Submission to the International Trade Committee, UK House of Commons

Inquiry on Digital Trade and Data

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
Danilo B. Garrido Alves, Research Officer, Blavatnik School of Government, University of Oxford

February 12th 2021

Executive Summary

1. The internet and digital technologies are upending global trade. Industries and supply chains are being transformed, and the movement of data across borders is now central to the operation of the global economy. Provisions in trade agreements address many aspects of the digital economy from cross-border data flows, to the protection of citizens' personal data, and the regulation of the internet and new technologies like artificial intelligence and algorithmic decision-making.

2. The UK Government has identified digital trade as a priority in its Global Britain strategy and one of the main sources of economic growth to recover from the pandemic. It wants the UK to play a leading role in setting the international standards and regulations that govern the global digital economy. The regulation of digital trade is a fast-evolving and contentious issue, and the United States, European Union, and China have adopted different approaches. Now that the UK has left the EU, it will need to navigate across multiple and often conflicting digital realms.

3. The UK Government has yet to set out its strategy for digital trade and the implications of digital trade provisions in UK trade agreements are yet to be thoroughly evaluated in the Government's impact assessments. As this is a relatively new area of trade policy, there is a paucity of robust information and analysis in the public domain. 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. To ensure the UK's approach to digital trade strikes an optimal balance between competing interests, broader participation and informed public debate with businesses, civil society organisations and other stakeholders is needed. As digital trade policy has implications for a range of policy areas, policy also needs to be designed through close collaboration between government departments and agencies, and regulatory bodies.

4. In this submission we examine the opportunities and challenges the UK faces in digital trade from a public policy perspective. We (1) define digital trade; (2) reflect on the UK's approach to date on digital trade, including in the UK-Japan, UK-EU agreements, and objectives for upcoming negotiations including CPTPP; (3) highlight policy options and trade-offs in key digital trade policy areas: cross-border data flows; internet access and content regulation; intellectual property and innovation; electronic commerce (including trade facilitation and consumer protection); and taxation (customs duties on e-commerce at the WTO and digital

services taxes) (4) highlight key domestic and international laws relevant to the Government's approach to digital trade.

5. We recommend that the UK Government:

   i. **Develops a digital trade strategy** to guide its trade negotiations and wider trade policy, setting out its policy objectives and how it intends to achieve them. This would ensure coherence between domestic and international policies, and across its different trade negotiations, and provide clarity and predictability to businesses, workers and citizens.

   ii. **Widens the range of public policy objectives the Government considers in its to digital trade policies, including it its negotiating objectives and impact assessments**. While facilitating and promoting digital trade is important for the UK economy, attention also needs to be paid to the protection and promotion of citizens' digital rights (including personal data protection and accountability of digital technologies); consumer protection (including promotion of a secure and safe internet, and consumer redress for cross-border digital transactions); promotion of a competitive and innovative digital economy; fair and effective taxation of digital economy; and cybersecurity. Ex-ante and ex-post impact assessments of trade agreements should include a far more detailed analysis on digital trade.

   iii. **Creates a far more robust mechanism for consulting and deliberating on its digital trade strategy and digital trade provisions in specific trade negotiations.** Given the breadth of policy issues and nature of policy trade-offs that need to be considered, digital trade policy needs to draw on the expertise and perspectives of a wide range of stakeholders in the business community (including SMEs and businesses that use digital products and technologies), consumer groups, digital rights groups, trade unions, and independent experts. Existing consultation mechanisms should be reviewed and strengthened to ensure they are more representative of diverse stakeholder groups.

   iv. **Takes a whole-of-Government approach to digital trade policy fully involving key departments and regulatory agencies in development and execution of digital trade policy**. This should include Department for Digital, Culture, Media & Sport (DCMS), the Department for Business, Energy and Industrial Strategy (BEIS), the Foreign, Commonwealth and Development Office (FCDO), the Information Commissioners Office (ICO), and National Cyber Security Centre (NCSC).

   v. **On cross-border data flows, carefully assesses its options and consults with stakeholders and makes a clear decision on whether to stay aligned with the EU's GDPR.** If the UK does wish to stay aligned, then it would be prudent to **insist on more robust exceptions for privacy measures in its upcoming trade negotiations**, including CPTPP, to ensure that the UK's data protection measures including its own data adequacy instruments are not at risk of challenge.

   vi. **On intellectual property and innovation, conducts and makes publicly available detailed analysis on the implications of provisions regulating the disclosure of source code, software, algorithms and cryptography in trade agreements**. The UK Government should ensure its commitments in trade agreements are sufficiently robust to safeguard its ability to regulate new technologies (including the

ability to audit and hold algorithms accountable), and strike an appropriate balance between protecting the intellectual property of companies and promoting other relevant public policy objectives, including access to technology, market competition, and open-source software.

vii. **On internet regulation, ensures that commitments in international trade agreements on the liability of online platforms are fully aligned with domestic laws and policies, in particular when it comes to moderation of online content and online harms**. The UK should establish a robust domestic regime that considers the relevant trade-offs before signing up to any commitments in future trade agreements that could restrict regulatory options.

viii. **On electronic commerce and consumer protection**, **pioneers a far more robust approach to consumer protection, working with other countries including New Zealand, Canada, and Singapore.** Specific regulation on electronic commerce and consumer protection would foster digital trade by ensuring consumers can have legal certainty and ways to pursue redress, improving consumer trust in digital trade.

ix. **On digital services taxes**, **designs a digital services tax that is in line with the UK's international trade, investment, and taxation obligations**. An active diplomatic strategy is needed to defend the UK's use of digital services taxes in light of the recent USTR finding that the UK's current design discriminates against US companies.

Introduction

6. 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 recently completed a working paper that reviews digital trade from a public policy perspective, and we draw on that paper in this submission. The full paper can be found here: https://www.bsg.ox.ac.uk/research/publications/uk-and-digital-trade-which-way-forward.

