Written evidence - Centre for Inclusive Trade Policy (CITP) and UK Trade Policy Observatory (UKTPO)[1]

Key points

- The UK government's stakeholder engagement with regard to digital trade governance lacks the involvement and inclusion of non-business stakeholders. Our recommendation is that the UK government promotes inclusive data and digital trade governance, from its policy-making process to the implementation process of its international agreements.
- In terms of substance, we observe that high-standard digital trade chapters under its FTAs and a digital economy agreement reflect business needs well. But the UK government has insufficiently taken into account non-business stakeholders' interests and concerns.
- For future negotiations, we recommend the UK government focuses more on promoting a sustainable and trustworthy digital trade environment rather than using the CPTPP's market driven approach as a template.
- The key policy area which the UK needs to revisit is with regard to the public policy space. We recommend the UK government aims to lead the debate on public policy space and inclusive digital trade governance. While the UK's continuous proactive role at the WTO is important, more efforts on promoting discussions regarding public policy space need to be made outside trade negotiation forums. Such discussions need to involve wide stakeholders.
- In the UK's future digital trade agreements, we recommend the inclusion of an independent public policy objective clause to affirm the UK's digital governance principle and an independent right to regulate clause to improve predictability.
- The UK government could also establish a clear and consistent UK approach which balances free dataflows and data privacy by examining the approach taken under the UK-EU TCA and the EU-Japan protocol on free data flows and data privacy in its future agreements.
- We do not recommend maintaining the strong prohibitions on disclosure of source code as these impose limitations on governments' regulatory power. We propose a more balanced model such as under the UK-Japan CEPA. We recommend promoting the engagement of technological experts, as technologies are rapidly evolving.

[1] The evidence was written by Dr. Minako Morita-Jaeger, Javier Ruiz, Dr. Phoebe Li and Prof. Maria Savona.

Q: How successful has the UK Government been in supporting digital trade in its international agreements to date?

a. **What more do you think it could do on bilateral, plurilateral, or multilateral levels?**

The UK government has been proactively using Free Trade Agreements (i.e. UK-Japan CEPA (hereafter UK-Japan), UK-NZ FTA (hereafter UK-NZ), UK-Australia FTA (hereafter UK-Australia) and the CPTPP) and the UK-Singapore Digital Economy Agreement (hereafter UK-Singapore) to promote digital trade since the UK left the EU. Among these, the UK-Singapore is a frontrunner digital agreement. Such agreements, which focus on free data flows and technological innovation and development, are expected to support UK business by improving predictability and legal certainty. However, there is an issue: the voices of non-business stakeholders are not reflected in these agreements.

The UK can be seen as one of the world leading countries of data governance, according to the Data Governance Mapping Project.[2] Recognising its achievement to date, we recommend that the UK government **promotes a sustainable and trustworthy data and digital trade environment using its digital trade agreements.** Creating such a policy requires **multi-stakeholder engagement which involves not only business stakeholders, but non-business stakeholders including consumers, civil society organisations, academia and individuals. These issues are explored more fully in the remainder of this submission.**

Bilateral and plurilateral levels

Free Trade Agreements (FTAs) are one of the preferred routes for addressing the demands of the data economy and for preventing digital protectionism. But the downside is that they can create trust deficits (e.g. lack of transparency, lack of stakeholder engagement, the prioritizing of private sector's interests at the expense of public interest).[3]

After leaving the EU, the UK government shifted its digital trade policy from the EU's human-rights centric approach towards the Asia-Pacific (or US) market-led approach in its digital trade agreements. The digital trade agreements with Japan, Australia, NZ and Singapore basically used the CPTPP as a template. It should be noted that the CPTPP's e-commerce chapter (originally Trans-Pacific Partnership) was heavily influenced by US Big-tech which preferred a more regulatory-free and laissez-faire approach.[4]

[2] See p8 , Report of the Global Governance Mapping Project Year4.

[3] For example, see Aaronson, S.A. (2023) 'Building Trust in Digital Trade Will Require a Rethink of Trade Policy-Making', *Oxford Review of Economic Policy* 39(1), 98–109. Burri, M. (2023) 'Cross-border Data Flows and Privacy in Global Trade Law: Has Trade Trumped Data Protection?', *Oxford Review of Economic Policy* 39(1), 85–97.

