Emily Jones, Beatriz Kira and Danilo B. Garrido Alves (Blavatnik School of Government, University of Oxford) – Written Evidence (CPT0036)

Executive Summary

1. In this submission we examine the digital trade provisions of the CPTPP, focusing on the implications of acceding this treaty for the regulation of the UK's digital economy.

2. Digital trade is a strategic priority for the UK Government and now that it has left the EU, the UK faces important decisions about how to regulate the digital economy and what approach to take in its trade negotiations.

3. There is no consensus internationally on how best to regulate the digital economy – this is a rapidly evolving area of policy and governments pursue very different approaches. In acceding to the CPTPP the UK would be departing from the EU's approach to digital trade regulation and aligning itself with the approach taken by the US and several Asia-Pacific countries, an approach which is also reflected in the recent UK-Japan agreement. In general, the US approach places greater emphasis on regulating the digital economy in the interests of large technology companies, while the EU tries to strike a balance between promoting digital trade and safeguarding the digital rights of citizens.

4. Despite a significant shift in its approach to digital trade, the UK Government is yet to set out a digital trade strategy or provide any detailed assessment of the costs and benefits of its new approach or its accession to digital trade provisions in the CPTPP.

5. We examine the digital provisions in CPTPP in four policy areas: cross-border data flows, including privacy and protection of citizen's data; regulation of new technologies, including algorithm accountability; regulation of the internet, including online harms; trade facilitation and consumer protection for online commercial transactions. We explain the key provisions in the CPTPP, compare them with other recent trade agreements, and highlight the public policy implications.

6. As we explain, CPTPP provisions impose significant limits on the scope and nature of policy measures the UK Government will be able to use to regulate cross-border data flows, including to protect the personal data of UK citizens; to regulate new technologies including automated decision-

making; and to regulate online content hosted by internet platform companies.

7. Given the importance of the digital trade agenda and ramifications for businesses, workers, and citizens, we recommend that stakeholder consultation, and processes for parliamentary scrutiny are strengthened.

8. With regards to cross-border data flows, we recommend that the Government provides further evidence and analysis on whether the UK's existing regulations on personal data protection meet the requirements specified in Articles 14.11 and 14.13 of the CPTPP, and explaining why it has chosen not to negotiate more substantial carve-outs for personal data protection such as those proposed by the EU in its trade agreements. We recommend that the Government negotiates more robust exceptions for privacy measures in its upcoming trade negotiations, including CPTPP accession, to provide reassurance that the UK's existing high standards of personal data protection can be maintained.

9. With regards to the regulation of new technologies, including algorithm accountability, we recommend that the Government provides further evidence and analysis on: whether there is scope to negotiate carve-outs and exceptions that are sufficiently broad to ensure individual rights to reasonable explanation and reasonable inferences and the ability of the Government to regulate new technologies; whether the restrictions to source code of software disclosure might negatively affect the development of open source in the UK. We recommend that the UK Government negotiates for the inclusion of wider exceptions in the CPTPP to ensure that 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.

10. With regards to regulation of the internet, including online harms, we recommend that Government provides further evidence and analysis on: the possible implications of the CPTPP provisions on safe harbours and 'notice-and-takedown' mechanisms on other fundamental rights; the extent to which the domestic liability regime currently adopted in the UK would meet the requirements of article 18.82 or qualify for one the carve-outs detailed in Annex 18-E and 18-F.

11. With regards to regulatory provisions on consumer protection and trade facilitation for digital trade we note that the CPTPP provisions are minimalist in nature. While this is unlikely to be a priority for the CPTPP accession negotiations, we recommend that in future trade negotiations

the Government looks to include stronger provisions on consumer protection, and additional provisions on digital trade facilitation, particularly to address constraints faced by smaller businesses.

Introduction[1]

12. We are submitting evidence in our capacity as researchers at the Blavatnik School of Government, University of Oxford.