7. Digitalisation is affecting trade in many different ways. Digital technologies, products and services have become core aspects of almost every economic sector.[i] The services sector is arguably most impacted, with a surge in digitally delivered services such as the streaming of movies, internet banking, and professional services like accounting. Digitalisation also impacts traditional supply-chains, including by making logistics more efficient, and firms increasingly communicate with suppliers and customers and raise funds online.[ii] As a result of digitalisation, trade in smaller, often lower value physical goods (parcels ordered online) are growing and new types of bundled goods and services are emerging (such as autonomous cars). The movement of data, or information, across borders underpins these processes of digitalisation.[iii]

8. In this fast-evolving environment, governments are facing new regulatory challenges. In the area of data flows, for instance, governments need to find ways to achieve public policy objectives such as privacy or security, and ensure cybersecurity, while maintaining the benefits of cross-border data flows which underpin the digital economy. In the area of intellectual property, governments are tasked with protecting the intellectual property of digital economy firms while also ensuring effective oversight and accountability of new technologies. The digital economy also raises questions about how the internet should be regulated in

order to protect internet users and prevent harms (ranging from hate speech to non-consensual pornography), promote fundamental rights such as free expression and information access, and encourage economic growth and technical innovation.

9. Governments have increasingly looked to trade agreements to negotiate common approaches to the regulation of the digital economy. This includes on-going negotiations at the World Trade Organisation (particularly the 'Joint Statement Initiative on e-commerce') and bilateral and regional free trade agreements. Negotiations in international standard-setting bodies are also important for the digital economy, including at the International Electrotechnical Commission (IEC), International Organization for Standardization (ISO), and International Telecommunication Union (ITU).

10. There is no consensus internationally on how best to regulate the digital economy, and governments pursue very different approaches. The US has championed the inclusion of digital trade chapters in trade agreements, alongside other countries including Singapore, Australia, and Japan. The focus of the US government has been to secure increased market access and intellectual property protection for its large technology companies, including by securing commitments from other governments that they will not impede cross border flows of data or require private companies to disclose source code or algorithms, except in a very narrow range of circumstances.

11. In contrast, the EU's policy priority has been to promote consumer and digital rights of its citizens, and this has been most pronounced in the area of data privacy. 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 'Brussels effect.'[iv] Although the EU has digital trade provisions in many of its trade agreements, the EU has, until recently, taken a minimalist approach, making few commitments and seeking to preserve a high level of regulatory autonomy. Only the most recent agreements have dedicated chapter on digital trade and even here the EU insists on the inclusive of extensive provisions that safeguard its 'right to regulate'.[v]

The UK's overall approach to digital trade

12. Digital trade is a strategic priority for the UK Government.[vi] 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.[vii] 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.[viii] **Although digital trade is a priority for the UK Government, the government is yet to set out a strategy.**

13. 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. Strategic rivalry between the US, China, and to some extent the EU, is generating concerns over the balkanisation of the digital economy, and poses challenges for other countries, including the UK, on how best to navigate between these different regulatory approaches.

14. At present the UK's strategic direction is unclear. While the UK has been aligned with the EU's approach, the recent UK-Japan Comprehensive Economic Partnership Agreement (hereafter UK-Japan) and the proposals it

has tabled in other negotiations signal that the UK is moving towards the approach taken by the United States and several Asia-Pacific countries in their recent trade agreements.[ix]

15. During 2021 the UK will be negotiating digital trade provisions as it negotiates in free trade agreements, including with Australia, New Zealand, Canada, and the United States; as it looks to accede to the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). Even with the recently agreed Trade and Cooperation Agreement (TCA) between the EU and the UK, there are still outstanding points related to digital trade to be agreed in the coming months. Importantly, the European Commission will decide whether to grant the UK an adequacy decision allowing the free flow of data from the EU to the UK to continue.[x]

16. In the context of CPTPP negotiations, it is important to note that this is a settled treaty to which the UK will be negotiating accession. The UK will have limited ability to shape the main text of the treaty or secure concessions from existing CPTPP members, at the same time the UK will be under pressure from existing members to make concessions. As the UK is already in negotiations with key CPTPP members, or has existing trade agreements with them, it is unclear that the CPTPP should be a strategic priority. Prior to embarking on formal negotiations to accede to the CPTPP it is important that a careful appraisal is made of the costs and benefits of accession, including in the area of digital trade.

17. **To ensure coherence across different trade agreements and with domestic policies, it is important that the Government sets out an overarching strategy for digital trade setting out its policy priorities and explaining how it will pursue them domestically and in the context of its trade negotiations.**

18. 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**. 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), the Department for Business, Energy and Industrial Strategy (BEIS), the Foreign, Commonwealth and Development Office (FCDO), the Information Commissioner's Office (ICO), and the National Cyber Security Centre (NCSC).

19. In all these areas there is room for improvement. To date, the quality and extent of publicly available evidence and analysis on digital trade has been limited, there is very little informed public debate, and government has yet to set out a detailed strategy for digital trade.[xi] Our own multi-stakeholder initiatives have signalled, for instance, that there is a greater degree of common ground across different interest groups, such as businesses and NGOs, especially regarding the key importance of GDPR for both privacy and trade.[xii]

20. The government has established a trade advisory group on telecoms and technology, but only businesses are represented, providing consumer groups, trade unions, and policy experts with limited opportunities for meaningful input.[xiii] Parliament has few scrutiny powers committees charged with scrutinising trade agreements, which have insufficient time to perform this role effectively.[xiv] This has severe implications for the public accountability of trade agreements. I**mproving the quality of information, consultation, and parliamentary scrutiny of digital trade would help to ensure high-quality decision-making and secure public confidence.**

21. To be effective, the UK's digital trade strategy must be integrated with other policy areas, including industrial, innovation and employment policies, competition policy, consumer protection policy, taxation policy, and environmental 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), the Department for Business, Energy and Industrial Strategy (BEIS), the Foreign, Commonwealth and Development Office (FCDO), the Information Commissioner's Office (ICO), the National Cyber Security Centre (NCSC).