This raises the question whether future digital trade agreements should be based on the CPTP approach. **We recommend the UK government focuses more on enhancing the "trust" aspect in digital trade agreements rather than using the CPTPP text as a template.**

In this context, it is very useful for the public to learn how the existing digital trade agreements help promote digital trade and make legal and societal impacts. We recommend the UK government conducts societal impact assessments in addition to economic impact assessments.[5] These impact assessments should be systemically established and widely shared with the public for "trust" building.

To date, the implementation of existing agreements lacks transparency. We recommend that the UK government, together with its FTA partner countries, **improve transparency in implementing the existing agreements**. For example, inviting multi-stakeholders to the existing digital trade committee of each trade/digital agreement and publishing reports regarding implementation will help improve transparency.

Multilateral level

Although bilateral and plurilateral agreements can address regulatory fragmentations between the signatories of the agreement, they can create a "digital noodle bowl" of different rules at the multilateral level - such as different prohibitions and requirements regarding free data flows.[6] Multilateral digital trade rules are one way to address the problem.

In this context, the text agreed under the WTO Joint State Initiative on E-commerce (26th July 2024), which the UK is part of, is an important first step. While the text is comprehensive (e.g. facilitation of electronic commerce, prohibition of imposing custom duties, open government data and consumer protection), there are two key deficiencies. First, the US (the major exporters of digitally delivered services, accounting for 16% of global exports of these) did not join the agreement.[7] Second, key provisions for digital trade governance, cross-border data flows, data localisation and source code are missing in the concluded text. This is because the US withdrew its support for these provisions due to its concern over rapidly evolving digital technologies and the need for technology regulation in the US.

---

[4] Li, W. Y. (2023). Regulatory capture's third face of power, *Socio-Economic Review*, Vol. 21, No. 2, 1217–1245.

[5] There is an economic analysis done by the OECD secretariat. See López González, J., Sorescu, S., Del Giovane, C. (2024). Making the most out of digital trade in the United Kingdom, OECD Trade Policy Papers No. 285.

[6] See Borchert, I., Bacchus, J, Morita-Jaeger, M. and Ruiz, J. (2024). Interoperability of Data Governance Regimes: Challenges for Digital Trade Policy, CITP Briefing Paper 12.

[7] Among the WTO JSI initiative participants (91 WTO member countries), the countries which did not join the agreement are: Brazil, Colombia, El Salvador, Guatemala, Indonesia, Paraguay, Separate Customs Territory of Taiwan, Penghu, Kinmen and Matsu, Türkiye and United States.

Even without these provisions in the agreement, the US still expressed concern that the security exceptions should be revised.

The US used to promote free data flows and bans on data localisation and of source code requirements taking the regulatory-free and a more laissez-faire digital trade approach as seen in the Trans-Pacific Partnership (TPP), the US-Canada-Mexico (USMCA) agreement, and the Japan-US agreement. For example, there is little scope for public policy space under USMCA and Japan-US.

Now the US government is concerned about data privacy and protection (how personal data is collected and stored by tech companies), US Big-Techs' dominant position in the market, ethical use of technology (e.g. AI) and national security (e.g. access to advanced technologies by China and Russia). Since the US does not have the federal-level legislation on data privacy and technology regulation at the domestic level, the US Congress is considering federal-level legislations including data privacy and regulation of the technology sector, such as establishing standards for digital platforms and technology firms.[8] However, it would take some time for the US to establish the federal-level legislations. It would be difficult for the US government to come back to international negotiations including the WTO until these issues are resolved at the domestic level.

Meanwhile, the UK could lead discussions on challenges surrounding cross-border data flows and the role of government outside the WTO and trade negotiation forums. These discussions should involve a wide range of stakeholders and promote collaboration with the UK's like-minded countries, such as the EU and Japan. Such grassroots activities might encourage the US to come back to the negotiation table in the future.

