] Notably, in the UK-Singapore DEA specifically mention 'cooperating on the development of policies and standards for data mobility, including consumer data portability' and 'sharing policy approaches and industry practices related to data sharing, such as data trusts' (Art. 8.61-I.2(b-c)). Data trusts are widely regarded as an important mechanism for enabling data sharing[xxix] and, although the Parties stop short of making strong commitments, effective collaboration in this policy area could help address inequities in access to data.

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 UK-Singapore DEA includes a provision on source code (Art. 8.61-K) 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 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 (including conformity assessment bodies) 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.[xxx] Importantly, like in the UK-Australia FTA, the safeguarding exception in the UK-Singapore DEA gives authorities actual *access* to the source code, rather than following the CPTPP and Australia-Singapore 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 UK-Singapore DEA text is closer aligned with experts' recommendations for source code exceptions.[xxxi] 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 advocated for commitments to ensure greater algorithmic and source code transparency to be included in trade agreements, especially in light of the growing use of AI in the hiring, management, and dismissal of workers.[xxxii]

On the use of **cryptography** for information and communication services the language found in the UK-Singapore DEA text (Art. 8.61-J) is similar to the provisions included in other UK agreements. Like in UK-Australia, UK-Japan and Australia-Singapore DEA, the UK-Singapore DEA 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.[xxxiii]

The UK-Singapore DEA includes an article on **AI and emerging technologies** (Art 8.61-R) under which the Parties will 'endeavour to' develop domestic governance and policy frameworks, that take into account relevant international principles and guidelines, for the ethical, trusted, safe and responsible development and use of AI and emerging technologies (Art 8.61-R.2) and 'shall endeavour' to cooperate on matters related to AI and emerging technologies, listing several potential areas for collaboration (Art 8.61-R.2). In a welcome departure from previous digital trade agreements, the UK-Singapore DEA explicitly provides for cooperation to address some of the challenges of AI, including human diversity and unintended biases, industry-led technical standards, and algorithmic transparency (Article 8.61-R.2(b)) although it stops short of placing substantive obligations on the Parties.

Like previous agreements including the UK-Australia FTA and the Australia-Singapore DEA, there is a mention of **Fintech** and **Regtech**[xxxiv] (Arts. 8.53), fast-growing areas in which UK companies are globally competitive (Fintech refers to the use of digital technologies used to deliver financial services, while Regtech is the use of digital technologies to ensures that companies comply with increasingly complex regulatory requirements). However, unlike the Australia-Singapore DEA where there was a stand-alone provision on Fintech and Regtech that listed specific areas of cooperation, in the UK-Singapore DEA they are only cited as examples of emerging services as part of a wider article on new financial services (Art. 8.53). Parties only commit to *endeavour* to collaborate, while in the Australia-Singapore DEA they state they *shall* encourage collaboration and specifically list areas of cooperation (Art 32).

The UK-Singapore DEA includes the first standalone provision on **Lawtech** (Art. 8.61-T) (the use of technologies to support, supplement or replace traditional methods for delivering legal services). Lawtech can reduce the costs of legal advice to customers and enhance efficiency within legal firms, although care has to be taken to ensure high levels of professional service are maintained, including quality and ethical standards.[xxxv] The article lists potential areas for collaboration including establishing a dialogue; encouraging the sharing of knowledge between their respective regulators, academics, representative bodies and industry bodies; and encouraging service suppliers to explore new business opportunities in the other Party's territory (Art. 8.61-T.1). The Parties 'recognise the value of encouraging the trusted, safe and responsible use of Lawtech' (Art. 8.61-T.2) but do not elaborate on how this will be pursued.

The UK-Singapore DEA also includes a stand-alone article on **standards and conformity assessment** (Art 8.61-D), modelled on the Australia-Singapore DEA but not contained in previous UK agreements. The article emphasises the role standards can play in reducing barriers to trade by increasing compatibility, interoperability, and reliability, and stipulates activities for possible cooperation in standard-setting and conformity assessment, including cooperation in international fora. The specific provision on transparency goes slightly further than the Australia-Singapore DEA as it includes a soft commitment to 'endeavour to' ensure that information on standards, technical regulations and conformity assessment procedures is provided by regulatory bodies 'within a reasonable period of time agreed by the Parties and, if possible, within 60 days' (Art 8.61-D.5).

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).[xxxvi] 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 UK-Singapore DEA does not include any new provisions, so directly incorporates the article on intermediary liability that was in the EU-Singapore FTA and incorporated into the UK-Singapore FTA (Art. 10.47).