22. To strengthen the UK's overall approach to digital trade we recommend that the Government:

    i. **Develops a digital trade strategy** to guide its trade negotiations and wider trade policy, setting out its policy objectives and how it intends to achieve them. This would ensure coherence between domestic and international policies, and across its different trade negotiations, and provide clarity and predictability to businesses, workers and citizens.

    ii. **Widens the range of public policy objectives the Government considers in its to digital trade policies, including it its negotiating objectives and impact assessments**. While facilitating and promoting digital trade is important for the UK economy, attention also needs to be paid to the protection and promotion of citizens' digital rights (including personal data protection and accountability of digital technologies); consumer protection (including promotion of a secure and safe internet, and consumer redress for cross-border digital transactions); promotion of a competitive and innovative digital economy; fair and effective taxation of digital economy; and cybersecurity. Ex-ante and ex-post impact assessments of trade agreements should include a far more detailed analysis on digital trade.

    iii. **Creates a far more robust mechanism for consulting and deliberating on its digital trade strategy and digital trade provisions in specific trade negotiations.** Given the breadth of policy issues and nature of policy trade-offs that need to be considered, digital trade policy needs to draw on the expertise and perspectives of a wide range of stakeholders in the business community (including SMEs and businesses that use digital products and technologies), consumer groups, digital rights groups, trade unions, and independent experts.

    iv. **Takes a whole-of-Government approach to digital trade policy fully involving key departments and regulatory agencies in development and execution of digital trade policy**. This should include the Department for Digital, Culture, Media & Sport (DCMS), the Department for Business, Energy and Industrial Strategy (BEIS), the Foreign, Commonwealth and Development Office (FCDO), the Information Commissioner's Office (ICO), and the National Cyber Security Centre (NCSC).

Cross-border data flows

23. The regulation of cross-border data flows is a contentious policy issue. Governments have taken very different approaches ranging from allowing and promoting the free flow of data to implementing extensive data restriction and localisation measures. Personal data have become a resource that drives much economic

activity online, and the way in which personal data are handled and used can raise concerns regarding privacy and the security of information. The global nature of the internet means that personal data can be quickly and easily transferred to parties in other jurisdictions, undermining domestic privacy goals when the personal data of citizens flows to jurisdictions which do not offer comparable levels of privacy protection.[xv] Governments may restrict the flow of data on the grounds that it is necessary for effective financial regulation or on national security grounds. The way in which personal data are handled and used can raise concerns regarding privacy and the security of information. The global nature of the internet means that personal data can be quickly and easily transferred to parties in other jurisdictions, undermining domestic privacy goals when the personal data of citizens flows to jurisdictions which do not offer comparable levels of privacy protection.[xvi] Many governments restrict cross-border data flows in order to protect personal data, as well as for a range of other reasons, ranging from financial regulation to national security.

24. The debate in the trade policy world is over the extent to which restrictions on data flows and data localisation requirements are necessary for pursuing legitimate public policy goals, or unnecessary barriers to trade.

25. The US is a strong advocate of cross-border data flows and in its trade negotiations it seeks positive commitments that governments will allow data flows, and to impose limits on the measures that governments can use to regulate data flows, including on the grounds of privacy. US trade agreements do recognise the need to protect personal information, but the provision are nowhere near as robust as those advocated by the EU.

26. The EU has taken a very different approach and has only recently begun to negotiate provisions on data flows in its trade agreements. In the EU, privacy and personal data of citizens and residents are protected as fundamental rights.[xvii] The EU has not made broad positive commitments that it will permit data to flow across borders out of concern that this would compromise its ability to implement the GDPR. Instead, it has agreed to prohibit the use of specific types of measures (including data localisation) and insisted on an extensive exception for privacy, which completely 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.[xviii]

27. A key decision for the UK is whether, and to what the extent to stay aligned with the EU's approach to data regulation. There have been signals that the UK is seeking to move away from the EU's approach 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.[xix]

28. The strongest sign that the government's approach is shifting is found in the UK-Japan free trade agreement, where the digital trade provisions are based on the CPTPP (to which Japan is a signatory) and which follow the general pattern of recent US agreements.[xx] In the UK-Japan agreement, the Parties make a general binding commitment to data flows and treats privacy as one possible consideration in the "legitimate objective" exception. While Parties commit to upholding personal data protections, the UK-Japan agreement does not set minimum standards. Notably, the UK commits in the UK-Japan agreement to maintain privacy standards which will meet the tests of not imposing restrictions on transfers of information that are "greater

than are required to achieve the objective" (art. 8.80 UK-Japan). The approach taken in the suggests that the UK is heading broadly in the direction of the US approach to regulating cross-border data flows and privacy.

29. In stark contrast, the UK-EU text follows the EU approach: the UK tabled proposals on data flows based on the CPTPP text and these were not accepted by the EU. In the UK-EU agreement, the Parties do not make a positive general commitment to allow free-flow of data. Instead, they agree to prohibitions on a list of specific data flow measures including data localisation, which will be kept under review (art. DIGIT.6 TCA). There is an extensive exception for personal data protection measures 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" (emphasis added) 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). **While less expansively drafted than the EU's initial proposals, provisions in the UK-EU agreement provide far greater regulatory autonomy than the UK-Japan agreement and CPTPP.**

30. The UK needs to be careful in departing from the EU's approach to cross-border data flows and privacy in its trade agreements for two reasons. First, it is far from clear that the GDPR (to which the UK currently adheres) would meet the necessity test stipulated in the UK-Japan agreement. While there are disagreements among experts, the available evidence certainly suggests that **the type of privacy exceptions found in the UK-Japan agreement, the CPTPP, and recent US agreements may not be sufficiently robust to safeguard the UK's own GDPR and adequacy arrangements.** Crucially, the EU has avoided making similar commitments in its trade agreements out of concern that it may lead to its GDPR being challenged.

31. Second, departing from the GDPR would place the UK's adequacy decision from the EU at risk. The EU is yet to confer adequacy on the UK. Instead, the recent EU-UK trade agreement provides a six-month window during which data can flow from the EU to the UK pending the outcome of the EU's adequacy decision, so long as the UK stays aligned with the EU GDPR.[xxi] To obtain adequacy, UK data protection standards must remain equivalent to those provided by the GDPR. Experts have also raised concerns about the type of commitments the UK has made in the UK-Japan agreement, arguing that if a country "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".[xxii] Indeed the European Data Protection Board (which leads on adequacy assessments for the EU) any agreement concluded between the UK and the US would have to be taken into account when assessing the level of protection of personal data in the UK, in particular to ensure continuity of protection in case of onward transfers.[xxiii]

32. Moving away from the GDPR and losing adequacy would be extremely costly for the UK. A recent study suggests that not obtaining EU adequacy would cost UK businesses between £1 billion and £1.6 billion in additional compliance costs.[xxiv] The government has also stated that it is also "extremely important" for effective UK-EU cooperation in law enforcement.[xxv]