Q: How do you think the government should balance issues such as the right to regulate to protect data privacy or to access source code, with commitments in treaties protecting free flows of data or intellectual property of software developers? What has its approach been to date and do you think it should approach these issues in future?

Striking the right balance between free data flows and regulations to achieve public policy objectives is not easy: signatories of an agreement have different interests and constraints reflecting their constitutional, political, economic, ethical and cultural backgrounds at the domestic level. For example, the speed of policy developments regarding digital trade provisions under FTAs or digital economy agreements is much faster than developments in domestic privacy regimes in signatory countries.

[8] See detail in Digital Trade and Data Policy: Key Issues Facing Congress, Congressional Research Service, July 30, 2024.

Below, we analyse (i) the general approach regarding the public policy space, (ii) a balance between free data flows and data privacy and (iii) the protection of intellectual property rights and access to source code, and suggest how these issues should be addressed in the future.

(i) General approach regarding the public policy space

- **Provide an independent objective clause with a clear public policy objective to affirm the UK's digital governance principle**

All the UK's digital trade agreements prohibit restrictions on free cross-border data flows. However, the general approach regarding the public policy space varies. The UK's FTAs/digital economy agreements to date can be categorised into four types: (i) the UK-EU which has a comprehensive objective clause and the UK-Japan with a simple objective clause from the public policy objective perspective, (ii) the UK-NZ and the UK-Singapore which have different types of objective clauses in comparison with the one under the UK-EU, and (iii) the CPTPP which includes a clause similar to an objective clause in the "scope and general provisions" highlighting more on economic objectives,[9] and (iv) the UK-Australia which has no objective clause.

The objective clause under the UK-EU (Art. DIGIT.1) and the UK-Japan (Art. 8.70) try to balance the promotion of digital trade and ensuring a trustworthy environment. The UK-EU stipulates that its objective is "(i) to facilitate digital trade and (ii) to address unjustified barriers to trade enabled by electronic means" while "to ensure an open, secure and trustworthy online environment for businesses and consumers". The UK-Japan (Art. 8.70) simply provides that its objective is "to create an environment of trust and confidence" and "to promote electronic commerce".

Other agreements such as the UK-NZ and the UK-Singapore have different approach. For example, the UK-NZ (Art. 15.2) objective clause stipulates that the signatories "recognise the economic growth and opportunities and the importance of frameworks that promote consumer confidence, promoting interoperability, avoiding unnecessary barriers and digital inclusion".

Using the objective clause is an effective way to affirm the signatories' key principles to digital trade governance and strong commitments to balancing economic objectives and public policy objectives. **We recommend the UK government includes an independent objective clause which balances economic objectives and establishes trustworthy online environments for all stakeholders in any future agreements.**

[9] The CPTPP stipulates in its "scope and general provisions" (Art. 14.2) that the signatories "recognise the economic growth and opportunities provided by electronic commerce, the importance of avoiding unnecessary barriers to its used and development, and the importance of frameworks that promote consumer confidence".

- **Provide an independent right-to-regulate clause to improve predictability**

The UK government has taken two approaches regarding the right to regulate to achieve public policy objectives under its agreements to date. The UK-EU has a stand-alone clause regarding the right to regulate (Art. DIGIT 3) which affirms the signatories' right to regulate to achieve legitimate policy objectives. It lists the legitimate areas of public policy including 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. These clearly indicate the government's policy priorities and improve predictability.

In comparison, UK's other five agreements (ones with Australia, Japan, NZ, and Singapore and the CPTPP) insert the public policy objective provisions in the cross-data flow clause, stipulating that nothing in the agreement shall prevent a Party from adopting or maintaining measures consistent with free data flow provisions for public policy objectives. Unlike the EU-UK, the types of measures to achieve public policy objectives are not provided. Thus, they lack clarity regarding the legitimate areas of public interests that may justify governmental regulations.

We recommend the UK government includes an independent right to regulate clause with listing of the legitimate areas of public policy measures in its future agreements to improve predictability. The UK-EU is a good a template for future negotiations.

