The Digital Trade Provisions in the New UK-Japan Trade Agreement

Submission to the International Trade Committee, UK House of Commons

Emily Jones, Associate Professor, Blavatnik School of Government, University of Oxford
Beatriz Kira, Senior Research and Policy Officer, Blavatnik School of Government, University of Oxford

7 November 2020

Executive Summary

1. The UK-Japan agreement is important as it signals a strategic departure from the EU's approach to digital trade. The digital trade provisions in the UK-Japan agreement are not simply a roll-over of the EU-Japan agreement as the Government has agreed substantial new provisions or altered previous provisions. These digital trade provisions have implications for the future of the UK's digital economy in many areas, from the cross-border flows of data, to the protection of citizens' personal data, and the regulation of the internet and new technologies like artificial intelligence and algorithmic decision-making. The provisions have implications for large and small businesses, as well as consumers, and workers. The UK-Japan agreement deserves careful scrutiny as its new digital trade are likely to set a baseline for future UK trade agreements, including with the EU and US.

2. There is a paucity of high-quality publicly available analysis on the digital trade provisions in the UK-Japan agreement, and the Government has yet to provide a detailed explanation for the changes it has made relative to the EU-Japan agreement. Although the Government has consulted stakeholders, detailed, in-depth consultation has been limited, with the government's advisory group on telecoms and technology comprising only of business representatives. Parliament has had limited oversight during the negotiations. **We recommend that more detailed evidence is obtained from Government and a range of independent experts, and is thoroughly discussed with stakeholders, before the UK-Japan agreement is debated in Parliament and ratified.**

3. We examine the provisions in the UK-Japan agreement in four policy areas: cross-border data flows, including privacy and protection of citizen's data; regulation of the internet, including online harms; regulation of new technologies, including algorithm accountability; trade facilitation and consumer protection for online commercial transactions, including spam. For each policy area we explain why these issues are important from a public policy perspective, explain how the UK-Japan agreement departs from the EU-Japan agreement, and explain the possible implications.

4. **We raise specific concerns and highlight issues where further evidence and explanation is warranted on the implications of specific provisions in the UK-Japan agreement. These include (1) The provisions on cross-border data flows and localisation, for personal data protection and obtaining an EU adequacy decision; (2) The provisions on source code, algorithms and cryptography, for the regulation of new technologies and citizens' rights to reasonable explanation and reasonable inferences; (3) The provisions on internet regulation, for online harms and freedom of expression; (4) The provisions on consumer protection for online commercial transactions and spam, for consumer rights in the digital economy.**

Introduction[1]

5. 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. We have examined the digital trade provisions of the UK–Japan Comprehensive Economic Partnership Agreement (CEPA), mainly found under Section F on electronic commerce.

6. We examine the provisions in the UK-Japan agreement in four policy areas: cross-border data flows, including privacy and protection of citizen's data; regulation of the internet, including online harms; regulation of new technologies, including algorithm accountability; trade facilitation and consumer protection for online commercial transactions, including spam. For each policy area we explain why these issues are important from a public policy perspective, explain how the UK-Japan agreement departs from the EU-Japan agreement, and explain the possible implications. We raise specific concerns and highlight issues where further evidence and explanation is warranted.

Importance of digital trade provisions in the UK-Japan Agreement

7. The UK's digital industry is sizeable and growing, accounting for 7.7% of the UK's gross value added in 2018, and employing an estimated 1.6 million people across the UK in 2019. In 2018, roughly one fifth of UK trade with the world in goods and services was digitally delivered, and the figure is higher for Japan, as around one third of UK trade with Japan was digitally delivered in 2018.[2] The Government has identified the growth and development of the UK's digital economy as a strategic priority in its Global Britain economic agenda.[3] Digital trade is a priority in UK trade negotiations, and the Government is consulting on a new National Data Strategy that includes a mission to 'champion the international flow of data'.[4]

8. Digital trade is a fast-moving and contentious area of international trade discussions, with the United States, European Union, and China, the three global superpowers in the digital realm, taking very different approaches. The EU for instance places greater priority on data privacy and consumer protection in its international trade agreements than the US, which prioritises ensuring the free-flow of data across borders, and minimising costs and protecting the intellectual property of its businesses

9. **The UK-Japan agreement is important as it signals a strategic departure from the EU's approach to digital trade. In the UK-Japan agreement the Government has agreed substantial new provisions or altered provisions found in the EU-Japan agreement – including on cross-border data flows and privacy, on regulation of the internet, on the regulation of new technologies, and on consumer protection.**

10. Digital trade provisions in the new UK-Japan agreement have substantial implications for trade between the UK and Japan, and set a baseline for the UK's future trading relations, including with the EU and US. The provisions address many important issues for the future of the UK's digital economy, from the cross-border flows of data, to the protection of citizens' personal data, and the regulation of the internet and new technologies like artificial intelligence and algorithmic decision-

making. The provisions have implications for UK businesses, large and small, as well as UK consumers, and workers.

11. The UK-Japan agreement also signals the Government's intention to influence digital trade policy at the global level, reflected in the Government's statement that the agreement places the UK "at the forefront of shaping new global standards on digital trade".[5] In the Government's words, "CEPA includes digital & data provisions that not only go far beyond the EU's, but also outpace the CPTPP [Comprehensive and Progressive Agreement for Trans-Pacific Partnership] in key areas. This makes CEPA a truly cutting-edge agreement and shows how the UK, through its trade agreements, will shape global standards on digital trade".[6]

12. The UK has an opportunity to take a new and different approach to digital trade and to help shape the future governance of the global digital economy. In doing so the Government has some important strategic decisions to make about which policy objectives will be prioritised, the optimal regulatory measures for furthering these objectives, and how best to achieve these when negotiating international trade agreements. To ensure that wise decisions are made that secure public confidence, including in contentious areas such as data protection and privacy and algorithm accountability, it is vital that digital trade policy decisions are made on the basis of robust evidence, and through deliberation with all stakeholders. Further, given CEPA's implications for domestic policy, it is also important that the digital trade provisions are subjected to cross-department consultation, including scrutiny by the Department for Digital, Culture, Media & Sport (DCMS) and the Department for Business, Energy and Industrial Strategy (BEIS).