33. It may be possible for the UK to move away from the GDPR and/or enter into commitments in trade agreements on free flow of data and still obtain an adequacy decision from the EU. Japan has done this

through a 'work-around', creating a two-tier data protection regime with different arrangements for personal data originating from the EU and from within Japan, including in the area of onward transfers.[xxvi] However the EU GDPR is widely regarded as the international gold standard for data protection and staying aligned is widely supported by UK businesses and wider stakeholders.[xxvii]

34. To strengthen the UK's overall approach on data flows and data localisation we recommend that the Government:

    i. **Carefully assesses its options and consults with stakeholders on data regulation and makes a clear decision on whether to stay aligned with the EU's GDPR. If the UK does wish to stay aligned, then it would be prudent to insist on more robust exceptions for privacy measures in its upcoming trade negotiations, including CPTPP, to ensure that the UK's data protection measures including its own data adequacy instruments are not at risk of challenge.**

Internet access and content regulation / Net neutrality

35. **Rules in trade agreements can have implications for the regulation of the internet access and online content, including rules on network neutrality and on the liability of internet platforms for online harms and illegal online content.** Countries have adopted different network neutrality rules domestically. In China, the government plays a leading role in the management of the internet traffic, and adopts filtering and throttling mechanisms that limit access to services and websites considered illegal by the Chinese Communist Party.[xxviii] In the US, the Federal Communications Commission (FCC) changed the rules on the classification of internet service providers in 2017, which *de facto* repealed the principle of network neutrality in the country.[xxix] Despite their importance to safeguard equal and non-discriminatory treatment of internet traffic, provisions in trade agreements have not so far established rules on network neutrality.

36. **Provisions in trade agreements that affect the regulation of internet content are likely to be more contentious.** 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, concerns remain as to whether and how these companies should be legally responsible for online harms (including child pornography and hate speech) and rights violations (including copyright infringement) caused by the content they host. To address these issues, governments have developed intermediary liability rules.

37. **Experts largely disagree on the best way to approach intermediary liability and on how to strike the delicate balance between the relevant public policy objectives at stake.** These rules typically have three main policy goals. The first is to protect internet users and prevent harms and criminal activity online; 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. There are legitimate concerns regarding the procedures required to enforce some regimes of intermediary liability, and the impact they could have on internet content moderation. Experts worry that some liability models would provide incentives for platforms to use filtering tools and adopt review procedures that are more likely to censor legitimate speech, with chilling effects for freedom of expression online and access to information.[xxx]

38. **Governments around the world are under pressure to clamp down on online harms and the online dissemination of illegal content and many countries – including in the UK, US, and EU – are currently revisiting their domestic legislation on intermediary liability**. In the UK, the government's full response to the Online Harms White Paper (OHWP) 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.[xxxi] In the US, section 230 of the US Communications Decency Act (CDA) limits the liability of internet companies that host user-generated contents, such as Facebook and Twitter, for the behaviour of their users. Adopted in 1996, CDA s. 230 is now highly contentious[xxxii] and there has been recent calls to overhaul its safe harbours.[xxxiii] The EU liability regime is currently under review and due to be replaced by the Digital Services Act (DSA), which will introduce a new set of rules for online intermediaries and platforms.[xxxiv] The new EU framework will require platforms that host user-generated content to implement a 'notice-and-action' mechanism, so that users can notify online intermediaries about potentially illegal online content or activities.[xxxv]

39. **Rules limiting the liability of internet companies have been included in recent trade agreements and need to be carefully drafted to ensure that they do not undermine proposals to regulate the moderation of online content, including the UK plans to address online harms.** The USMCA was the first US agreement to include provisions explicitly modelled on the contentious section CDA s.230 (art. 19.17.2 USMCA).[xxxvi] The agreement was ratified and implemented whilst a heated debate regarding the efficacy of the regime was unfolding domestically, as discussed above. This led experts to argue that internet companies lobbied for the inclusion of this provision in the agreement to protect against domestic reforms.[xxxvii] In contrast to the US, the EU has largely refrained from including liability provisions in trade agreements, and when it has, they are less prescriptive than the US provisions and restricted to copyright infringements. Consequently, the EU has largely preserved its regulatory autonomy with regards to conducting domestic reforms in the liability regime. The UK has so far not signed up to any trade agreements that include general rules governing the liability of intermediary service providers, but has taken a more proactive approach when it comes to intellectual property rights, with the introduction of a specific intermediary liability regime for copyright infringement in the UK-Japan agreement (Article 14.59 CEPA).

40. **In trade negotiations going forward, provisions on intermediary liability deserve close analysis.** The government will need to carefully consider any interaction between trade policy and domestic regulation of the internet, in particular when it comes to online harms policy. The UK will have to decide what is the right balance between the competing policy goals and establish a robust domestic regime before signing up to any commitments in future trade agreements that could restrict regulatory options.

41. To strengthen the UK's overall approach on net neutrality, internet access and content regulation we recommend that the Government:

    i. **Ensures that commitments in international trade agreements on the liability of online platforms are fully aligned with domestic laws and policies, in particular when it comes to moderation of online content and online harms. The UK should establish a robust domestic regime that considers the relevant trade-offs before signing up to any commitments in future trade agreements that could restrict regulatory options.**

Intellectual property and algorithm disclosure

42. Provisions and exceptions in trade agreements establishing protections for intellectual property can have relevant implications for regulations that aim to ensure accountability and oversight over emerging technologies such as artificial intelligence, and can have an impact on innovation, including on policies that support technology transfer and open-software.

43. **There is a pressing need for well-defined rights and safeguards to regulate the deployment of algorithmic decision-making tools.** Despite the many benefits of algorithms and automated decision-making 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.[xxxviii] One recent example was the controversy involving the use of algorithms to predict GCSE and A-level grades in the UK, that placed the use of machine-learning and automated decision-making systems in the public spotlight.[xxxix] AI ethics advocates argue that algorithms should be made visible enough to be inspected and understood, particularly when they lead to decisions that have questionable or negative consequences,[xl] such as a job application denial or a driverless vehicle accident.[xli] Experts have argued that, in order to protect individuals subject to automated decision-making, citizens should have a 'right of explanation', by which the reasoning behind a decision is presented to them.[xlii]