Regarding the legitimate public policy measures, the five agreements other than the UK-EU stipulate that signatories must fulfil the WTO-type (GATT Article XX and GATS XIV) two legitimacy requirements to pursue public policy objectives.[10] Legal experts observe that the WTO's legitimacy requirements limit signatories to adopt its measures.[11] For example, EU GDPR could be potentially judged as WTO inconsistent. **We recommend that the UK Government assesses the rapidly evolving digital policy landscape with regard to evolving issues such as security, competition, AI technologies, consumer protection, and data privacy, and conduct policy discussions involving business and non-business stakeholders to establish the UK's coherent position - including whether the UK takes WTO-type approach in its future agreements.**

(ii) A balance between free data flows and data privacy

[10] A signatory must fulfil two conditions: (i) a measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (ii) a measure does not impose restrictions on transfers of information greater than are required to achieve the objective.
[11] For example, see Bartels, L. (2015). The Chapeau of the General Exceptions in the WTO GATT and GATS Agreements: A Reconstruction, American Journal of International Law 109, 95-125.

- **Include a clause in future digital agreements which balances free data flows and data privacy based on an inclusive trade policy making process**

Regarding the relation between free data flows and personal data protection, the UK-EU differs significantly from other five agreements (with Australia, Japan, NZ, Singapore and the CPTPP). First, the UK-EU is the only agreement which sets personal data protection and privacy as a fundamental right (DIGIT.7). This means in practice that data protection is outside the scope of trade negotiations. It is the EU which decides whether its partner has an adequate level of legal regime regarding data privacy protection. In comparison, other agreements recognise the economic and social benefits of personal data protection. Second, the UK-EU is the only agreement which sets the adequacy decisions as a condition for free data flows (where decisions on adequacy and its implementation are set outside of the trade negotiations). The other five agreements take a more flexible approach. For example, agreements, such as the CPTPP, the UK-Japan, and the UK-Australia, allow for sector-specific privacy laws or laws that provide for the enforcement of voluntary undertakings by firms (e.g. APEC CBPR). As for the convergence methods, these agreements allow for mutual arrangements and broader international frameworks other than unilateral decisions.

This raises several questions, such as how could the UK or countries which adopt domestic privacy laws based on the EU GDPR, manage the conflict between CPTPP-like data privacy commitments and free data flows, including onward transfers of data to third parties. This is an area which requires clarity. We recommend the UK government assesses the issue and shares the outcome of that assessment with the public and the business community. The available information on data and trade tends to focus on the impact for businesses.[12] The government should explain how digital trade agreements involving different privacy regimes might impact on the data rights of ordinary people, and their exercise of redress in relation to any problems with cross-border data transfers.

Furthermore, the UK government could revisit balancing free data flow provisions and data privacy provisions. While the UK shifted from the EU style approach under the UK-EU to the Asia-Pacific style market-driven approach under the other agreements, Japan's policy shift went in the opposite direction -from the Asia-Pacific style approach to the EU style approach as can be seen from the EU-Japan protocol on free data flows and personal data protection. The EU-Japan protocol, which further developed on the UK-EU approach, has detailed provisions to clarify the position of the two signatories regarding free data flows and personal data protection.[13] Since

[12] https://assets.publishing.service.gov.uk/media/5faa756dd3bf7f03b1de43de/uk-japan-cepa-digital-and-data-explainer.pdf

[13] As for analysis regarding this issue in detail, see Morita-Jaeger, M. (2024). Can the UK lead on data flow governance? Insights from the EU-Japan protocol on free data flows and personal data protection, UKTPO, 23

the UK is well-positioned to encourage its trade partners to adopt high standard data protection regimes, creating, what might be termed, UK style provisions using the UK-EU and the EU-Japan protocol seems the way forward in its future agreements.

The UK's digital trade agreements (except for the UK-EU) include clauses requiring the existence of a data protection framework following international standards. However, in some agreements, such as the UK-Japan CEPA, this commitment is footnoted with an explanation that such frameworks may include *"a comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy"* (Art. 8.80.2 footnote 1).[14] This wording potentially commits the UK to accept palpably lower protections - such as voluntary undertakings and similar CPTPP-style regulation - as equal to the higher data standards in the UK GDPR. In the case of Japan, this is not an issue because there is an underlying mutual adequacy agreement. However, it could cause problems in other contexts, and therefore **we recommend that such a footnote is not included in future digital trade deals**.