Unlike previous agreements signed by the UK, the UK-Singapore DEA has no stand-alone provision on **open internet access** – only a general mention that 'Parties shall endeavour to maintain an open, free and secure Internet in accordance with their respective laws and regulations' within the Article on safety and security online (Art. 8.61-O). This is striking as Singapore has agreed to standalone articles in other treaties (e.g., CPTPP, Art 14.10). In the UK-Japan agreement (Art 8.78) and the TCA (Art 170) the Parties committed to ensure non-discriminatory access to the internet, consistent with network neutrality principles. In the UK-Australia FTA the Parties agreed to a watered-down wording that was closer to the CPTPP, where the relevant provision merely *recognises the benefits* for consumers of having access to internet services and applications in a non-discriminatory way. The absence of any express mention of open internet access goes against calls from UK consumer organisations[xxxvii] and means that the UK missed the opportunity to obtain a stronger commitment from Singapore 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.

However, it should be noted that in the UK-Singapore DEA there is a specific provision on **safety and security online** (Art. 8.61-O). This is the first provision of its kind that the UK has agreed to, despite repeated support from UK consumer organisations.[xxxviii] The provision in the UK-Singapore DEA is nonetheless much softer in language than the Australia-Singapore DEA. The Parties merely 'recognise that a safe and secure online environment supports the digital economy' and 'shall endeavour to cooperate to advance collaborative solutions to global issues affecting online safety and security, including in international fora' (Art. 8.61-O.1&3). In contrast in the Australia-Singapore DEA the Parties entered stronger obligations including 'The Parties shall create and promote a safe online environment where users are protected from harmful content, including terrorist and violent extremist content, and where businesses, innovation and creativity can thrive' (Art 18.1) and 'The Parties shall work together and within international fora to create a safe online environment, in accordance with their respective laws and regulations' (Art 18.4).

An article in the UK-Singapore DEA specifically addresses **competition policy in digital markets** (Art. 8.61-U), which is modelled after the Australia-Singapore DEA and is the most substantive article on competition issues in digital markets

in any UK agreement to date. Aspects of this article are contained in the competition chapter of UK-New Zealand FTA (Art. 18.5), but no mention is made of competition issues in digital markets in the UK-Australia FTA or in the UK-Japan FTA. The article focuses on the 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. Possible technical cooperation activities include exchanging information and experiences; sharing best practices; and providing advice or training, including through the exchange of officials (Art. 8.61-U.1). In addition, the Parties 'shall endeavour to cooperate, where practicable, on issues of competition law enforcement in digital markets between their respective authorities, including through notification, consultation and the exchange of information' (Art. 8.61-U.2). The need to address market concentration in digital markets has become a policy priority for competition authorities in many jurisdictions, including the UK, and there is widespread agreement that the conventional competition law toolkit needs updating to address the challenges of digital markets and that international cooperation is important. The UK's Competition and Markets Authority (CMA) has published studies showing the need to rethink competition in these markets, underscoring the need to for effective international cooperation, and the UK Digital Markets Taskforce has proposed a new pro-competitive regulatory framework.[xxxix] The inclusion of this article is welcome and although it falls short of identifying specific anti-competitive practices and placing obligations on the Parties to address them, it is a step towards stronger cooperation.

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 UK-Singapore DEA provision on **online consumer protection** (Art. 8.61-M), 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 the UK-Australia FTA, 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 8.61-N), the Parties follow the same approach as the UK-Australia, 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 UK-Singapore DEA follows the UK-Australia FTA language, both of which provide slightly stronger consumer protection than the Australia-Singapore DEA, as they include the requirement that 'Each Party shall ensure that unsolicited commercial electronic messages are clearly identifiable as such, clearly disclose on whose behalf they are made, and to the extent provided for in a Party's laws and regulations, contain the necessary information to enable end-users to request cessation free of charge and at any time.' (Art 8-61-N.2).

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. The UK-Singapore DEA contains an extensive provision on **cybersecurity** (Art 8.61-L) which is similar to articles in the UK-Australia FTA and UK-New Zealand FTA and more substantial than provisions in the CPTPP and Australia-Singapore DEA. In some places the wording is watered down in comparison to the UK-Australia FTA as the Parties merely 'recognise the importance of' (rather than 'shall endeavour to') building national capabilities for cyber security incident response; strengthening collaboration mechanisms to cooperate to anticipate, identify and mitigate malicious intrusions or dissemination of malicious code that affect electronic networks, and use those mechanisms to swiftly address cyber security incidents; maintaining a dialogue on matters related to cyber security (Art 8.61-L.1). The UK-Singapore FTA includes novel clauses recognising the importance of 'establishing mutual recognition of a baseline security standard for consumer Internet of Things devices' and 'collaborative cyber security research and development' which were not found in previous agreements (Art 8.61-L.1). As with the UK-Australia FTA and UK-New Zealand FTA, agreements, each Party 'shall encourage' juridical persons within its territory to use risk-based approaches that rely on open and transparent industry standards to 'manage cyber security risks and to detect, respond to, and recover from cyber security events' and 'otherwise improve the cyber security resilience of these juridical persons and their customers' (Art 8.61-L.2).