13. On 1st February 2021, the UK Government notified the CPTPP countries of its intention to accede to the agreement.[2] The economic gains from accession are expected to be minimal, as the UK already has trade agreements with seven of the eleven CPTPP states (Canada, Chile, Japan, Mexico, Peru, Singapore and Vietnam) and is negotiating trade agreements with two more (New Zealand and Australia).[3] The UK's interest in the CPTPP is arguably more political than economic, a mechanism for signalling that the UK is actively taking steps to diversify its trade relations away from the EU.

14. Crucially, and unlike the other trade negotiations that the UK is currently engaged in, the CPTPP is a settled treaty to which the UK will be acceding. As such, the UK will come under pressure to make significant market access concessions in order to 'join the club' and is unlikely to be able to secure changes to the main treaty text, although it may be able to secure specific exceptions. The Government's bargaining power will be limited: although several CPTPP member states have an interest in expanding CPTPP membership, the UK is not a major trading partner for most CPTPP member states (the average share of the UK in the exports of the CPTPP in 2019 was less than 2%).[4] Existing members are likely to be wary of giving the UK specific derogations as this would set an unfavourable precedent for future accessions.

15. In this submission we examine the digital trade provisions of the CPTPP, focusing on the implications of acceding TPP for the regulation of the UK's digital economy. We examine the provisions in CPTPP 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, compare the CPTPP provisions with other agreements that the UK is party to, and highlight public policy

implications of accession. We highlight issues where further evidence and explanation is warranted and make proposals for the negotiation of specific exceptions.

Importance of digital trade provisions in the CPTPP

16. Digital trade is a strategic priority for the UK Government.[5] The UK's digital sector is sizeable and growing rapidly. It accounted for an estimated 7.6% of the UK economy in 2019, and employed an estimated 1.7 million people in 2020, and is growing more quickly than most other sectors.[6] UK trade flows are increasingly digital: an estimated two-thirds of UK services exports and a half of UK services imports were digitally delivered in 2018.[7]

17. Now that it has left the EU, the UK faces important decisions about how to regulate the digital economy and what approach to take in its trade negotiations. There is no consensus internationally on how best to regulate the digital economy – this is a rapidly evolving area of policy and governments pursue very different approaches.

18. The US was the impetus behind the digital trade provisions in the CPTPP. The CPTPP originated from the TPP, a flagship US initiative under President Obama which - in his words – "allows America – and not countries like China – to write the rules of the road in the 21st century".[8] In the TPP (and subsequent CPTPP), governments committed not to impede the flow of data across borders, not to impose data localisation requirements, not to levy customs duties on digital trade, and not to require private companies to disclose source code, all subject to specific and limited exceptions. Similar provisions on digital trade were also negotiated in the USMCA and US-Japan Digital Trade Agreement under the Trump administration.[9]

19. The UK, by virtue of its membership of the EU, has historically taken a very different approach to digital trade, particularly in the area of data regulation. The EU has made few commitments on digital trade in its trade agreements as it has sought to preserve a high level of regulatory autonomy. Only the EU's most recent trade agreements (including with the UK) contain dedicated chapters on digital trade and even here the EU insists on the inclusive of extensive provisions that safeguard its 'right to regulate'.[10] Rather than turn to trade agreements the EU has relied foremost on leveraging its market power to ensure that other governments uphold the digital rights of EU citizens – the so-called 'Brussels effect.'[11]

20. There have been signals that the UK Government is looking to move away from the EU's approach to digital economy regulation and adopt a more liberalising stance. The government's new National Data Strategy includes a mission to "champion the international flow of data" and the UK Prime Minister has indicated that data protection standards in the United Kingdom are likely to diverge from the GDPR after Brexit.[12] The strongest evidence of a shift in approach is found in the recent UK-Japan Agreement, which includes a digital trade chapter that is based on the CPTPP. Together with the decision to accede to the CPTPP, the UK appears to be moving away from the EU's approach to digital trade and towards the approach taken by the US and several Asia-Pacific countries.[13]