(iii) A balance between Protection of intellectual property of software developers and access to source code

- **The prohibition on disclosure of source code imposes limitations on the government's regulatory power**

The use of intellectual property especially patenting has been a key incentive for driving innovation. One of the key requirements for acquiring patents is to disclose the key know-how to the public domain. This disclosure requirement is a trade-off to the 20-year market monopoly set by the WTO TRIPS Agreement. However, in recent years, the reliance on trade secrets for the protection of software is increasing as opposed to traditional patent protection which requires public disclosure of data. Trade secrets are intellectual property rights on confidential information. Particularly, the ban of source code disclosure as a claim of trade secret protection has been used in trade agreements not only in the UK but also in others (e.g. US-Japan Digital Trade Agreement (DTA), US-Mexico-Canada Agreement (USMCA) and the EU-Japan Economic Partnership Agreement (EPA)).

Article 39 of the TRIPS Agreement offers protection for trade secrets, yet the prohibition of software code disclosure provisions goes beyond the TRIPS Agreement and places limitations on the government's regulatory power. This measure aims to encourage international trade by protecting with trade secret foreign software developers' source code underlying their products

July 2024.

[14] This is inherited from the CPTPP (see Art. 14.8 footnote 6).

and service. However, **prohibition on disclosure of source code, software and algorithms imposes significant limitations on government's power to examine source code when it is necessary to ensure principles for AI governance, such as transparency and accountability for meeting regulatory, judicial, and procurement needs.** In other words, the prohibition of source code disclosure undermines the governments' power to implement key principles for digital, AI, and data governance. We analyse the issues in the UK's digital agreements in comparison with the selected US-led trade agreements (USMCA and US-Japan).

In terms of terminology, the term 'source code' refers to a set of characters expressed in a programme language for software to operate, and 'algorithm' refers to the idea behind the source code, which does not be written down in a programming language. The texts of the UK-Australia and the UK-EU make reference to source code of software, but not to algorithms. The UK-Singapore and the UK-Japan include a reference to the 'algorithm expressed in that source code'.

Overall, the scope for public policy regarding source code disclosure in trade agreements is limited. The US-led agreements such as the USMCA and the US–Japan contain the narrowest scope for public policy. We therefore do not recommend that the government follows this model. Except for the UK–NZ, which does not have a source code provision. This is due to the Waitangi Tribunal's finding of the source code provision in the CPTPP to be in breach of the Treaty of Waitangi. Other UK trade agreements (UK-Japan (Art 8.73), UK-EU (Art 207), UK-Singapore (Art 8.61 -K), UK–Australia (Art 14) and CPTPP (Art. 14.17)) provide little scope for governments' regulatory powers to access source code or algorithms.[15]

In terms of governments' capacity to analyse the source code, the UK–Japan has the broadest scope by referring to the possibility of transferring or providing access to the source code for the purposes of investigation, inspection examination, enforcement action, or judicial proceeding (Art 87.3). It also provides for a broader scope of exceptions to the ban of source code disclosure, including a broader scope for regulatory body and judiciary authority as well as national security considerations (see below). The UK-EU has the narrowest scope, only allowing for the regulatory body to require access 'pursuant to a Party's law or regulation related to the protection of public safety with regard to users online' (Article 207(3)(b)). This excludes access by judicial authorities and sets a high threshold on the possibilities of referring to this provision.[16]

[15] Jones, E., Kira, B., and Tavengerwei, R. (2024) Norm Entrepreneurial in Digital Trade: The Singapore-led Wave of Digital Trade Agreements. World Trade Review 23, 208-241.

[16] Slok-Wodkowska, M and Mazur, J. (2022). Secrecy by Default: How Regional Trade Agreements Reshape Protection of Source Code. Journal of International Economic Law 25. 91-109.