13. **The quality and extent of publicly available evidence and analysis on digital trade in the UK-Japan agreement and the reasons for the policy changes is thin.** To our knowledge, there is no publicly available, thorough appraisal of the different policy options available to the Government in negotiating the UK-Japan agreement, or digital trade more generally, nor any detailed explanation for the decisions taken to stay with or depart from the EU's approach in the UK-Japan agreement. The UK Government has published analysis of the UK-Japan agreement but the level of detail on the digital provisions is limited.[7]

14. **In-depth stakeholder consultation on the specifics of the digital trade components of the UK-Japan agreement has been limited.** The Government has undertaken wide, general consultation on the UK-Japan agreement, including through townhalls and online questionnaires. However, in-depth and detailed discussion with stakeholders on the specifics of the UK policy agenda on digital trade and on its proposed approach in the UK-Japan agreement has been limited. Notably, the government's trade advisory group on telecoms and technology comprising only of business representatives.[8] As far as we are aware, consumer groups, trade unions, and policy experts, have had very limited opportunities for meaningful input on the specifics of the UK-Japan text.

15. **Parliament has had limited oversight during the negotiations**, only gaining access to the text of the UK-Japan agreement once it had been signed. This is unlike the practice in the EU, which makes its negotiating proposals public after negotiating rounds, and provides MEPs with access to confidential texts during the negotiations. It is also unlike the US where members of Congress rehave access to the negotiating text during the negotiations.[9]

16. **We recommend that more detailed evidence on the digital trade provisions of the UK-Japan agreement is obtained from Government and a range of independent experts, and is thoroughly discussed with stakeholders, before the UK-Japan agreement is debated in Parliament and ratified.**

17. The UK has an opportunity to set a new, world-class standard for transparent and inclusive trade-policymaking. **Given the importance of the digital trade agenda and the shortcomings identified above, we strongly recommend that the publicly available evidence, mechanisms for stakeholder consultation, and processes for parliamentary scrutiny of policy in digital trade are strengthened.**

Cross-border data flows, including privacy and protection of citizen's data

Key policy issues

18. Data underpins the digital economy, and the flow of data across borders is vital for integrated supply chains and cross-border provision of digital products and services, cloud computing applications, the Internet of Things and artificial intelligence. Yet enabling cross-border data flows also raises concerns.[10] The way in which personal data are handled and used can raise concerns regarding privacy and the security of information, illustrated by recent cases such as those involving Facebook and Cambridge Analytica, and frequent reports of data breaches.[11] These concerns have international dimensions as the global nature of the internet means that personal data can be quickly and easily transferred to parties in other jurisdictions. This transfer can undermine domestic privacy goals when the personal data of citizens flows to jurisdictions which do not offer comparable levels of privacy protection.

19. While restrictions and regulations on cross-border data flows can increase costs for businesses, there are many public policy reasons why governments regulate and restrict data flows, including to safeguard the fundamental rights of their citizens, public interests and values that matter for their constituencies. Governments may prevent data flows to jurisdictions with lower levels of regulatory protection. They may also require the localisation of data to ensure they can perform regulatory functions, including in the financial services sector. Balancing the policy objective of promoting cross-border data flows, with other policy objectives, including protecting personal data is challenging, and a contested area of trade policy. In practice governments have taken very different approaches ranging from allowing and promoting the free flow of data, as the US government does in its trade agreements, to implementing extensive data restrictions, which is the approach of the EU and the approach taken by the UK to date.

The UK's approach in the UK-Japan Agreement

20. In its negotiating objectives for the UK-Japan agreement, the Government stated that it would seek "Ambitious digital provisions, including supporting the free flow of data between Japan and the UK, can help us take the lead on innovation, supporting the development of important emerging technologies such as blockchain, driverless cars and quantum computing". In the same document the Government noted stakeholders' concerns on the importance of data protection and privacy standards

and states that it would "seek to facilitate the continued flow of data with the EU and international partners, whilst ensuring the UK's high standards of personal data protection".[12]

21. **In reconciling the objectives of promoting data flows and safeguarding privacy, the Government has taken a very different approach in the UK-Japan agreement to that taken by the EU. The Government has moved away from the EU-style provisions on cross-border data flows and privacy, to an approach based on that taken by the US and CPTPP countries.**

22. In the EU privacy and personal data of citizens and residents are protected as fundamental rights.[13] The General Data Protection Regulation (GDPR) is an extensive system of data regulation that *inter alia* makes it illegal to transfer data outside of the EU unless privacy is adequately protected in the data destination country. In practice this has meant a privacy regime that is equivalent to the EU, as has been confirmed in recent rulings by the Court of Justice of the European Union (Schrems I and II).[14]

23. Until recently, the EU was hesitant about making legally binding commitments on cross-border data flows in its trade agreements, fearing that this might undermine its ability to implement the GDPR. In the EU-Japan agreement for example, there are no provisions on cross-border data flows, and the Parties agreed to revisit this after three years (art. 8.81 EU-Japan). Separately, the EU evaluated Japan's regime for data protection, and issued an adequacy decision in 2019.[15]

24. The EU's position changed in 2018, when it finally agreed text to would propose in trade negotiations, after an intense institutional dialogue between different branches of the Commission and with the involvement of the European Parliament and Member States. The EU's recent proposals, which have been tabled in negotiations with the UK, have two core components: to prohibit specific types of restriction on cross-border data flows, rather than a broad commitment to allow cross-border flows; and to include an extensive, self-judging exception for privacy, which carves out privacy measures from the scope of the agreement. The aim of these provisions is to promote cross-border data flows while ensuring the EU unconditionally preserves its autonomy to regulate in the interest of data privacy, so that the GDPR is immune from challenge.[16]

25. UK-Japan agreement replaces the rendezvous clause of the EU-Japan agreement with provisions on cross-border data flows (art.8.84 UK-Japan), data localisation (art.8.85 UK-Japan), and protection of personal information (art.8.80 UK-Japan).[17] The approach taken in the UK-Japan agreement is based on approach taken in the CPTPP (to which Japan is a signatory) and the US in its recent trade agreements.

26. **The UK-Japan agreement includes a new general, binding commitment to 'not prohibit or restrict the cross-border transfer of information by electronic means' and treats privacy as one possible consideration under the 'legitimate public policy objective' exception** (art.8.84 UK-Japan). Notably, the Parties commit to only implement restrictions on cross-border data flows, including privacy restrictions, if the measure 'is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade' and 'does not impose restrictions on transfers of information greater than are required to achieve the objective', subject to limited exceptions (art.8.84 UK-Japan).[18] The Parties also agree to a prohibition on data localisation requirements, subject to similar exceptions (art.8.85 UK-Japan).