21. The differences between the US and EU approaches are substantial. As a recent World Bank report explains, in the area of cross-border data flows, the US adopts an 'open transfers' model, defined by the general absence of government restrictions on cross-border transfers of personal data and reliance on voluntary private sector standards and practices. This minimises the regulatory burden on service providers at both ends of a data transfer, maximizing the freedom businesses can enjoy in their data partnerships as well as their own business models, but providing few safeguards to boost trust in such data transfers. The EU in contrast adopts a 'conditional transfers' model, setting out a series of mandatory regulatory safeguards that, once met, allow for the free flow of cross-border data. As such the EU seeks to strike a balance between imperatives to safeguard citizens' rights and the need to promote data transfers and facilitate business in the digital economy.[14]

22. **Despite a significant shift in its approach to digital trade, the UK Government is yet to set out a digital trade strategy or provide any detailed assessment of the costs and benefits of its new approach or its accession to digital trade provisions in the CPTPP**.

23. 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. However, the government's trade advisory group on telecoms and technology comprising only of business representatives.[15] 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 CPTPP accession.

24. 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 are strengthened.**

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

Key policy issues

25. 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.[16] The way in which personal data are handled and used raise concerns regarding privacy and the security of information, illustrated by recent cases involving Facebook and Cambridge Analytica, and frequent reports of data breaches.[17] The global nature of the internet means that personal data can be quickly and easily transferred to parties in other jurisdictions, which can undermine domestic privacy goals if data flows to jurisdictions which do not offer comparable levels of privacy protection. 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.

The UK's approach in the CPTPP

26. A key decision for the UK is whether, and to what the extent to stay aligned with the EU's approach to data regulation and personal data protection. In the EU, privacy and personal data of citizens and residents are protected as fundamental rights.[18] The EU has not made broad positive commitments in any of its trade agreements on cross-border data flows, out of concern that this would compromise its ability to implement its data protection regime, embodied in the GDPR. Instead, the EU makes much narrower commitments in its trade agreements, including prohibitions on the use of specific regulatory measures (including data localisation), and it insists on an extensive privacy exception. 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.[19]

27. The UK agreed to a very different approach in the UK-Japan agreement, where the Parties made a general binding commitment to allow cross-border data flows, and the CPTPP contains a very similar provision. The UK-Japan agreement includes a general, binding negative commitment to 'not prohibit or restrict' the cross-border transfer of information by electronic means (Art. 8.84 UK-Japan). The CPTPP words its equivalent provision as a positive obligation to 'allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person' (Art. 14.11 CPTPP).

28. Notably, in both the UK-Japan and CPTPP agreements 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, Art. 14.11 CPTPP).[20] The Parties also agree to a prohibition on data localisation requirements in both agreements, subject to similar exceptions (Art. 8.85 UK-Japan, Art. 14.15 CPTPP).

29. Both the UK-Japan agreement and the CPTPP text have stand-alone articles on personal data protection under which 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; Art. 14.8 CPTPP). Neither agreement stipulates minimum standards or principles for personal data protection, and the CPTPP explicitly states that this requirement can be met via "laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy" (footnote 6 to Article 14.8 CPTPP).

30. This is very different to the UK-EU agreement where the Parties do not make a positive general commitment to allow free-flow of data. Instead, they agree to prohibit a list of specific data flow measures including data localisation, which will be kept under review (art. DIGIT.6 TCA). The UK-EU agreement also includes an extensive exception for personal data protection measures. The UK-EU text 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 the law of the Party provides for instruments enabling transfers under conditions of general application for the protection of the data transferred" where "conditions of general application" refer to "conditions formulated in objective terms that apply horizontally to an unidentified number of economic operators and thus cover a range of situations and cases" (art. DIGIT.7 TCA).