There are also other references made as to which government or industrial bodies could require disclosure. For example, the UK-Japan includes a mention of conformity assessment bodies, and the UK-EU includes exceptions for measures adopted in the context of a 'certification procedure'. The UK-Australia allows more government bodies to require disclosure (including a government agency, regulatory body, administrative tribunal, judicial authority, or a designated conformity assessment body). The UK-Singapore mentions conformity assessment bodies and allows access in a wider range of contexts (including for monitoring compliance with codes of conduct and standards). However, in these agreements the role of other stakeholders such as technical experts, academia and civil society is not clear. **We recommend that the government clarifies the ways in which stakeholders could engage in the demarcation of intellectual property protection and source code disclosure.**

- **It is imperative to adopt sufficient grounds for exceptions to source code protection**

In international trade agreements, exception provisions are critical to define the scope of states' rights to regulate. The exception provisions set the limits on the secrecy of source code. Overall, there are three types of exceptions: (1) public procurement, (2) disclosure requirements necessary to secure compliance with law or regulations, and (3) allowing access to the source code by regulatory and/or judicial bodies.

(1) Public procurement

The UK–EU and the UK–Japan make explicit the limits to source code secrecy; however, the limitation is confined to public procurement procedures. In the agreements such limits must be voluntary, therefore governments are dependent on the goodwill on the part of the contracting company, but not the law the state adopts. **We recommend that the government considers making voluntary disclosure mandatory disclosure, under certain circumstances, such as fulfilling the legal obligations of transparency and explainability in AI/data governance**.

(2) Disclosure of source code or algorithm is necessary to secure compliance with law or regulation

These types of exceptions incorporate GATS (Art XIV) and/or GATT (Art XX) requirements of the disclosure and/or modification of source code is necessary to comply with laws or regulations, such as the transparency and explainability requirements in the EU AI Act. These include the UK–EU (Art 412(1)), the UK–Japan (Art 8.3(2)), and the CPTPP (Art 14.7(3)).

(3) Provisions foresee an exception granting access to the source code to government and/or judicial bodies

Strengthening the state's capacities to analyse the source code with a view to making the source code available for specific purposes, e.g. investigation, inspection, examination, enforcement action, or judicial proceeding, which is a manner of preserving the states' law-making and law-enforcement capacities. As mentioned above, the UK-Japan contains the broadest scope for regulatory bodies or judiciary authorities to access the source code. It also explicitly excludes 'services supplied, or activities performed in the exercise of government authority' and national security interests (Art 8.73.4). The UK–Singapore has similar exceptions but not as detailed and comprehensive. The UK– EU contains limited scope of access by judicial authorities. It also sets a high threshold of 'users online' when referring to this provision.

- **The UK-Japan CEPA is a more balanced model but the interpretation of the scope of protection still requires broad engagement of technological experts**

To strike a balance between intellectual property protection and source code disclosure, we recommend following **the approach taken under the UK–Japan agreement, with a view to engaging multi-stakeholders such as industrial or academic technological experts, and identifying current vulnerabilities and strengthening risk management.** These are also essential steps to pave the way for open innovation. **Initiatives are required to aim to support new, distributed, community-driven open-source ecosystems.** Such an approach may offer an improved path to navigate the complexities of closed innovation, especially those inherent in the patentability standards of AI inventions, as well as issues related to disclosure, enablement, and protectionist measures based on national security.

Q: How effective would you say stakeholder engagement been in the development and implementation of digital trade agreements, or in the digital provisions of international agreements?

- **Public engagement should involve non-business stakeholders**

We do not see that the processes of stakeholder engagement have been satisfactory. To date, the Trade Policy Engagement team at the Department of Business and Trade (DBT) has been very active in sharing information through emails and conference calls with stakeholders. However, most of the outreach tends to cover agreements that are completed or about to be signed, and not early stages of negotiations. In some of those information webinars, involving large numbers of stakeholders, there is some

space for questions and answers. However, the regular input channels on the policy are more limited to business stakeholders. There is also almost no feedback to non-business stakeholders.