27. The UK-Japan agreement, like the CPTPP, does have a stand-alone article on personal data protection. **Unlike the EU proposals in recent trade agreements, which aim to fully carve out privacy measures, under the UK-Japan article the Parties make more general commitments and *inter alia* commit to 'adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce' (art.8.80 UK-Japan). This is a radically different approach from that of the EU.**

28. These shifts are important and raise questions about the UK's ability to maintain its current standards of privacy protection. **The EU not made types of commitments that the UK is making in the UK-Japan agreement on cross-border data flows and data localisation as the EU and privacy scholars argue that the GDPR is unlikely to meet such requirements**.[19] Indeed, the US has often argued that the GDPR is more restrictive than necessary for safeguarding privacy.

29. In departing from the EU's approach to cross-border data flows and privacy, the UK has a delicate balancing act to strike. The UK's Data Protection Act 2018 is based on the EU's GDPR, as is the UK's International Data Transfers Framework. Although the UK Prime Minister has indicated that data protection standards in the United Kingdom are likely to diverge after Brexit, the nature and magnitude of intended changes is unclear.[20] At the same time, the Government is seeking to secure an adequacy agreement with the European Commission under the GDPR before the end of the transition period.[21] Such an adequacy decision would recognise that British data protection standards were equivalent to those ensured by GDPR and would allow free flows of data from the EU to the UK after the end of the transition period.[22] Obtaining adequacy is extremely important for businesses and the Government has stated that it is also "extremely important" for effective UK-EU cooperation in law enforcement.[23]

30. **The Government has stated that its commitments in the UK-Japan agreement are commensurate with its aims of upholding high standards of privacy under the UK's Data Protection Act 2018**.[24] While Japan has obtained an adequacy agreement from the EU and made commitments in other trade agreements that are similar to those in the UK-Japan agreement, the interaction between the EU's adequacy decisions and commitments in trade agreements is complex and disputed. Privacy scholars have argued that a country that "commits to free cross-border data flows in a free trade agreement with yet other countries, it is risking its strategic ability to obtain a finding of adequacy by the Commission**".[25] So far, there is little publicly available analysis providing detailed and convincing evidence that substantiates the Government's argument.**

31. **Further evidence and analysis are needed on the implications of the new provisions in the UK-Japan agreement on cross-border data flows and localisation for personal data protection and obtaining an EU adequacy decision. In particular on: (1) whether the new commitments in the UK-Japan agreement are sufficiently robust to ensure the UK's existing standards for the protection of personal data are immune from challenge, appraising the risk that the UK's existing standards fail to meet the requirements specified in Articles 8.84 and 8.84 of the UK-Japan agreement; (2) detailed analysis of the implications of the commitments in the new Japan-UK agreement for the EU's adequacy decision; (3) a detailed explanation of the reasons why the Government has chosen not to provide more substantial carve-outs for privacy such as those proposed by the EU in its trade agreements, and how it intends to change UK data protection measures in future.**

Regulation of new technologies, including algorithm accountability

Key policy issues

32. The recent controversy involving the use of algorithms to predict GCSE and A-level grades in the UK placed the use of machine-learning and automated decision-making systems in the public spotlight.[26] The use of these systems is increasingly common in many areas of the economy and public life more generally, including in employment, policing and education. Despite the benefits of such systems, they give rise to relevant public policy concerns related to the risks of discrimination, including gender-based and racial-based, and lack of fairness and accountability. Experts have argued that, in order to protect individuals subject to automated decision-making, algorithms should be accountable and governments should implement a 'right of explanation', where the reasoning behind a decision is presented to individuals affected by it.[27] There can be many ways of explaining an algorithm, and views on what would be the correct way vary,[28] but some forms of transparency could potentially clash with trade secrets and copyright provisions in trade agreements.

The UK's approach in the UK-Japan Agreement

33. **In the UK-Japan agreement the Government has agreed to ban mandatory disclosure of source code, software and algorithm expressed in that software (art.8.73 UK-Japan).** The Government negotiating objectives clearly include the provision of "comprehensive protections for software, algorithms, and encryption technologies". **The stated goal is to protect innovators while the protection of individuals subjected to algorithmic decision-making is notably absent from the objectives.** Previous EU agreements, including the one with Japan, already included prohibitions on forced disclosure of source code and software, but the UK-Japan agreement innovated by expanding the scope of the protection to include "algorithms expressed in that source code". The wording in the UK-Japan provision on source code is, in fact, very similar to the analogue articles in the USMCA (art. 19.16) and the CPTPP (art. 14.17), which prohibit parties from requiring transfer of or access to source code, software or algorithm as a condition to access the market.

34. **While the scope of the UK-Japan provisions is similar to those in recent US agreements, the exceptions are more similar to the ones found in EU agreements and provide greater flexibility for government policy-making.** While the exceptions in the US agreements are restricted to regulatory bodies and judicial authorities requiring access for a specific procedure, the UK-Japan agreement, like the EU-Japan agreement, includes exceptions to allow access to source codes and algorithms not only by regulatory or judicial bodies, but also to protect national security, integrity of the financial system, and a series of public policy objectives listed in the general exceptions (art. 8.3 UK-Japan).

35. Including provisions on source code and algorithms in trade agreements poses challenges, particularly with regards to the crafting of exceptions. As technology landscape surrounding emerging technologies is constantly evolving. Governments have not yet started to impose strict liability requirements on AI developers that make them liable for improper use of their products.[29]

Governments and experts have yet to determine effective ways of regulating new technologies and it may be that access the underlying lines of code is not needed for effective regulation.[30].The challenge for trade negotiators is to craft the language on exceptions so that they are broad enough to accommodate the unknown nature of future regulations that aim to ensure the accountability and oversight over automated decision-making – especially *vis a vis* individuals' rights to explanation and reasonable inferences.