31. In addition, the UK-EU agreement contains a stand-alone article on the 'right to regulate' whereby "The Parties reaffirm the right to regulate within their territories to achieve legitimate policy objectives, such as the protection of public health, social services, public education, safety, the environment including climate change, public morals, social or consumer protection, privacy and data protection, or the promotion and protection of cultural diversity" (art. DIGIT.3 TCA). There is no analogous article in the digital trade chapter of the UK-Japan or CPTPP.[21]

32. **Simply put, under the UK-EU has retained a high degree of autonomy over the types of policy measures it can introduce in order to regulate cross-border data flows. Under the UK-Japan and CPTPP, this regulatory autonomy is substantially curtailed. While this provides UK businesses, trading partners and foreign investors with greater regulatory certainty, these commitments limit the scope and nature of public policy measures that the UK Government will be able to use in future, including to protect the personal data of UK citizens**.

33. **The UK needs to be careful in departing from the EU's approach to cross-border data flows and personal data protection in its trade agreements as it is far from clear that the UK's existing data protection regulations (enacted under the UK Data Protection Act 2018 and modelled on the EU's GDPR) are commensurate with the type of commitments that the UK is making in the UK-Japan and CPTPP agreements.** The EU has avoided making similar commitments in its trade agreements out of concern that it may lead to its GDPR being successfully challenged.[22] Crucially, it is unclear that the UK's existing data protection regime would meet the requirement in the CPTPP of not imposing "restrictions on transfers of information greater than are required to achieve the objective' (Art. 14.11 CPTPP) especially when the same agreement explicitly recognises voluntary undertakings by

enterprises as a legitimate mechanism for upholding personal data protection (footnote 6 to Article 14.8 CPTPP).

34. The UK 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.[23] So far, there is little publicly available analysis providing detailed and convincing evidence that substantiates this argument.

35. **We recommend that the Government provides evidence and analysis on the implications of the CPTPP provisions on cross-border data flows and localisation for personal data protection.** In particular: (1) examining in detail whether the UK's existing regulations on personal data protection meet the requirements specified in Articles 14.11 and 14.13 of the CPTPP; (2) explaining why the Government has chosen not to negotiate more substantial carve-outs for personal data protection such as those proposed by the EU in its trade agreements.

36. **We recommend that the Government negotiates more robust exceptions for privacy measures in its upcoming trade negotiations, including CPTPP accession, to provide reassurance that the UK's existing high standards of personal data protection can be maintained.**

Regulation of new technologies, including algorithm accountability

Key policy issues

37. 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.[24] 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.[25]

There can be many ways of explaining an algorithm, and views on what would be the correct way vary,[26] but some forms of transparency could potentially clash with trade secrets and copyright provisions in trade agreements.

The UK's approach in the CPTPP

38. **In the CPTPP the Government would agree to prohibit mandatory disclosure of source code of software (Art. 14.17 CPTPP).** The CPTPP provision prohibits Parties from requiring the "transfer of, or access to, source code of software owned by a person of another Party" as a condition of doing business in their territory. The UK-Japan text includes a similar prohibition, but has innovated by expanding the scope of the protection to include "algorithms expressed in that source code" (Art. 8.73). **The stated goal these provisions is to protect innovators, but they are problematic for a number of reasons, in particular because the protection of individuals subjected to algorithmic decision-making is notably absent from the objectives.**

39. **The prohibition in the CPTPP provides little flexibility for government policy-making, and fewer exceptions than previous treaties agreed by the UK**. While provisions preventing the parties from requiring the transfer of source code of software have been found in previous EU agreements (eg EU-Japan and EU-Mexico), they also included wider exceptions. The exceptions included in the UK-Japan agreement are also wider than the ones in the CPTPP, and provide more flexibility for policymaking. The UK–Japan agreement includes exceptions to allow regulatory or judicial bodies to access source codes and algorithms, which can also be requested to protect national security, integrity of the financial system, and for a series of public policy objectives listed in the general exceptions (art. 8.3 UK–Japan). In contrast, the CPTPP exceptions are limited to commercially negotiated contracts, law enforcement, and judicial authorities. Rather than carving out exceptions for public policy objectives, the CPTPP merely introduced an 'appropriate balance' clause concerning copyright and related rights, as well as limitations and exceptions, "including those for the digital environment" (art. 18.66 CPTPP). This provision is consistent with fair use exceptions to copyright in the US and could allow for the use of copyright protected data to better train AI systems.[27]