44. **In recent years, a number of bilateral and regional trade agreements have included intellectual property provisions that expand the scope of protections of trade secrets to explicitly cover software and algorithms** – which arguably would not be covered under the general WTO rules on trade secrets.[xliii] Recent agreements negotiated by the EU have included provisions banning forced disclosure of source code and software but have not gone as far as the language in US agreements to expressly include algorithms in the scope of provision. The US provides extensive intellectual property protections in its recent trade agreements, and the most extensive are found in the USMCA. It explicitly includes source code-related algorithms into the subject matter of IP protection, in addition to just software protection. The USMCA does not including balancing clauses that are found in other recent trade agreements. CPTPP text for instance 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, which 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.[xliv]

45. **So far, the UK approach with regards to disclosure of source code, software, and algorithms is located mid-way between that of the US and of the EU, negotiating relatively stringent intellectual property rules for digital technologies, but including wider exceptions that are more similar to the ones found in EU agreements and provide greater regulatory flexibility**. In the UK-Japan agreement the UK Government has agreed to ban mandatory disclosure of source code, software and algorithm expressed in that software (art. 8.73 UK-Japan), but included 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). The UK-Japan agreement also includes a novel provision banning the Parties from requiring access to cryptography technology. 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 UK Government rationale was in adopting this specific provision. More recently, the UK-EU Trade and Cooperation Agreement (TCA) includes binding commitments against the forced transfer of source code of software (art. DIGIT.12), but, in contrast to the UK-Japan agreement, it does not explicitly mention algorithms. As with previous EU agreements, this provision is subject to general exceptions, security exceptions, and prudential carve-out (Article DIGIT.4), and the ban does not apply to disclosure requests made by court or administrative tribunal nor by regulatory bodies.

46. **Depending on how provisions banning forced disclosure of algorithms are drafted, and the scope of their exceptions, they could potentially clash with existing proposals to improve algorithmic accountability**.[xlv] One the one hand, a flat-out ban on forced disclosure of source code, software and algorithm could make it harder to obtain explanations for automated decisions (including machine and deep learning) that affect individuals.[xlvi] On the other hand, full disclosure and 'opening of the black box' might undermine intellectual property rights and would not necessarily be required in order for automated systems to be accountable and to provide meaningful explanations to individuals.[xlvii] Striking the right balance between these two policy objectives is a difficult task, in particular in light of the fast-pacing nature of emerging technologies such as AI. As technology landscape surrounding AI is constantly evolving, a central issue is to figure out *a priori* what type of information will be needed to police algorithms.

47. **Prohibitions on disclosure of source code, software, and algorithms can also have important implications for access to technology, market competition, and open-source software.** These rules have gained particularly relevance in light of growing concerns with governments' domestic policies requiring the disclosure of trade secrets as a condition to operate in some industries – a common policy in China.[xlviii] While the stated goal of these rules is to promote innovation by protecting firms' IP, provisions seeking to prohibit source code disclosure without appropriate limitations and exceptions can in fact choke access to technology that is essential to innovation, especially in less industrialised countries.[xlix] As source code constitutes an integral component of digital technologies, provisions prohibiting their transfer can effectively prevent the transfer of technology altogether, a problem which is even more acute for developing countries.[l] Another concern is that closing access to source code and software can stifle competition and create incentives for concentration in software markets and industry, by locking buyers into proprietary software. Further, provisions aimed at maximising the protection of intellectual property could inhibit the use or promotion of free and open-sourced software (FOSS) domestically, a relevant public policy instrument which governments should not be too hasty to relinquish. In fact, the UK Government has been a pioneer in creating open-source software, and there is concern that trade agreement provisions could lead to challenging types of public procurement seen as preferring open source.[li]

48. To strengthen the UK's overall approach on intellectual property and algorithm disclosure we recommend that the Government:

    i. **Conducts and makes publicly available detailed analysis on the implications of provisions regulating the disclosure of source code, software, algorithms and cryptography in trade agreements**. The UK Government should ensure its commitments in trade agreements are sufficiently robust to safeguard its ability to regulate new technologies (including the ability to audit

and hold algorithms accountable), and strike an appropriate balance between protecting the intellectual property of companies and promoting other relevant public policy objectives, including access to technology, market competition, and open-source software.

Electronic commerce and consumer protection

49. The main question regarding consumer protection in digital trade is **how ambitious the UK wants to be in terms of the coverage of e-commerce provisions and strength of consumer protection provisions (including promotion of a secure and safe internet, and consumer redress for cross-border digital transactions)**. 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. Online consumer protection rules have the potential to regulate the 'pre-purchase' stage (including advertising, information requirements, unfair commercial practices, etc.), the 'purchase' stage (including unfair contract terms, online payment security, etc.) and the 'post-purchase' stage (including dispute resolution, redress requirements, etc.). While many countries have consumer protection laws for online transactions, regulatory approaches vary. Some governments 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.[lii]

50. **The UK has so far not been particularly ambitious, and has opted to simply follow the EU's fairly minimalist approach**. In the TCA, the UK proposed weaker language than the EU, and the final text largely reflects the EU proposals. The TCA stipulates in detail the nature of the consumer protection measures that the Parties will adopt. These include measures that "proscribe fraudulent and deceptive commercial practices"; "require suppliers of goods and services to act in good faith and abide by fair commercial practices, including through the prohibition of charging consumers for unsolicited goods and services"; "require suppliers of goods or services to provide consumers with clear and thorough information"; and "grant consumers access to redress for breaches of their rights, including a right to remedies if goods or services are paid for and are not delivered or provided as agreed" (art. DIGIT.13 TCA). The Parties also "recognise the importance of entrusting their consumer protection agencies or other relevant bodies with adequate enforcement powers" and the importance of cooperation between these agencies to protect consumers and enhance online consumer trust (art. DIGIT.13 TCA). These provisions are stronger than in the UK-Japan agreement, which simply replicated the minimalist approach of the EU-Japan agreement (art. 8.79 UK-Japan).

51. To strengthen the UK's overall approach on electronic commerce and consumer protection we recommend that the Government:

    i. **Pioneers a far more robust approach to consumer protection, working with other countries including New Zealand, Canada, and Singapore. Specific regulation on electronic commerce and consumer protection would foster digital trade by ensuring consumers can have legal certainty and ways to pursue redress, improving consumer trust in digital trade.** To ensure such provisions strike an optimal balance between competing interests, broader participation and informed public debate with civil society organisations, businesses and other stakeholders is highly recommended.