36. The UK Information Commissioner's Office has recently issued a guidance on AI and data protection to assist organisations in determining how they should navigate the complex trade-offs that the use of an AI system to make decisions may require.[31] While the far-reaching prohibition of disclosure of algorithms is problematic from the point of view of potential bias and unfairness in the decision-making that they govern, prohibition of the disclosure of source codes also has implications for the promotion of open source software. **The UK government has been a pioneer in creating open source software, and there is concern that trade provisions such as those included in the UK-Japan agreement could lead to challenging types of public procurement seen as preferring open source.**[32]

37. **More analysis and evidence are needed on the exceptions in the UK-Japan agreement to ensure they are sufficiently broad to ensure future regulatory measures on the accountability and oversight over automated decision-making are permitted, and to ensure that the provisions support the use of open source software.** A detailed discussion is needed with technology experts, consumers, and organisations advocating for individual rights. In considering provisions on algorithms, the Government might look to the recent Digital Economy Partnership Agreement (DEPA) between New Zealand, Singapore and Chile which went beyond the UK-Japan by also including no-binding commitments to adopt AI governance frameworks, considering explainability, transparency, fairness and human-centred values (art. 8.2 DEPA).

38. **The UK-Japan agreement includes a novel provision banning the Parties from requiring access to cryptography technology**, prohibiting the mandatory transfer or**. As cryptography is often a privacy-enhancing tool, this could be in the benefit of consumers.** The provision bans measures which require companies to transfer or provide access to any proprietary information relating to cryptography, including the disclosure of a private key or algorithm specification (art.8.86 UK-Japan). As cryptography is often a privacy-enhancing tool, this could be in the benefit of consumers, but it is unclear what the Government rational was in adopting this specific provision. A similar provision on cryptography was included in the recent Digital Economy Partnership Agreement between New Zealand, Singapore and Chile (art. 3.4 DEPA).

39. **In order to fully understand the implications of the new provisions in the UK-Japan agreement on source code, algorithms and cryptography, further evidence and analysis is needed, including on: (1) Whether the exceptions included in the source code, software and algorithm provision (art. 8.73.3 UK-Japan) are sufficiently broad to ensure individual rights to reasonable explanation and reasonable inferences and the ability of the Government to regulate new technologies; (2) whether the restrictions to source code and software disclosure might negatively affect the development of open source in the UK; (3) The reasons why the Government has chosen to include novel rules restricting access to encryption technologies in the UK-Japan agreement.**

Regulation of the internet, including online harms

Key policy issues

40. Internet platforms that host user-generated content such as Facebook, YouTube and Twitter are usually considered intermediaries and not publishers of such content. From a public policy perspective, there remains concerns on whether and how these companies should be legally responsible for online harms – including child pornography and hate speech – and rights violations caused by the content they host.

41. To address these issues, governments have developed intermediary liability rules. These rules typically have three main policy goals. The first is to protect internet users and prevent harms (ranging from copyright infringement to non-consensual pornography); the second is to promote fundamental rights such as free expression and information access; and the third is to protect businesses and encourage economic growth and technical innovation. Balancing these objectives has proven complicated. In the wake of growing citizen concerns about harmful online content and criticism that the rules do not strike the right balance, governments have been revisiting their domestic legislation on intermediary liability, including in the UK, US, and EU.

The UK's approach in the UK-Japan Agreement

42. **The UK-Japan agreement, like the EU-Japan agreement, does not include general rules governing the liability of intermediary service providers. However, the Government has taken a more proactive approach when it comes to intellectual property rights, introducing a specific intermediary liability regime for copyright infringement which was absent from the EU-Japan agreement.** In its negotiating objectives for the UK-Japan agreement, the Government has clearly stated that it would enhance enforcement of intellectual property rights in the digital environment to "reduce the scale of counterfeiting and pirating in relevant industries thereby helping to protect consumers".[33] This was reflected in the negotiated text, as the parties agreed to ensure that enforcement procedures "are available under its law so as to permit effective action against an act of infringement of intellectual property rights which takes place in the digital environment, including expeditious remedies to prevent infringement and remedies which constitute a deterrent to further infringements" (art.14.59.1 UK-Japan).

43. **The UK-Japan agreement also includes a new 'safe harbour' for intermediaries, under certain circumstances**. The Parties commit to "limit the liability of, or the remedies available against, online service providers for intellectual property rights infringement by the users of their online services or facilities" (art.14.59.2 UK-Japan). This safe harbour would only apply "where the online service providers take action to prevent access to the materials infringing intellectual property rights". **This language is distinctive from the liability exceptions identified in other EU agreements (e.g. CETA), as it requires platforms to take action against rights' infringements in order to benefit**

from the safe harbour. The UK-Japan agreement also stands out in terms of the procedures for enforcement of the liability rules, including new language requiring them not to create barriers to legitimate activity and to preserve fundamental principles such as "freedom of expression, fair process, and privacy".

44. Safe harbours for intermediaries in case of intellectual property infringement are not entirely new in EU agreements. The EU-Canada agreement (CETA) establishes binding commitments for parties to provide limitations or exceptions in their domestic law regarding the liability of service providers, when acting as intermediaries, for infringements of copyright on the internet (art.20.11 CETA). However, CETA is less prescriptive than the UK-Japan agreement in terms of the requirements and procedures, allowing parties to prescribe in domestic law the conditions for service providers to qualify for the copyright safe harbour. Domestically, the EU e-Commerce Directive adopts a safe harbour regime that apply to internet intermediaries in general, establishing that they should not be held liable for hosting content they do not have knowledge that is unlawful, or when they act quickly to remove or to disable access to the information once they are aware of the illegal nature of it.[34] Intellectual property infringements, in particular, are addressed in the EU Digital Single Market Copyright Directive, which requires content-sharing providers (including platforms such as YouTube or Facebook) to obtain prior authorisation from right holders (e.g. a license agreement) or, in the absence of such license, to make their 'best efforts' to ensure that authorised content is unavailable, and to remove specific unauthorised content from their websites upon receiving a notification from right holders.[35]

45. **In terms of procedures, by requiring that ISPs take action in order to qualify for the IP safe harbour, in the UK-Japan agreement the Government has taken an approach which is closer to that of the US and CPTPP countries.** Both the USMCA (art.20.88) and the CPTPP (art.18.82) provide safe harbours to internet service providers, offering them immunity to claims of copyright infringement if, among other requirements, they promptly remove or block access to infringing materials after copyright holders give appropriate notice. This so called 'notice-and-take-down' system mimics section 512 of the Digital Millennium Copyright Act (DMCA).[36]

46. **Notably, the UK-Japan agreement has not taken the approach of recent US agreements in including broader commitments that limit the liability of internet intermediaries.** Intermediary liability rules in US trade agreements go beyond provisions on intellectual property infringements and have included highly controversial binding commitments limiting intermediary liability more broadly. The USMCA was the first US agreement to include provisions explicitly modelled on the contentious section 230 of the US Communications Decency Act (CDA), which provides a blanket waiver liability of internet companies that host user-generated content for the behaviour of their users.[37] The USMCA was ratified and implemented whilst a heated debate regarding the efficacy of ISP liability safe harbours was unfolding domestically in the US, with calls to overhaul the regime under CDA s.230.[38] This led experts to argue that internet companies lobbied for the inclusion of this provision in the agreement to protect against domestic reforms.[39] While the UK has not committed to this type of provision in the UK-Japan agreement, this will be an important consideration in upcoming negotiations with the US.