40. Including provisions on source code 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.[28] 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.[29] 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. **The UK has negotiated the inclusion of wider exceptions for public policy objectives in the agreement with Japan, and could aim to include similar language in the accession letter to CPTPP.**

41. 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.[30] 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 CPTPP could lead to challenging types of public procurement seen as preferring open source.**[31]

42. **We recommend that the UK Government negotiates for the inclusion of wider exceptions in the CPTPP to ensure that 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 procedural obligations for Parties to adopt AI governance frameworks, considering explainability, transparency, fairness and human-centred values (art. 8.2 DEPA).

43. **In order to fully understand the implications of the new provisions in the CPTPP agreement on source code of software, we recommend that the Government provides further evidence and analysis on: (1) Whether there is scope to negotiate carve-outs and exceptions that 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 of software disclosure might negatively affect the development of open source in the UK.**

Regulation of the internet, including online harms

Key policy issues

44. 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 concerns remain on whether and how these companies should be held legally responsible for online harms – including child pornography and hate speech – and rights violations caused by the content they host.

45. 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 approach in the CPTPP

46. **The CPTPP does not include general rules governing the liability of intermediary service providers. However, it provides a very detailed framework of intermediary liability for copyright infringements.**

47. **The CPTPP (art.18.82) provides safe harbours to internet service providers, limiting their liability for 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 resembles section 512 of the US Digital Millennium Copyright Act (DMCA).[32] The Parties commit to ensuring that "that legal remedies are available for right holders to address such copyright infringement and shall establish or maintain appropriate safe harbours in respect of online services that are Internet Service Providers" (art.18.82.1 CPTPP). ISPs can qualify for safe harbours with respect to copyright infringements that "they do not control, initiate or direct, and that take place through systems or networks controlled or operated by them or in their behalf" (art.18.82.1(b) CPTPP). In addition, for ISPs that function as search engines, or that provide hosting or storage services, there is also the requirement that they "expeditiously remove or disable access" to infringing material upon obtaining knowledge of the copyright infringement, "such as through receiving a notice of alleged infringement from the right holder or a person authorised to act on its behalf" (art.18.82.3(a) CPTPP).

48. **The model proposed in the CPTPP goes beyond those provided in existing international copyright treaties and is reported to be an US-led effort to provide right holders internationally with a tool for cross-border online copyright enforcement**.[33] The CPTPP framework is inspired by existing domestic notice-and-take-down systems in the US and in other jurisdictions, but does not go as far as to include the detailed safe-harbour procedures found in the DMCA. Notably, the CPTPP's notice and takedown system "does not mandate that Member States adopt any ISP policies concerning repeat infringers, establish specific damages for ISPs non-compliance with the notice and takedown system, or require that ISPs register their notice and takedown system agents".[34]

49. **The CPTPP carves-out detailed exceptions for Parties that adopt and maintain a domestic system for intermediary liability that meet certain criteria**. The agreement provides two specific exemptions, based on Canada's and Chile's existing ISP safe harbour regimes. Annex 18-E provides details of conditions modelled on the Canadian Copyright Act (2012). According to this provision, in order to qualify for the exception, Parties would have to adopt domestic legislation requiring ISPs to establish a system for forwarding notices of alleged infringement of copyright. This type of ISP safe harbour has been commonly referred to as a 'notice-and-notice' system. Importantly, it differs from the 'notice-