Digital Services Taxes (DSTs)

52. **Digital services taxes are an increasingly contentious topic that require more expert and policy considerations**. In the past few years, governments have started to introduce taxes on the provision of digital services, including Austria, Brazil, Czech Republic, France, India, Indonesia, Italy, Spain, Turkey, and the UK.[liii] The UK introduced a digital services tax in April 2020, a tax of 2% on revenues made by large platforms that service UK-based users. It applies to businesses which provide social media platform, search engine, or online marketplace services which have global revenues of more than £500m a year and UK revenues of more than £25m a year.[liv] The rationale for these taxes is that internet platforms should pay tax not only where they are located, but also where they make their profits (i.e. where their users reside).[lv]

53. **Digital services taxes are likely to be key in the context of trade negotiations with the US, with US senators warning that the UK's digital sales tax could derail trade negotiations**.[lvi] The US, which is home to many of the world's largest digital services companies, has strongly opposed the introduction of digital services taxes. In 2020, it launched an investigation into several countries' digital services taxes, including the UK's. In January 2021, the USTR reported that the UK's digital services tax was inconsistent with the principles of international taxation.[lvii] No tariffs or similar retaliations have been applied against the UK yet, however.

54. **Some experts argue that the UK digital services tax may contravene GATS obligations on non-discrimination**.[lviii] Specifically, the 'low profit' threshold for exemption might be incompatible with GATS national treatment obligations, as UK-based companies would have a more favourable treatment than foreign-based companies. Similarly, as the tax only applies to companies of a certain economic size, it could be *de facto* discriminatory if all or most of the companies subject to it were foreign-based,[lix] though it is still unclear whether that is indeed the case.

55. As the UK negotiates free trade agreements with other countries, and looks to accede to the CPTPP, care will need to be taken to ensure that the commitments it makes are compatible with the design of its digital services tax. The UK might consider including stronger tax exceptions. For instance, the general exception for tax measures in the UK-Japan agreement replicates the provision in the EU-Japan agreement, which is less extensive than the tax carve-outs in DEPA and CETA.

56. To strengthen the UK's overall approach on digital services taxes we recommend that the Government:

    i. **Designs its digital services taxes to ensure they are in line with the UK's international trade, investment, and taxation obligations. An active diplomatic strategy is needed to defend the UK's use of digital services taxes in light of the recent USTR finding that its current design discriminates against US companies.**

Limitations imposed by domestic and international law

57. **Several existing domestic and international law commitments limit what the UK Government might agree upon in matters of digital trade.** These include the UK's obligations under international trade law,

international tax law, international human rights law and international environmental law, as well the Data Protection Act 2018 and the UK's Digital Services Tax (DST). This is a non-exhaustive list, however, the main aspects of which will be flagged below.

58. **Even though existing multilateral trade rules were negotiated when digital trade was in its infancy, they nonetheless have implications for digital trade as they are technologically neutral.** This means that commitments made under the General Agreement on Trade in Services (GATS) and the General Agreement on Tariffs and Trade (GATT), including the prohibition of discriminatory treatment (most favoured nation obligations and national treatment obligations), apply regardless of the means through which the good or service is delivered, digital or otherwise. However, there is no consensus as to whether digital services that did not exist at the time of adoption of such instruments (such as cloud storage or music streaming) are covered by existing commitments.[lx]

59. **The WTO Moratorium on customs duties on electronic transmissions, as the name suggests, currently prohibits the application of customs duties on electronic transmissions as a matter of practice.** The WTO Moratorium was agreed in 1998 for a period of two years, so as to encourage the emerging digital aspect of global trade,[lxi] and has been renewed at every Ministerial Conference since.[lxii] However, the definition of the term 'electronic transmissions' has never been agreed and is disputed, so the scope of this obligation remains unclear.[lxiii] While there is general agreement that the WTO Moratorium applies to digitally delivered products and does not apply to domestic and internal taxes, there are major disagreements on coverage and on whether it should be made permanent. The UK has declared itself a strong supporter of the WTO Moratorium and is calling for it to be made permanent.[lxiv]

60. **The International Covenant on Civil and Political Rights (ICCPR, Art 17), the Convention on the Rights of the Child (CRC, Art 16), the Universal Declaration of Human Rights (UDHR, Art 12) and the European Convention on Human Rights (ECHR, Art 8) require that the UK Government respect, protect and fulfil the fundamental human right to privacy.** These international obligations are also applicable on the digital realm,[lxv] and could be breached by digital trade commitments to the extent that they imply undue limitations or flexibilizations regarding the privacy of UK citizens (for instance, by facilitating data flow to countries with low data protection standards). In this regard, the **UK Data Protection Act 2018 also establishes relevant practical obligations on how to respect, protect and fulfil UK citizens' right to privacy**, which must be taken into account when signing free trade agreements.

61. **The UK's international environmental and climate change law obligations should also be taken into consideration when negotiating or acceding to trade agreements.** More digital trade might imply more imports and exports of physical goods, which in turn rise carbon emissions. New developments promoted by digital trade, such as the mining of cryptocurrencies, are also extremely energy intensive, and usually takes place in countries like China,[lxvi] where non-renewable energy matrixes are still largely used. This is especially relevant as **the UK has committed, under its Paris Agreement Nationally Determined Contributions (NDCs), to 'reduce economy-wide greenhouse gas emissions by at least 68% by 2030, compared to 1990 levels'**.[lxvii] In order to comply with its international environmental obligations and its Paris Agreement emission reduction targets, the UK should consider how to offset the environmental impacts of the growth in trade (e.g. environmental tax). The inclusion of such provisions in trade agreements might be desirable to ensure environmental compliance in the context of digital trade.