These collaborations are further elaborated in an accompanying **MoU on cybersecurity cooperation**. Collaboration under the MoU will include working to improve cyber security professional development and build a cyber security skills base; sharing good practices on the approach to cyber and digital technology, including the cyber security of emerging critical technologies and addressing cyber security risk associated with digital service providers (such as managed service providers, cloud service providers and critical software vendors); supporting IoT security through the development of assurance mechanisms, working towards mutual recognition, and working to promote strong IoT security through the ASEAN-Singapore Cybersecurity Centre of Excellence, the Commonwealth and other relevant bodies; and promoting strategic frameworks for conflict prevention, cooperation and stability in cyberspace; promoting a secure by default approach including supporting efforts to build a global consensus. [xl] Whilst non-binding,

there are concerns that the decision to regulate over time through MoUs (Art. 3) hinders Parliamentary oversight and public participation.

Issue 7: Labour standards

Prior to the UK-Singapore DEA, trade agreements had made no mention of strengthening gig-economy labour protections. This is striking given the number of people working in the gig economy (more than 4 million people in the UK),[xli] widespread concerns about gig economy employment practices, and, as platform companies operate across borders, there is the need for regulatory cooperation. The provision on **digital inclusion** (Art. 8.61-P) is a step in the right direction, as it recognises 'the importance of adopting or maintaining labour policies that promote decent conditions of work for workers who are engaged in or support the digital economy, in accordance with each Party's laws and regulations.' It also stipulates that cooperation may include 'promoting labour protection for workers who are engaged in or support digital trade' (Art. 8.61-P.2(e)). However, there is still room for innovation and leadership in this field, as there is no firm commitment to progressively improve labour conditions or any reference to international labour standards that should be upheld for gig workers, for instance. Moreover, labour standards are included in a wider provision on digital inclusion. Framing labour rights as a digital inclusion issue fails to take into consideration those workers that are already part of the digital economy, but that might have been adversely impacted by it.

Issue 8: SMEs, digital inclusion, and stakeholder engagement

Like previous agreements, the UK-Singapore DEA has a specific provision on **Small and Medium Enterprises** that aims to reduce barriers to participation in the digital economy. The Parties 'shall, subject to their available resources, seek opportunities to' promote close cooperation on digital trade between SMEs of the Parties and cooperate in promoting jobs and growth for SMEs; encourage SMEs participation in platforms that help link SMEs with international suppliers, buyers and other potential business partners; and exchange information and share best practices in improving digital skills and leveraging digital tools and technology to improve access to capital and credit, participation in government procurement opportunities, and other areas that could help SMEs adapt to digital trade (Art 8.61-Q). The digital inclusion article contains similar commitments to reduce barriers to participation focusing on 'women and other groups that may disproportionately face barriers to participation in the digital economy' (Art. 8.61-P.2) as well as 'countries who face barriers to such participation' (Art. 8.61-P.4).

Like the Australia-Singapore DEA, the UK-Singapore DEA creates a '**Digital Economy Dialogue**' between the Parties and their stakeholders (Art 8.61-V). This will be held 'at times agreeable to the Parties' and 'to promote the benefits of the digital economy' and 'may include participation from other interested stakeholders, such as researchers, academics, and industry'. The wording of the article is vague and stops far short of creating an effective multi-stakeholder dialogue to address both the opportunities and challenges that arise in the digital

economy. However, this provision is a step in the right direction, as the UK-Australia FTA only envisioned a 'Strategic Innovation Dialogue' (Art. 20.5) with even less opportunity for stakeholder participation.