Non-business stakeholders can reach out to policy makers, but to our knowledge there have been only some limited engagement activities, such as the roundtables with the consumer group Which? and the Oxford Blavatnik School. In comparison, there is a primacy of businesses engagement over other stakeholders, as reflected in the various events organised by the government alongside trade discussions, such as parallel sessions for SMEs during rounds of US-UK trade discussions.

The breadth of engagement in policymaking around digital trade was rolled back some years ago. The initial Expert Trade Advisory Group (ETAG) on Digital Trade included representatives from public interest groups and experts, but it was later restricted exclusively to businesses. Other groups, such as the advisory group on trade and intellectual property managed to maintain a broader participation using confidentiality agreements. The participation of civil society was channelled at the time into a single engagement group: this was primarily concerned with traditional trade justice and development issues. Despite this limited engagement, a coalition of Civil Society Organisations lodged a formal complaint in 2022 over the Government's failure to consult the public on the impacts of several trade deals.[17]

Policy questions elicited by the UK government tend to focus on the economic case for digital trade and not on the wider social impacts on the UK. The CITP project on citizen juries, which aimed to understand public engagement and attitudes to trade including digital trade,[18] shows that the public sees economic growth as the overall objective of trade. When asked about specific trade-offs, the majority prioritised workers' rights, human rights, data privacy and maintaining food standards over simple price reductions from FTAs. The result of the citizen juries also shows that the public recognises that the government should be making decisions in these complex areas, though more out of lack of alternatives than of real trust. The results also show some disenchantment toward the government making transparent and accountable decisions. There is also a demand for more public consultation, accountability mechanisms and calls for the government to be informed by independent experts rather than sector experts or businesses.

We recommend the Government implements citizen juries or similar innovative forms of public engagement to understand the concerns and priorities of the UK public. There are issues of trust in

[17] "UK Government accused of breaching international law over trade deals", Trade Justice Movement Blog, July 2019 2022

[18] CITP Press Release, It's not all about the money, say UK public when considering trade policy, circumstances matter, 25th April 2023.

policymakers that may benefit from additional support from experts. One possible solution here would be to create an independent source of advice and analysis on digital trade policy.[19]

Engagement with the public after trade deals are signed and implemented is even more limited. Each of the UK's digital trade agreements has a special committee, such as the committee on electronic commerce, to implement digital trade provisions. However, there is little transparency regarding its implementation. **The implementation process under a special committee on the digital trade chapter of each agreement should be shared with public. Also, the UK government should improve public engagement, including both business and non-business stakeholders during the implementation process, such as inviting stakeholders to a special committee on digital trade.**

- **The UK could lead digital trade policies supported by a wider social consensus amid the policy shift in the US.**

As stated in the answer to the first question (see page 3), the need to improve public engagement and stakeholder participation in digital trade policy has gained more urgency with the recent policy changes in the United States.

It is noteworthy that the USTR has started to improve public engagement in its digital trade policymaking. For example, it has ramped up efforts at public engagement with trade unions, minority groups and other social actors.[20] Also, the USTR has expressed that they will try to align their digital trade policy with their internal regulations of the technology sector. Increasing the participation of UK regulators in digital trade policy would likely improve public trust and the quality of these policies.

The US policy shift could potentially open space for policy innovation, requiring wider public engagement. This could prompt the UK government to revisit data and digital trade governance.

The regulation of cutting-edge digital technologies such as AI, requires international efforts. The UK has been at the forefront of such initiatives with the first AI Safety Summit in November 2023. **The UK government has an opportunity to lead in the development of the next generation of data and digital trade policies that incorporate a broader perspective and are supported by a wider social consensus.**

Summing up, the new government has an opportunity to make great improvements in this area. **Data and digital trade governance should be inclusive – listening to both business stakeholders and non-business**

[19] Winters, A. (2024). How do we make trade policy in Britain? How should we?, *The World Economy*, Vol 47 (9).
[20] USTR Requests Comments on Advancing Inclusive, Worker-Centered Trade Policy, USTR, 15th June 2023.

stakeholders is the key to creating a sustainable and trustworthy data and digital trade environment. We recommend that the UK government incorporates a wider range of perspectives from civil society, beyond business interests, in the policymaking and negotiations of digital trade agreements and their implementation.

4 October 2024