47. **Experts largely disagree on the best way to approach intermediary liability.** Some argue that a blanket waiver, such as included in the USMCA, permits tech companies to get away with not

moderating harmful content sufficiently, allowing hate speech and other forms of harassment in their platforms.[40] Technology companies, in turn, argue that the current provision is crucial to ensuring competition and freedom of expression on the internet.[41] Some of these concerns are shared by scholars and civil society organisations, who see intermediary safe harbours as a cornerstone of free internet speech.[42]

48. **The enforcement procedures for the intermediary liability provision on intellectual property in the UK-Japan agreement deserve close analysis.** The agreement explicitly mentions that they are to be implemented in a manner that preserves fundamental principles such as freedom of expression, fair process and privacy probably speak to these concerns (art.14.59.3 UK-Japan), but **it is unclear whether it strikes the right balance between the interests of intellectual property rightsholders and those of consumers**. Experts have shared concerns in the past that providing incentives for platforms to remove content could make technology companies more likely to censor legitimate speech, with chilling effects for freedom of expression online.[43]

49. **The Government has expressed its commitment to ensure that consumers are covered by high standards in online consumer protection in the negotiating objectives for the UK-Japan agreement. So far it has only adopted rules regarding intermediary liability and not yet established rules governing the circumstances under which online platforms would be responsible for harms to individuals.** The absence of such provisions is prudent as a domestic Online Harms Bill is expected to be introduced in 2021 and there is currently no consensus on which liability model the Government should adopt.[44]

50. The UK-Japan agreement also includes a new binding provision on regulation of internet access and network neutrality. The principle of network neutrality requires broadband providers to provide equal and non-discriminatory treatment of internet traffic. The UK-Japan text requires Parties to adopt or maintain appropriate measures to ensure that consumers can access and use internet services and applications, "subject to reasonable, transparent and non-discriminatory network management" (art.8.78 UK-Japan). This provision was absent from the EU-Japan agreement, but is in line with recent proposals from both the UK and EU in the context of a UK-EU future agreement (e.g. art.18.12 of the UK proposal to the EU) and provides a more robust protection of network neutrality by limiting the situations under which network management would be allowed. This is likely to be a more contentious consideration in upcoming negotiations with the US which, in line with its domestic policy,[45] has adopted a less protective approach to network neutrality. Analogue provisions found in the CPTPP and recent US agreements (e.g. USMCA) make no binding commitments and mention 'reasonable network management' very broadly, without the further limits found in the UK-Japan agreement.

51. **Internet regulation provisions in the UK-Japan agreement represent a blend of approaches adopted by the US and the EU in previous agreements, and overall tend to be more protective of the interests of businesses than of the interests of individuals. Further evidence and analysis are needed, including on: (1) The reasons why the Government has chosen to provide intermediary liability rules only with regards to intellectual property infringements; (2) The possible implications of the requirement for internet companies to 'take action' to prevent access to materials infringing intellectual property rights (art.14.59 UK-Japan) on other fundamental**

rights; (3) The extent to which the liability regime adopted in the UK-Japan agreement has implications for the future Online Harms Bill.

Trade facilitation and consumer protection for online commercial transactions, including spam

Key policy issues

52. Paper-based documents have been used to support commercial transactions for centuries, whether in a national or a cross-border context. Moving these processes online poses challenges. In the digital environment, parties need to find ways to ensure the people signing documents are who they say they are, without necessarily seeing them in person; or, that the transaction document in question has not been tampered with, copied or otherwise changed. Parties also need to have confidence that their information will not be misappropriated or details copied.[46] Consumers in many countries are wary of engaging in online transactions, particularly when they are cross-border, out of concern that transactions and delivery are less secure, and remedies do not exist for when something goes wrong.

53. Governments have enacted a range of different domestic rules that aim to facilitate trade in the new digital environment and protect consumers. Approaches vary widely. In the area of consumer protection, some governments including the US rely on industry self-regulation and market supervision by consumer associations, while others regulate more explicitly, adopting laws and regulations that provide e-consumers with rights regarding the return and cancellation of goods and services, and relating to the protection of data privacy.[47] Divergent domestic rules make cross-border digital activities more complex and raise the cost of doing business in multiple markets,[48] and there are concerns of a 'race to the bottom' in terms of online consumer protection.

The UK's approach in the UK-Japan Agreement

54. Consumer protection is notably absence from the UK's negotiating objectives on digital trade for UK-Japan, which were simply to 'Secure cutting-edge provisions which maximise opportunities for digital trade across all sectors of the economy' and 'Promote a world leading eco-system for digital trade that supports businesses of all sizes across the UK'.[49] Although the Government does state in its analysis of the UK-Japan agreement that it 'takes the protection of personal data, the right to privacy and consumer protection extremely seriously'.[50]

55. **The UK-Japan agreement includes a stronger commitment on consumer protection than that found in the EU-Japan agreement, although the Government could arguably have gone further.** In the EU-Japan agreement, the Parties merely stated that they 'recognise the importance' of consumer protection measures and cooperation (art.8.78 EU-Japan). The UK-Japan agreement provision is modelled on provisions in the CPTPP and recent US agreements. The Parties commit to 'adopt or maintain consumer protection laws and regulations to proscribe fraudulent and deceptive commercial activities that cause harm or potential harm to consumers engaged in online commercial

activities' and 'shall promote cooperation between their respective competent authorities (art.8.79 UK-Japan). The Government could have gone further in update this provision to reflect more specific and extensive consumer protection commitments such as those found in DEPA (art.6.3 DEPA) and EU proposals in the context of UK-EU trade negotiations (art.DIGIT.13), which stipulate at length the nature of the consumer protection measures that the Parties shall implement.[51]

On spam, the UK-Japan agreement actually waters-down the article in the EU-Japan agreement, dropping the requirement that consumers have to opt-in to receive commercial electronic messages, although it maintains the requirement that commercial electronic messages should be clearly identifiable and to provide recourse against suppliers of unsolicited commercial electronic messages that do not comply. The EU-Japan agreement specified *inter alia* that 'Each Party shall adopt or maintain measures regarding unsolicited commercial electronic messages that: (a) require suppliers of unsolicited commercial electronic messages to facilitate the ability of recipients to prevent ongoing reception of those messages; *and* (b) require the prior consent, as specified according to its laws and regulations, of recipients to receive commercial electronic messages. (art. 8.79 EU-Japan, emphasis added). In the UK-Japan agreement the word "and" is replaced with the word "or", thereby dropping the requirement of prior consent (art. 8.81 UK-Japan). In so doing, the UK-Japan agreement adopts the approach found in the CPTPP and recent US agreements.

