Open Rights Group submission to UK consultation on the UK joining the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)

Javier Ruiz <javier@openrightsgroup.org**>**

23 November 2018

We have general concerns about the process of trade policy, shared with much of civil society. Modern trade agreements regulate more than trade, covering a staggering range of public policy, as evidence in the list of topics presented in these consultations.

As a rights organisation we believe that a focus on trade weakens the wider international framework of rules. Trade treaties are easier to enforce than other types of international treaties and end up taking precedent. The special tribunals staffed by trade experts that can impose tariff sanctions on sectors not related to the original dispute are problematic. For example, the EU has been paying the US for years to avoid importing hormone-treated beef, while the US pays the Caribbean island of Antigua over restrictions on the burgeoning internet gambling industry based on the small nation.

As a digital rights organisation we find particularly worrying that the complex issues we deal with could be literally traded away by negotiators. This is particularly the case given the track record of secrecy surrounding trade deals, which create a democratic deficit, with the executive legislating through diplomacy without proper parliamentary input. This is being criticised in debates over the Trade Bill, with no sign of the government agreeing to give up their powers.

While thanks to grassroots pressure WTO proposals are now public, most Free Trade Agreements are secret and only made public once the consolidated texts have been agreed. At that point it is too late to make any modifications. We expect the UK government will be fully transparent and engage civil society.

In this note we focus on the aspects of digital trade. There is evidence of a concerted global lobby by the "Big Tech" companies of Silicon Valley to rewrite the rules of trade to consolidate their global position through the"e-commerce" or "digital trade" agenda[i]. In this they are copying the model that Big Pharma used 30 years ago to irreversibly rewrite the rule of intellectual property worldwide. Once that these treaties are fixed there are not sunset clauses, no proper courts to evolve jurisprudence or even strike treaties down. CPTPP is a central plank of this process.

We see the current discussion on digital trade as an existential threat to digital rights and are unambiguously opposed to the UK joining the CPTPP. We also believe that some of the clauses in CPTPP would create a fundamental regulatory conflict with EU policies and could lead to problems with future data flows with the EU, including jeopardising a UK future adequacy decision under GDPR.

The TPP, now renamed CPTPP is the most important trade agreement for digital as it contains the spot cutting edge provision. Furthermore, its clauses both consolidate and spread the digital trade agenda to other FTAs. The US has pulled out of TPP but most of their proposals are still there, so ironically they have introduced their policies without needing to open up their markets.

It is unclear whether the UK will actually benefit from the CPTPP. Various studies on the economic benefits of TPP have predicted very low economic gains for the participating countries, or even deficits. One study forecasts the loss of 771,000 jobs across the TPP nations.[ii]

Our main concerns with the CPTPP centre around Chapter 14 on E-commerce. Restrictions on data localisation requirements are found in article 14.13: "No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory." Article 14.11 includes complementary measures on data transfers: "Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person."

Data transfer restrictions are a key element of the European Union's approach to privacy, which restricts data transfers to those countries with laws that meet the "adequacy" standard for protection.

Canadian scholar Michael Geist analyses how these measures are subject to at least three exceptions: government data, financial services and a general four-step test exception, where a measure:

- must achieve a legitimate public policy objective;
- cannot be applied in a manner that would constitute a means of arbitrary or unjustifiable discrimination;
- is not a disguised restriction on trade; and
- does not impose restrictions greater than required to achieve the objective (i.e., a minimal impairment requirement on the use or location of computing facilities).

Geist argues that given the 1999 reference to privacy by the World Trade Organization (WTO), privacy could be viewed as a legitimate public policy objective and therefore qualify for an exception. However, in his view the historical record suggests that reliance on this exception is rarely accepted.[iii]

One areas of particular concern is the restriction on the disclosure of source code (Article 14.17). Governments are banned from requiring the disclosure of source code as a condition of import, distribution, sale or use of software or of products containing software. This prohibition focuses on “mass-market” software or products and excludes “critical infrastructure”. In the UK critical infrastructure is defined in cybersecurity legislation, but this is not the case in every CPTPP country.

There are concerns for open source software. The focus on “mass market” excludes commercially negotiated contracts for bespoke software development, but open source software may fall out of scope. So called viral open source licenses are not negotiated, they simply force third parties using such code to make future derivative source code public and allow others to modify it, thus ensuring that openness is carried forward.

Chapter 14 of CPTPP also contains some positive headlines, including requirements to protect personal information (Art 14.8), however, this a very weak provision, as it allows weak data protection frameworks instead of the robust GDPR approach the UK currently enjoys.

Other measures included are protection for net neutrality (14.10), but this is also weak as it allows blocking of content for “reasonable network management” and it excludes traffic shaping or degradation outside outright blocking.

Other measures that can have some impact in the UK include electronic signatures, custom duties and non-discrimination of digital products or spam. We will not go into more detail on these and other issues CPTPP raises as our partner civil society organisations from the participating countries have extensively analysed these provisions. See the joint briefing by the US group Public Citizen and the Canadian CIPPIC for a detailed discussion[iv].

In addition to the e-commerce provisions the original TPP also contained draconian intellectual property measures. Some the most worrying provisions on copyright terms, criminalising secondary DRM circumvention (TPM) and others have been suspended, not fully removed.

One areas that remain is the criminalisation of copyright infringement in Article 18.77. The measures in the CPTPP are not dissimilar to those introduced by the UK government the Digital Economy act 2016, and contested vigorously by ORG[v]. Joining CPTPP would cement these measures in the statute. One new measure would be the criminalisation of "the unauthorised copying of a cinematographic work from a performance in a movie theatre that causes significant harm to a right holder" (para 4). This could in practice criminalise many teenagers who film excerpts of movies and put them online.

Article 18.78 on Trade Secrets also brings new criminal offences. In some cases, the unauthorised access to computer systems will already be an offence under the Computer Misuse Act, but the would reject he expansion of criminal measures. This is particularly problematic at a time when cutting edge algorithms and AI systems are subjected to scrutiny and reverse engineering for innovation and accountability purposes.

i https://www.theguardian.com/commentisfree/2018/may/22/data-big-tech-eu-regulation-gdpr

ii https://www.weforum.org/agenda/2016/06/who-would-the-tpp-really-benefit

iii https://www.cigionline.org/articles/data-rules-modern-trade-agreements-toward-reconciling-open-internet-privacy-and-security

iv https://www.citizen.org/sites/default/files/tpp-ecommerce-chapter-analysis.pdf

v see https://www.gov.uk/government/news/open-rights-group-campaign