---

[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, 'Impact Assessment of the Free Trade Agreement between the United Kingdom of Great Britain and Northern Ireland and Australia' 21.
[vi] UK Department for International Trade, 'UK-Singapore Digital Economy Agreement: agreement in principle explainer' (GOV.UK, 9 December 2021) <https://www.gov.uk/government/publications/uk-singapore-digital-economy-agreement-agreement-in-principle-explainer/uk-singapore-digital-economy-agreement-agreement-in-principle-explainer>.
[vii] 'UK Agrees World's Most Comprehensive Digital Trade Deal with Singapore' (*GOV.UK*) <https://www.gov.uk/government/news/uk-agrees-worlds-most-comprehensive-digital-trade-deal-with-singapore> accessed 21 March 2022.
[viii] 'Memorandum of Understanding on Digital Identities Cooperation' (*GOV.UK*) <https://www.gov.uk/government/publications/memoranda-of-understanding-with-singapore-digital-trade-facilitation-digital-identity-and-cyber-security/memorandum-of-understanding-on-digital-identities-cooperation> accessed 22 March 2022.
[ix] 'Memorandum of Understanding on Digital Trade Facilitation' (*GOV.UK*) <https://www.gov.uk/government/publications/memoranda-of-understanding-with-singapore-digital-trade-facilitation-digital-identity-and-cyber-security/memorandum-of-understanding-on-digital-trade-facilitation> accessed 22 March 2022.
[x] 'Memorandum of Understanding on Cyber Security Cooperation' (*GOV.UK*) <https://www.gov.uk/government/publications/memoranda-of-understanding-with-singapore-digital-trade-facilitation-digital-identity-and-cyber-security/memorandum-of-understanding-on-cyber-security-cooperation> accessed 22 March 2022.
[xi] UK House of Lords European Union Committee, 'Scrutiny of International Agreements: Lessons Learned' (2019).
[xii] 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.
[xiii] CityLogistics, 'Singapore Builds a National Carrier-Agnostic Parcel Locker Network' (27 March 2020) <http://www.citylogistics.info/business/singapore-builds-a-national-carrier-agnostic-parcel-locker-network/> accessed 24 March 2022.
[xiv] ICC UK and Coriolis, '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)' (2021) <https://cdn.shopify.com/s/files/1/2992/1976/files/ICCUK-Coriolis-MLETR-Alignment-UK_Business_Case.pdf?v=1619683679> accessed 24 March 2022; Law Commission, 'Electronic Trade Documents' (2021) <https://www.lawcom.gov.uk/project/electronic-trade-documents/> accessed 24 March 2022.
[xv] 'Memorandum of Understanding on Digital Identities Cooperation' (n 8).
[xvi] 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; UK Government, 'New Legislation Set to Make Digital Identities More Trustworthy and Secure' (*GOV.UK*, 10 March 2022) <https://www.gov.uk/government/news/new-legislation-set-to-make-digital-identities-more-trustworthy-and-secure> accessed 24 March 2022.
[xvii] Mira Burri, 'The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation' (2017) 51 UCDL Rev. 65, 116.
[xviii] 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.
[xix] 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.
[xx] 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.
[xxi] 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.
[xxii] UK Government, 'UK Data Partnerships' <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1013047/UK_Data_Partnerships___Map_V2_.jpg> accessed 24 March 2022.
[xxiii] CMS Law, 'A Guide to GDPR for Companies in Singapore' (2018) <https://cms.law/en/media/affiliates/singapore/images/publications/gdpr-guide-for-singapore-companies> accessed 24 March 2022.
[xxiv] 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.

[xxv] 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

[xxvi] Information Commissioner's Office, 'Regulatory Sandbox' <https://ico.org.uk/for-organisations/regulatory-sandbox/> accessed 24 March 2022.

[xxvii] For a useful discussion see Radostina Parenti, 'Regulatory Sandboxes and Innovation Hubs' (2020) <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652752/IPOL_STU(2020)652752_EN.pdf>.

[xxviii] 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.

[xxix] See e.g. Neil Lawrence and Seongtak Oh, 'Enabling Data Sharing for Social Benefit through Data Trusts' (Aapti Institute, Open Data Institute and Global Partnership on AI 2021) <https://gpai.ai/projects/data-governance/data-trusts/enabling-data-sharing-for-social-benefit-through-data-trusts.pdf> accessed 24 March 2022.

[xxx] 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>.

[xxxi] See ibid. p. 128.

[xxxii] 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.

[xxxiii] 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.

[xxxiv] 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

[xxxv] The Law Society, 'Using LawTech in Your Practice' (21 May 2020) <https://www.lawsociety.org.uk/topics/client-care/using-lawtech-in-your-practice> accessed 24 March 2022.

[xxxvi] 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.

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

[xxxviii] ibid 29.

[xxxix] 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>.

[xl] 'Memorandum of Understanding on Cyber Security Cooperation' (n 10).

[xli] TUC (n 13).