and-takedown' mechanism whereby it requires Parties to adopt a system that merely 'induces' ISPs to remove content, as opposed to requiring them to do so. The domestic legislation is required to induce ISPs that act as search engines to remove results that link to copyright infringing material upon notification, and to induce hosting ISPs to remove or disable access to the content following a court decision establishing the violation of the right. Importantly, the regime established in the Annex 18-E also requires Parties to adopt a secondary liability regime for online copyright circumventing tools, that is the provision of services primarily for the purpose of enabling acts of copyright infringement (Annex 18-E, 1(b)). Any future TPP Member State wishing to benefit from the exception laid out in Annex 18-E would have to have adopted a notice and notice system pursuant to these detailed requirements, which at the moment apply only to Canada. A different carve-out is established in Annex 18-F, which exempts from the general liability regime Parties that adopt the expedited judicial-based safe-harbour model that was agreed in the US-Chile agreement (art. 17.23(e) US-Chile), allowing Chile to maintain its existing regime. In order to qualify for this exception, future TPP Member States would have to adopt domestic legislation establishing that an ISP should remove content following an injunctive takedown order. Under this model, any take down request should first be submitted to a domestic court that would evaluate the alleged infringement of the copyright before deciding on the removal of the content.

50. **Since the UK has left the European Union, there is uncertainty regarding the liability regime for online copyright infringement currently in place, and it is not clear whether or not this framework would be consistent with CPTPP safe harbour provisions, or any of the exceptions**. In the UK, action against websites providing access to copyright infringing material can be taken under the Copyright, Designs and Patents Act (CDPA). The CDPA establishes that website owners found by the courts to be infringing copyright can be fined and or imprisoned, under certain circumstances. In 2000, the EU adopted the eCommerce Directive, which introduced a notice-and-take-action safe harbour regime for intermediaries also in the UK. Under the eCommerce Directive, platforms would not be held liable for infringing content when they act quickly to remove or to disable access to the material once they are aware of its illegality. The EU has recently adopted a new liability regime specific for copyright infringement, through the Directive on Copyright in the Digital Single Market, approved in 2019. The new European legislation introduced a distinction between 'online content-sharing service providers' and other online service

providers, removing content-sharing providers (including platforms such as YouTube or Facebook) from the scope of the e-Commerce Directive safe harbours. This new regime was not adopted by the UK because of Brexit.

51. **Since the end of the transition period, the European eCommerce Directive also no longer applies to the UK, but the Government has declared its commitment to upholding the liability protections.** For the time being, for companies that host user-generated content on their online services, there will continue to be a 'notice and take down' regime whereby the platform must remove illegal content that they become aware of or risk incurring liability.[35] However, there is no clarity regarding the specific rules that will apply. In December 2020, the government's full response to the OHWP has proposed the introduction of a statutory duty of care for internet companies, requiring platforms to take action to prevent the proliferation of illegal content and activity online. Breaches of intellectual property rights, however, were explicitly removed from the scope of the new proposed regime.[36] It is unclear whether the UK has plans to introduce a new liability regime specifically for online infringement of copyright. **Unless the UK Government is able to negotiate a specific carve-out, before joining the CPTPP it will have to adopt either the general notice-and-take-down regime modelled on the US legislation, or one of the two alternative models provided in the Annex – following either Canadian or the Chilean models.**

52. **Notably, the CPTPP does not follow 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, and it is not

included in the CPTPP agreement, this will be an important consideration in upcoming negotiations with the US.