56. **In the area of facilitating digital trade, the UK has opted to follow the fairly minimalist approach found in the EU-Japan text.** The UK-Japan agreement contains an article on the conclusion of contracts by electronic means, which replicates the provision in the EU-Japan agreement, with Parties agreeing not to use measures that deny the legal effect, validity or enforceability of a contract, solely on the grounds that it is concluded by electronic means (art.8.76 UK-Japan). On electronic authentication and electronic signatures, the UK-Japan agreement largely replicates the EU-Japan article although it incorporates more specific and restrictive language regarding the exception for government regulations: performance standards may be imposed for 'a particular category of transactions' and 'shall be objective, transparent and non-discriminatory and shall relate only to the specific characteristics of the category of transactions concerned' (art.8.77 UK-Japan). This is in line with recent proposals from both the UK and EU in the context of UK-EU (e.g. art.18.8 UK proposals to EU) and appears uncontroversial.

57. **The UK-Japan text does not include specific commitments on paperless trading, cross-border logistics, expedited customs procedures and *di minimis* thresholds, electronic payments, or e-invoicing** which are starting to emerge in other recent agreements, notably DEPA, the recent agreement between New Zealand, Singapore, and Chile.[52] While this is understandable given the time constraints that the government was working under, this is an area that could be strengthened in future.

58. The UK-Japan agreement, like the UK-EU agreement, contains a prohibition on customs duties on electronic transmissions. The UK-Japan agreement is more specific as it specifies that the prohibition includes 'content transmitted digitally' and specifies that the prohibition 'does not apply to internal taxes, charges and other fees unless they are imposed in a manner inconsistent with the Agreement' (art. 8.72 UK-Japan). This reflects the UKs position at the WTO where it has declared itself a strong supporter of calls for the WTO moratorium on customs duties to be made permanent.[53] In this it is supported by the EU and US, although strongly opposed by some developing countries, including South Africa and India.[54]

59. There is a high level of publicly available information and analysis about the type of provisions agreed in the UK-Japan agreement on trade facilitation and consumer protection for online commercial transactions. For this reason, there is less need for additional research and analysis. **Overall, while the UK-Japan general provision on consumer protection is stronger than in the EU-Japan agreement, it could have been more extensive, and it is surprising that the Government has chosen to water-down provisions on spam. In future trade agreements the Government could look to include stronger provisions on consumer protection, and additional provisions on digital trade facilitation, particularly to address constraints faced by smaller businesses.**

---

[1] We are grateful to participants in a workshop at the Blavatnik School of Government on Nov 5th 2020 for discussion on UK digital trade policy. While we have worked hard to ensure the accuracy of our analysis and incorporate feedback, it is not exhaustive, and any errors and omissions remain our own.

[2] UK Government, Final Impact Assessment of the Agreement between the United Kingdom of Great Britain and Northern Ireland and Japan for a Comprehensive Economic Partnership, 2020; The UK–Japan Comprehensive Economic Partnership Benefits for the UK, 2020.

[3] Department for International Trade and E. Truss, *Liz Truss Launches Future Trade Strategy for UK Tech Industry*, 9 June 2020, GOV.UK, available at https://www.gov.uk/government/news/liz-truss-launches-future-trade-strategy-for-uk-tech-industry (last visited 26 October 2020]. *Ibid.*

[4] UK Government, *National Data Strategy: Policy Paper* (2020), available at https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy#data-2-5.

[5] UK Government, *UK and Japan Sign Historic Free Trade Agreement*, 22 October 2020, Press Release, available at https://www.gov.uk/government/news/uk-and-japan-sign-historic-free-trade-agreement.

[6] UK Government, *supra* note 2.

[7] See pages 8, 26 UK Government, *supra* note 2.

[8] UK Government, *Trade Advisory Groups: Membership* (2020), available at https://www.gov.uk/government/publications/trade-advisory-groups-tags/trade-advisory-groups-membership.

[9] Jones and Sands, 'Ripe for Reform: UK Scrutiny of International Trade Agreements', *The Global Economic Governance Programme Working Paper* (2020), available at https://www.geg.ox.ac.uk/publication/ripe-reform-uk-scrutiny-international-trade-agreements.

[10] See for instance concerns raised by the Open Rights Group J. Ruiz, *Leaked UK US Trade Talks Risk Future Flow of Data with the EU*, 11 December 2019, Open Rights Group, available at https://www.openrightsgroup.org/blog/leaked-uk-us-trade-talks-risk-future-flow-of-data-with-the-eu/.

[11] UNCTAD, *Digital Economy Report 2019. Value Creation and Capture: Implications for Developing Countries*, UNCTAD/DER/2019 (Overview) (2019), available at https://unctad.org/en/PublicationsLibrary/der2019_overview_en.pdf.

[12] UK Government, *UK-Japan Free Trade Agreement: The UK's Strategic Approach* (2020), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/885176/UK_Japan_trade_agreement_negotiations_approach.pdf.

[13] Charter of Fundamental Rights of the European Union (articles 7 and 8); TFEU (article 16); Europe Convention 108 (article 1); European Convention on Human Rights (article 8)

[14] *The Court of Justice Invalidates Decision 2016/1250 on the Adequacy of the Protection Provided by the EU-US Data Protection Shield*, Press Release No. 91/20 (2020), available at https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf. On Schrems II see Chander, 'Is Data Localization a Solution for Schrems II?', *SSRN Electronic Journal* (2020) , available at http://dx.doi.org/10.2139/ssrn.3662626.