[i] WTO, *World Trade Report 2020: Government Policies to Promote Innovation in the Digital Age* (2020) 208, available at https://www.wto.org/english/res_e/booksp_e/wtr20_e/wtr20_e.pdf (last visited 18 January 2021).
[ii] Mark Wu, 'Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System' (IDB and ICTSD 2017) RTA Exchange Overview Paper <https://e15initiative.org/wp-content/uploads/2015/09/RTA-Exchange-Digital-Trade-Mark-Wu-Final-2.pdf>.
[iii] Global Internet Protocol (IP) traffic, a proxy for data flows, grew from about 100 gigabytes (GB) per day in 1992 to more than 45,000 GB per second in 2017. And yet the world is only in the early days of the data-driven economy; by 2022 global IP traffic is projected to reach 150,700 GB per second, fuelled by more and more people coming online for the first time and by the expansion of the Internet of Things (IoT). See UNCTAD, 'Digital Economy Report 2019. Value Creation and Capture: Implications for Developing Countries' (United Nations Conference on Trade and Development 2019) UNCTAD/DER/2019 (Overview) <https://unctad.org/en/PublicationsLibrary/der2019_overview_en.pdf>.
[iv] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020).
[v] Mira Burri, 'Data Flows and Global Trade Law' [2020] SSRN Electronic Journal <https://ssrn.com/abstract=3634434>.
[vi] 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.*
[vii] UK Government, 'DCMS Economic Estimates 2019 (Provisional): Gross Value Added' (*Department for Digital, Culture, Media & Sports*, 10 December 2020) <https://www.gov.uk/government/publications/dcms-economic-estimates-2019-gross-value-added/dcms-economic-estimates-2019-provisional-gross-value-added> accessed 5 February 2021; UK Government, 'DCMS Sector Economic Estimates: Employment Oct 2019 - Sep 2020' (*Department for Digital, Culture, Media & Sports*, 21 January 2021) <https://www.gov.uk/government/statistics/dcms-sector-economic-estimates-employment-oct-2019-sep-2020> accessed 5 February 2021.
[viii] Michael Lee and others, 'Understanding and Measuring Cross-Border Digital Trade - Final Research Report' (Department for International Trade and the Department for Digital, Culture, Media and Sport 2020) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/885174/Understanding-and-measuring-cross-border-digital-trade.pdf>.
[ix] Emily Jones and Beatriz Kira, 'The Digital Trade Provisions in the New UK-Japan Trade Agreement: Submission to the International Trade Committee, UK House of Commons' <https://committees.parliament.uk/writtenevidence/14812/html/> accessed 19 January 2021.
[x] techUK, 'Data, Adequacy and the Future Relationship – an Explainer' (28 December 2020) <https://www.techuk.org/resource/data-adequacy-and-the-future-relationship-an-explainer.html> accessed 18 January 2021.
[xi] In the government's impact assessment and analysis of the UK-Japan agreement for instance, there was very little detail on digital trade. See pages 8, 26 UK Government, *The UK–Japan Comprehensive Economic Partnership Benefits for the UK* (2020), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/929065/UK-Japan-Trade-Agreement-sectoral-benefits.pdf.
[xii] Danilo B Garrido Alves, 'Developing the UK's Digital Trade Strategy: Insights from Our Digital Trade Workshop' (*Blavatnik School of Government*, 3 February 2021) <http://blogs.bsg.ox.ac.uk/2021/02/03/developing-uks-digital-trade-strategy-workshop-insights/> accessed 12 February 2021.
[xiii] UK Government, 'Trade Advisory Groups: Membership' (Department for International Trade 2020) <https://www.gov.uk/government/publications/trade-advisory-groups-tags/trade-advisory-groups-membership>.
[xiv] E. Jones and A. Sands, *Parliamentary Scrutiny of Trade Deals: How Does the UK Measure Up?*, 30 September 2020, UK Trade Policy Observatory, available at https://blogs.sussex.ac.uk/uktpo/2020/09/ (last visited 21 January 2021]*UK-Japan Comprehensive Economic Partnership Agreement: Second Report of Session 2019–21* (2020], available at https://publications.parliament.uk/pa/cm5801/cmselect/cmintrade/914/914.pdf (last visited 21 January 2021), page 5.
[xv] Aaditya Mattoo and Joshua P Meltzer, 'International Data Flows and Privacy: The Conflict and Its Resolution' (2019) 21 Journal of International Economic Law 769.
[xvi] ibid.
[xvii] 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).
[xviii] Svetlana Yakovleva and Kristina Irion, 'Pitching Trade against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade' (2020) 10 International Data Privacy Law 201.
[xix] "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).
[xx] *Japan-UK Comprehensive Economic Partnership Agreement*, Ministry of Foreign Affairs of Japan, available at https://www.mofa.go.jp/ecm/ie/page24e_000270.html (last visited 26 October 2020).
[xxi] Eleonor Duhs, 'EU-UK Data Flows, Adequacy and Regulatory Changes from 1 January 2021' (*Fieldfisher*, 24 December 2020) <https://www.fieldfisher.com/en/insights/an-adequate-agreement-what-the-brexit-deal-means-f> accessed 5 February 2021.
[xxii] Yakovleva and Irion (n 18).
[xxiii] European Data Protection Board, 'Letter Regarding the Agreement between the UK and the US on Access to Electronic Data for the

Purpose of Countering Serious Crime', (2020) , available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf.

[xxiv] New Economics Foundation, UCL European Institute, and UCUCL European Institute, 'The Cost of Data Inadequacy: The Economic Impacts of the UK Failing to Secure and EU Adequacy Decision' (2020) <https://www.ucl.ac.uk/european-institute/sites/european-institute/files/ucl_nef_data-inadequacy.pdf> accessed 5 February 2021.

[xxv] Para 20 House of Commons, 'The Need for Progress in the Negotiations' (Committee on the Future Relationship with the European Union 2020) <https://committees.parliament.uk/publications/1538/documents/14358/default/>.

[xxvi] Graham Greenleaf, 'Japan: EU Adequacy Discounted' (Social Science Research Network 2018) SSRN Scholarly Paper ID 3276016 <https://papers.ssrn.com/abstract=3276016>. Also see Flora Wang, 'Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement' (2020) 33 Harvard Journal of Law & Technology 31.

[xxvii] Garrido Alves (n 12).

[xxviii] Freedom House, *China's New Leaders Refine Internet Control* (2013), available at https://freedomhouse.org/report/special-report/2013/chinas-new-leaders-refine-internet-control (last visited 18 January 2021).

[xxix] See Susan Ariel Aaronson and Patrick Leblond, 'Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO' (2018) 21 Journal of International Economic Law 245.

[xxx] 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).

[xxxi] UK Government, 'Online Harms White Paper: Full Government Response to the Consultation' (Secretary of State for Digital, Culture, Media and Sport and by the Secretary of State for the Home Department by Command of Her Majesty 2020) <https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response>.

[xxxii] FT, 'New Realities Confront a Maturing Internet', *Financial Times* (2017) , available at https://www.ft.com/content/33e0372c-96f9-11e7-b83c-9588e51488a0 (last visited 1 November 2020).

[xxxiii] 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.

[xxxiv] European Commission, 'The Digital Services Act Package' (15 December 2020) <https://ec.europa.eu/digital-single-market/en/digital-services-act-package>.