53. **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]

54. **The enforcement procedures for the intermediary liability provision on intellectual property in the CPTPP agreement deserve close analysis.** In particular, there are concerns related to whether they will be implemented in a manner that preserves fundamental principles such as freedom of expression, fair process and privacy, and 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] The interplay between the detailed obligations related to removal of copyright infringement material and UK proposals to regulate online content also deserve further scrutiny. In particular, whether the UK will need to approve a new domestic liability regime for online copyright infringement, in addition to the rules proposed under the Online Harms Bill, which will provide further details on a general liability model for online intermediaries.[44]

55. **The CPTPP does not include robust protections with regards to internet access and network neutrality.** The principle of network neutrality requires broadband providers to provide equal and non-discriminatory treatment of internet traffic. In the CPTPP, Parties recognise the benefits of consumers having the ability to "access and use services and applications of a consumer's choice available on the Internet, subject to reasonable network management"; "connect the end-user devices of a consumer's choice to the Internet, provided that such devices do not harm the network"; and "access information on the network management practices of a consumer's Internet access service supplier" (art. 14.10 CPTPP). This provision makes no binding commitments and mentions 'reasonable network management' very broadly, without the further limits found in other UK agreements, such as the UK-Japan. 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 wording provides a more robust protection of network neutrality by more clearly delimiting the situations under which network management would be allowed. In contrast, the CPTPP fails to provide details of or limits to the situations under which network management would be allowed. This is closer to the position adopted by the US which, in line with its domestic policy,[45] has committed to a less protective approach to network neutrality.

56. **Internet regulation provisions in the CPTPP overall tend to be more protective of the interests of businesses than of the interests of individuals. We recommend that the Government provides further evidence and analysis on: (1) The possible implications of the CPTPP provisions on safe harbours and 'notice-and-takedown' mechanisms on other fundamental rights; (2) The extent to which the domestic liability regime currently adopted in the UK would meet the requirements of article 18.82 or qualify for one the carve-outs detailed in Annex 18-E and 18-F.**

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

Key policy issues

57. Recent trade agreements, including the CPTPP, seek to support businesses and consumers in the shift to a digitalised trading environment. For centuries, paper-based documents have been used to support commercial transactions, 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.

58. 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, and there are concerns of a 'race to the bottom' in terms of online consumer protection.

The UK's approach in the CPTPP

59. **The CPTPP agreement acknowledges the importance of consumer protection, but does little to meaningfully enhance consumer protection in the digital economy.** In CPTPP, 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. 14.7 CPTPP). While trade agreements often provide stronger protections for businesses than workers and consumers, the provisions in CPTPP (and UK-Japan) are noticeably weaker than those in the recent UK-EU agreement and DEPA where the Parties enter into more specific and extensive consumer protection commitments (art.DIGIT.13 TCA, art.6.3 DEPA).[48]

60. On spam (unsolicited direct marketing communications), the CPTPP, UK-Japan, and EU-UK agreements contain weaker provisions than are found in recent EU agreements which require that governments commit to implement regulatory frameworks under which consumers have to consent (opt-in) in order to receive commercial electronic messages (e.g. art 8.79 EU-Japan). In contrast, the CPTPP text allows governments to take a variety of approaches to minimising unsolicited electronic messages and consumer consent is not a requirement (art. 14.14 CPTPP).

61. The CPTPP includes several provisions aimed at facilitating digital trade including on electronic authentication and electronic signatures (art. 14.6 CPTPP), paperless trading (art. 14.9 CPTPP). However, it does not include specific commitments on electronic contracts, cross-border logistics, expedited customs procedures and *di minimis* thresholds, electronic

payments, or e-invoicing which are starting to emerge in more recent trade agreements, notably DEPA, the recent agreement between New Zealand, Singapore, and Chile.