[15] European Commission, *Commission Implementing Decision (EU) 2019/419* (2020), available at http://data.europa.eu/eli/dec_impl/2019/419/oj.

[16] Yakovleva and Irion, 'Pitching Trade against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade', 10 *International Data Privacy Law* (2020) 201.

[17] For example, the UK-Japan agreement article on privacy stipulates that each Party 'shall' publish information on the personal information protections it provides to users of electronic commerce whereas the CPTPP text read 'should'.

[18] Note that there are additional exceptions including for government procurement and government-held data (art.8.84 UK-Japan), and financial regulation (art.8.63 UK-Japan).

[19] Yakovleva and Irion, *supra* note 16.

[20] "The UK will in future develop separate and independent policies in areas such as (but not limited to) the points-based immigration system, competition and subsidy policy, the environment, social policy, procurement, and data protection, maintaining high standards as we do so", Prime Minister, Statement UIN HCWS86, 3 February 2020. Available at https://questions-statements.parliament.uk/written-statements/detail/2020-02-03/HCWS86 (7 October 2020).

[21] Minister John Whittingdale, HC Deb, 29 September 2020, cW. Available at https://questions-statements.parliament.uk/written-questions/detail/2020-09-24/95167 (7 October 2020).

[22] The UK has conferred adequacy on the EU on a transitional basis under the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019 No. 419) – see paragraphs 4 and 5 of Schedule 21 to the Data Protection Act 2018 as inserted by paragraph 102 of Schedule 2 to SI 2019 No. 419. This enables a free flow of data to continue from the UK to the EU after the end of the transition period. UK Government, The Data Protection, Privacy and Electronic Communications (Amendments Etc) (EU Exit) Regulations 2019, UK Statutory Instruments.

[23] Para 20 House of Commons, *The Need for Progress in the Negotiations* (2020), available at https://committees.parliament.uk/publications/1538/documents/14358/default/.

[24] UK Government, *supra* note 2.

[25] Yakovleva and Irion, *supra* note 16.

[26] Bedingfield, 'Everything That Went Wrong with the Botched A-Levels Algorithm', *WIRED* (2020) , available at https://www.wired.co.uk/article/alevel-exam-algorithm.

[27] The Alan Turing Institute, *A Right to Explanation*, available at https://www.turing.ac.uk/research/impact-stories/a-right-to-explanation.

[28] Science and Technology Committee, House of Commons, *Algorithms in Decision-Making*, Fourth Report of Session 2017-2019 (2018) 52, at 28. *Ibid.*

[29] H. Lee-Makiyama, *Briefing Note: AI & Trade Policy*, Tallinn Digital Summit (2018), available at https://ecipe.org/wp-content/uploads/2018/10/TDS2018-BriefingNote_AI_Trade_Policy.pdf.

[30] Wachter, Mittelstadt and Russell, 'Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR', 31 *Harvard Journal of Law and Technology* (2018) 841.

[31] *Algorithmic Decision-Making and the UK ICO's Guidance on AI | Data Protection Report*, available at https://www.dataprotectionreport.com/2020/09/algorithmic-decision-making-and-the-uk-icos-guidance-on-ai/ (last visited 29 October 2020].

[32] J. Ruiz, *US Red Lines for Digital Trade with the UK Cause Alarm*, 14 March 2019, Open Rights Group, available at https://www.openrightsgroup.org/blog/us-red-lines-for-digital-trade-with-the-uk-cause-alarm/ (last visited 29 October 2020].

[33] UK Government, *supra* note 12.

[34] This provision will be reformed by the Digital Services Act (DSA), which will be formally proposed in December 2020, which will make intermediaries liable for *illegal* content, but exempt them from liability for hosting *harmful content, hate speech and disinformation*. See A. A. Saliba, *Digital Services Act - Improving the Functioning of the Single Market*, IMCO Report 2020/2018 (INL) (2020), available at https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/IMCO/DV/2020/09-28/p.4_CAs_Saliba_DSA_EN.pdf.

[35] Curto, 'EU Directive on Copyright in the Digital Single Market and ISP Liability: What's Next at International Level?', 11 *Journal of Law, Technology and the Internet,* (2020) 84.

[36] The Digital Millennium Copyright Act (DMCA), adopted by the US in 1998, created a safe harbour for online service providers (OSPs), as long as they comply with certain requirements and block access to alleged infringing material upon receiving notification of an infringement claim from a copyright holder or their agent.

[37] The USMCA requires that "no Party shall adopt or maintain measures that treat a supplier or user of an interactive computer service as an information content provider in determining liability for harms related to information stored, processed, transmitted, distributed, or made available by the service, except to the extent the supplier or user has, in whole or in part, created, or developed the information" (art.19.17.2 USMCA). It also establishes that service providers will not be held liable "on account of any action voluntarily taken in good faith" to restrict access to or availability of material that the supplier or user considers to be harmful or objectionable; or "for any action taken to enable or make available the technical means that enable an information content provider or other persons to restrict access to material that it considers to be harmful or objectionable" (art.19.17.3 USMCA).

[38] In 2019, the Senate introduced a bill to prohibit large social media companies from moderating 'politically biased' information on their platform (Ending Support for Internet Censorship Act, S. 194, 116th Cong., 2019). The critique of s.230 also underlies the executive order issued by President Trump on "Preventing Online Censorship" from May 2020. In September 2020, the Department of Justice sent draft legislation to Congress to execute the presidential directive and to reform the DCA. See: US Congress, S.1914 - Ending Support for Internet Censorship Act, 2020-2019; US DoJ, Proposed Section 230 Legislation, 23 September 2020; US Government, Executive Order on Preventing Online Censorship, 28 May 2020.

[39] Madigan, 'NAFTA Shouldn't Include Outdated Internet Safe Harbors', *The Hill* (2018) , available at https://thehill.com/opinion/technology/370956-nafta-shouldnt-include-outdated-internet-safe-harborsN.
Turkewitz, *NAFTA: Preserving the Status Quo & Inviting a Future That We Are Incapable of Shaping*, 31 August 2018, Medium, available at https://medium.com/@nturkewitz_56674/nafta-preserving-the-status-quo-inviting-a-future-that-we-are-incapable-of-shaping-ff4c2ad0890e (last visited 1 November 2020].