[xxxv] European Commission, Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC 2020.

[xxxvi] 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).

[xxxvii] 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).

[xxxviii] Centre for Data Ethics and Innovation, 'Review into Bias in Algorithmic Decision-Making' (2020) <https://www.gov.uk/government/publications/cdei-publishes-review-into-bias-in-algorithmic-decision-making>.

[xxxix] Will Bedingfield, 'Everything That Went Wrong with the Botched A-Levels Algorithm' *WIRED* (19 August 2020) <https://www.wired.co.uk/article/alevel-exam-algorithm>.

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

[xli] ITUC, 'E-Commerce Free Trade Agreements, Digital Chapters and the Impact on Labour' (International Trade Union Confederation 2019) <https://www.ituc-csi.org/IMG/pdf/digital_chapters_and_the_impact_on_labour_en.pdf>.

[xlii] The Alan Turing Institute, 'A Right to Explanation' <https://www.turing.ac.uk/research/impact-stories/a-right-to-explanation>.

[xliii] Hosuk Lee-Makiyama, 'Briefing Note: AI & Trade Policy' (2018) Tallinn Digital Summit <https://ecipe.org/wp-content/uploads/2018/10/TDS2018-BriefingNote_AI_Trade_Policy.pdf>.

[xliv] Joshua P Meltzer, 'Governing Digital Trade' (2019) 18 World Trade Review S23.

[xlv] Science and Technology Committee, House of Commons, 'Algorithms in Decision-Making' (2018) Fourth Report of Session 2017-2019 28; Wachter, Mittelstadt and Russell (n 40); Brent Mittelstadt, Chris Russell and Sandra Wachter, 'Explaining Explanations in AI', *Proceedings of the Conference on Fairness, Accountability, and Transparency* (ACM 2019)

<https://dl.acm.org/doi/10.1145/3287560.3287574> accessed 18 January 2021. Science and Technology Committee, House of Commons 28.

[xlvi] During the negotiation of the TPP, there were concerns that the provision banning governments from requiring access to source code would restrict US regulators' access to information necessary to audit firms, limiting their ability to evaluate deceitful practices as well as security flaws in several industries, including auto manufacturers. Klint Finley, 'Trade Pact Could Bar Governments From Auditing Source Code' [2015] *Wired* <https://www.wired.com/2015/11/trade-pact-could-bar-governments-from-auditing-source-code/> accessed 3 February 2021.

[xlvii] Wachter, Mittelstadt and Russell (n 40).

[xlviii] Theodore Moran, 'Should US Tech Companies Share Their "Source Code" with China?' (*PIIE*, 28 October 2015) <https://www.piie.com/blogs/china-economic-watch/should-us-tech-companies-share-their-source-code-china> accessed 3 February 2021.

[xlix] WTO (n 1).

[l] *ibid.*

[li] Javier Ruiz, 'US Red Lines for Digital Trade with the UK Cause Alarm' (*Open Rights Group*, 14 March 2019) <https://www.openrightsgroup.org/blog/us-red-lines-for-digital-trade-with-the-uk-cause-alarm/> accessed 29 October 2020.

[lii] WEF, 'The Global Governance of Online Consumer Protection and E-Commerce' [2019] World Economic Forum <http://www3.weforum.org/docs/WEF_consumer_protection.pdf> accessed 1 November 2020.

[liii] USTR, 'Initiation of Section 301 Investigations of Digital Services Taxes' <https://ustr.gov/sites/default/files/assets/frn/FRN.pdf> accessed 1 November 2020.

[liv] Antony Seely, 'Research Briefing: Digital Services Tax' (House of Commons Library 2020) <https://commonslibrary.parliament.uk/research-briefings/cbp-8719/>. Note that the UK has said that it will disapply the tax if an appropriate global solution is agreed.

[lv] Gary Clyde Hufbauer and Zhiyao Lu, 'Policy Brief 19-14 Global E-Commerce Talks Stumble on Data Issues, Privacy, and More' (Peterson Institute for International Economics 2019).

[lvi] Aime Williams, 'US Senators Warn UK Digital Services Tax Could Derail Trade Talks' *FT* (23 July 2020) <https://www.ft.com/content/a20bf740-c310-4a90-9dd8-81369cfb1bdc>.

[lvii] USTR, 'Section 301 Investigation: Report on the United Kingdom's Digital Services Tax' <https://ustr.gov/sites/default/files/files/Press/Releases/UKDSTSection301Report.pdf> accessed 18 January 2021.

[lviii] 'Is the DST Compatible with the UK's International Obligations?' (*Hogan Lovells*, 11 November 2019) <https://www.hoganlovells.com/en/publications/is-the-dst-compatible-with-the-uks-international-obligations> accessed 1 November 2020.

[lix] Chris Noonan and Victoria Plekhanova, 'Taxation of Digital Services Under Trade Agreements' (2020) 23 Journal of International Economic Law 1015.

[lx] ibid.

[lxi] Declaration on Global Electronic Commerce, WT/MIN(98)/DEC/2, adopted 20 May 1998.

[lxii] World Trade Organization, Work Programme on Electronic Commerce, General Council Decision of 10 December 2019, WTO Doc. WT/L/1079 (2019)

[lxiii] See discussion on 8-10 of OECD, 'Electronic Transmissions and International Trade – Shedding New Light on the Moratorium Debate' <https://one.oecd.org/document/TAD/TC/WP(2019)19/FINAL/en/pdf> accessed 1 November 2020.

[lxiv] UK Government, 'WTO General Council: UK Statement on Work Programme on Electronic Commerce' (13 October 2020) <https://www.gov.uk/government/speeches/uk-statement-to-the-wto-general-council--6>.

[lxv] United Nations Human Rights Council, 'The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights' <https://undocs.org/pdf?symbol=en/A/HRC/39/29> accessed 10 February 2021.

[lxvi] Samuel Shen and Alun John, 'Global Chip Shortage Hits China's Bitcoin Mining Sector' *Reuters* (22 January 2021) <https://www.reuters.com/article/us-crypto-currency-china-mining-idUSKBN29R1AY> accessed 10 February 2021.

[lxvii] UK Government, 'United Kingdom of Great Britain and Northern Ireland's Nationally Determined Contribution' <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/943618/uk-2030-ndc.pdf> accessed 10 February 2021.