62. The CPTPP, like many recent EU and US agreements contains a prohibition on customs duties on electronic transmissions (art. 14.3 CPTPP). This reflects the UK's 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.[49] It is important to note that while the UK's position is supported by the EU and US, it is strongly opposed by some developing countries, including South Africa and India.[50]

63. In general, the CPTPP contains regulatory provisions on consumer protection and trade facilitation for digital trade that are minimalist in nature. This arguably reflects the fact that the CPTPP is now quite a dated agreement in a fast-changing regulatory environment. **In future trade negotiations 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.**

26 March 2021

---

[1] While 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] Department for International Trade (2021) 'Formal Request to Commence UK Accession Negotiations to CPTPP' *News Story* 1st February 2021 https://www.gov.uk/government/news/formal-request-to-commence-uk-accession-negotiations-to-cptpp

[3] Gasiorek, Micheal et al (2021) 'The Value of the CPTPP for the UK' *UKTPO blog* 3rd February 2021 https://blogs.sussex.ac.uk/uktpo/2021/02/03/the-value-of-the-cptpp-for-the-uk/

[4] Gasiorek, Micheal et al (2021) 'The Value of the CPTPP for the UK' *UKTPO blog* 3rd February 2021 https://blogs.sussex.ac.uk/uktpo/2021/02/03/the-value-of-the-cptpp-for-the-uk/

[5] 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.*

[6] UK Government, *DCMS Economic Estimates 2019 (Provisional): Gross Value Added*, 10 December 2020, Department for Digital, Culture, Media & Sports, available at https://www.gov.uk/government/publications/dcms-economic-estimates-2019-gross-value-added/dcms-economic-estimates-2019-provisional-gross-value-added (last visited

5 February 2021]; *DCMS Sector Economic Estimates: Employment Oct 2019 - Sep 2020*, 21 January 2021, Department for Digital, Culture, Media & Sports, available at https://www.gov.uk/government/statistics/dcms-sector-economic-estimates-employment-oct-2019-sep-2020 (last visited 5 February 2021).

[7] M. Lee et al., *Understanding and Measuring Cross-Border Digital Trade - Final Research Report* (2020) 93, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/885174/Understanding-and-measuring-cross-border-digital-trade.pdf.

[8] Office of the Press Secretary (2016) 'Statement by the President on the Signing of the Trans-Pacific Partnership' The White House, February 3rd 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/02/03/statement-president-signing-trans-pacific-partnership

[9] Streinz, Thomas. "Digital Megaregulation Uncontested? TPP's Model for the Global Digital Economy." Megaregulation Contested: Global Economic Ordering After TPP. : Oxford University Press, July 18, 2019. Oxford Scholarship Online

[10] Burri, 'Data Flows and Global Trade Law', *SSRN Electronic Journal* (2020) , available at https://ssrn.com/abstract=3634434.

[11] A. Bradford, *The Brussels Effect: How the European Union Rules the World* (2020).

[12] "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).

[13] E. Jones and B. Kira, The Digital Trade Provisions in the New UK-Japan Trade Agreement: Submission to the International Trade Committee, UK House of Commons, 7 November 2020.

[14] World Bank (2021) *World Development Report 2021: Data for Better Lives* World Bank https://www.worldbank.org/en/publication/wdr2021 pp238-243

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

[16] 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/.

[17] 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.

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

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

[20] Note that there are additional exceptions including for government procurement and government-held data, and financial regulation

[21] Note that in all three agreements there are separate general exceptions provisions which also apply

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

[23] 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), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/929059/final-impact-assessment-UK-Japan-comprehensive-economic-partnership.pdf.

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

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

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

[27] Meltzer, 'Governing Digital Trade', 18 *World Trade Review* (2019) S23.

[28] 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.

[29] 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.

[30] *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].

[31] 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].

[32] 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.

[33] Lucas S. Michels. The effectiveness of the Trans Pacific Partnership's internet service provider copyright safe harbour scheme, E.I.P.R. 2016, 38(7), 409-415

[34] *Ibid.* At 411.

[35] UK Government, *The ECommerce Directive and the UK*, 18 January 2021, GOV.UK, available at https://www.gov.uk/guidance/the-ecommerce-directive-and-the-uk (last visited 24 March 2021].

[36] *Ibid.*

[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-harbors; N. 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-failed; Wakabayashi, '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) 153; Seng, '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] 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.

[49] 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.

[50] 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/.