[40] Former vice president and 2020 presumptive Democratic presidential nominee Joe Biden suggested that s.230

should be revoked. Kelly, 'Joe Biden Wants to Revoke Section 230', *The Verge* (2020) , available at https://www.theverge.com/2020/1/17/21070403/joe-biden-president-election-section-230-communications-decency-act-revoke (last visited 1 November 2020]. See also: Gillette, 'Section 230 Was Supposed to Make the Internet a Better Place. It Failed', *Bloomberg Businessweek* (2019) , available at https://www.bloomberg.com/news/features/2019-08-07/section-230-was-supposed-to-make-the-internet-a-better-place-it-failedWakabayashi, 'Legal Shield for Websites Rattles Under Onslaught of Hate Speech', *New York Times* (2019) , available at https://www.nytimes.com/2019/08/06/technology/section-230-hate-speech.html.

[41] CEO's from Facebook, Twitter and Google gave testimony to the US Senate on 28. Mark Zuckerberg, for example, argued that with the removal of the section, technology companies would be more likely to censor content in order to avoid being held responsible for hate speech and harassment. Twitter's Jack Dorsey said that changing the rule will make it more difficult for small platforms to survive, due to the high compliances costs associated with monitoring content, and that internet communication will be, as a result, controlled by a small number of large companies. Lima, 'Facebook Embraces Updating Tech's Legal Shield While Twitter, Google Urge Restraint', *Politico* (2020) , available at https://www.politico.com/news/2020/10/27/facebook-twitter-google-hearing-legal-shield-432903.

[42] EFF, *Section 230 of the Communications Decency Act*, Electronic Frontier Foundation, available at https://www.eff.org/issues/cda230. Letter from Scholars Regarding NAFTA and S.230, 21 January 2018.

[43] See Romero Moreno, ''Upload Filters' and Human Rights: Implementing Article 17 of the Directive on Copyright in the Digital Single Market', 34 *International Review of Law, Computers & Technology* (2020) 153Seng, 'The State of the Discordant Union: An Empirical Analysis of DMCA Takedown Notices', *SSRN Electronic Journal* (2014) , available at http://www.ssrn.com/abstract=2411915 (last visited 7 November 2020].

[44] J. Woodhouse, M. Lalic and S. Lipscombe, *Research Briefing: Online Harms*, 1 October 2020, House of Commons Library, available at https://commonslibrary.parliament.uk/research-briefings/cdp-2020-0093/.

[45] The US Federal Communications Commission (FCC) changed American ISPs rules in 2017, *de facto* repealing the network neutrality principle in the country. See Aaronson and Leblond, 'Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO', 21 *Journal of International Economic Law* (2018) 245.

[46] WEF, 'Making Deals in Cyberspace: What's the Problem?', *World Economic Forum* (2017) , available at http://www3.weforum.org/docs/WEF_White_Paper_Making_Deals_in_Cyberspace.pdf (last visited 1 November 2020].

[47] WEF, 'The Global Governance of Online Consumer Protection and E-Commerce', *World Economic Forum* (2019) , available at http://www3.weforum.org/docs/WEF_consumer_protection.pdf (last visited 1 November 2020].

[48] WEF, *supra* note 46.

[49] UK Government, *supra* note 12.

[50] UK Government, *supra* note 2.

[51] DEPA art 6.3 includes "Each Party shall adopt or maintain laws or regulations to proscribe fraudulent, misleading or deceptive conduct that causes harm, or is likely to cause harm, to consumers engaged in online commercial activities. Such laws or regulations may include general contract or negligence law and may be civil or criminal in nature. "Fraudulent, misleading or deceptive conduct" includes: (a) making misrepresentations or false claims as to material qualities, price, suitability for purpose, quantity or origin of goods or services; (b) advertising goods or services for supply without intention to supply; (c) failing to deliver products or provide services to consumers after the consumers have been charged; or (d) charging or debiting consumers' financial, telephone or other accounts without authorisation. Each Party shall adopt or maintain laws or regulations that:

(a) require, at the time of delivery, goods and services provided to be of acceptable and satisfactory quality, consistent with the supplier's claims regarding the quality of the goods and services; and (b) provide consumers with appropriate redress when they are not. Each Party shall make publicly available and easily accessible its consumer protection laws and regulations. The Parties recognise the importance of improving awareness of, and access to, policies and procedures related to consumer protection, including consumer redress mechanisms, including for consumers from one Party transacting with suppliers from another Party. The Parties shall promote, as appropriate and subject to the respective laws and regulations of each Party, cooperation on matters of mutual interest related to misleading and deceptive conduct, including in the enforcement of their consumer protection laws, with respect to online commercial activities. The Parties endeavour to explore the benefits of mechanisms, including alternative dispute resolution, to facilitate the resolution of claims relating to electronic commerce transactions.

[52] The DEPA text includes stronger commitments on paperless trading, with Parties committing to make all existing publicly available trade administration documents public in machine-readable electronic formats; with limited exceptions, to accept electronic versions of trade administration documents as the legal equivalent of paper documents; to establish or maintain a 'seamless, trusted, high-availability and secure interconnection' of their respective single windows to facilitate the exchange of data relating to trade administration documents; promotion systems for the exchange of electronic records used in commercial trading activities between the Parties' businesses (art.2.2 DEPA). The DEPA text also includes new commitments to share best practices on cross-border logistics (art.2.4 DEPA); to work together to promote the adoption of e-invoicing by businesses, and base any measures related to e-invoicing on international standards, guidelines or recommendations in order to support cross-border interoperability (art 2.5 DEPA); and implement expedited customs procedures for express shipments and provide for a *de minimis* shipment value or dutiable amount for which customs duties will not be collected (art 2.6 DEPA). There is a provision on electronic payments, with Parties committing to support the development of efficient, safe and secure cross border electronic payments by fostering the adoption and use of internationally accepted standards, promoting interoperability and the interlinking of payment infrastructures, and encouraging useful innovation and competition in the payments ecosystem (art.2.7 DEPA).

[53] UK Government, *WTO General Council: UK Statement on Work Programme on Electronic Commerce*, 13 October 2020, available at https://www.gov.uk/government/speeches/uk-statement-to-the-wto-general-council--6.

[54] Communication from India and South Africa - The E-Commerce Moratorium: Scope and Impact, 10 March 2020; *WTO Members Highlight Benefits and Drawbacks of E-Commerce Moratorium*, 23 July 2020, SDG Knowledge Hub, available at https://sdg.iisd.org/news/wto-members-highlight-benefits-and-drawbacks-of-e-commerce-moratorium/.