

11 November 2020

SUBMISSION TO THE CALL FOR EVIDENCE - INTERNATIONAL TRADE COMMITTEE

1. Open Rights Group are grateful for the opportunity to provide our input to the EU International Agreements Subcommittee on the UK-Japan trade agreement. Open Rights Group are a digital rights campaigning organisation. We seek to help build a society where rights to privacy and freedom of speech online are respected, protected and fulfilled. We have over 20,000 engaged supporters across the United Kingdom. We advocate evidence-based policy, guided by respect for fundamental human rights.

2. Trade deals can weaken citizens' rights by enacting mutually enforceable commitments to deregulation with limited public debate and democratic oversight. We find the UK-Japan trade agreement especially problematic, as it poses threats to both a range of digital rights as well as the process of securing a post-Brexit data protection agreement from the EU. This submission summarises our concerns, which are also available in a fuller briefing on our web site.¹ **We ask the Committee to help us seek clarity on these issues from government, and we look forward to continuing to engage with you.**

DATA PROTECTION, FLOWS, AND THE EU ADEQUACY AGREEMENT

3. Our most critical concerns are based around the trade deal's implications for the UK's data protection regime. Data protection underpins the entire service economy from shopping to banking to healthcare. The UK-Japan agreement places all of this data at risk of abuse.

4. The language of the data protection clauses of the UK-Japan trade deal are consistent with the publicly acknowledged US strategy to replace the European rights-based privacy framework which currently protect UK citizens' personal data with the Asia-Pacific framework's self-regulatory system as the global trade norm.² The EU's Japan adequacy decision explicitly mentions the APEC-CBPR as an example of rules that "do not guarantee the required level of protection".³ The EU required Japan to change its data protection regime, including supplementary rules on onwards transfers of EU data to other countries. The EU Parliament has expressed further concerns⁴ and Japan is considering further changes.⁵ The UK, through this trade deal, is committing to align with the APEC-CBPR standard regardless.

5. The Trade Agreement is not the only evidence of this policy shift. Dr Minako Morita-Jaeger, a Japan expert at the Sussex University UK Trade Observatory, has said that "*the National Data Strategy, launched in September 2020, appears to be consistent with the Asia-Pacific approach to data governance.*"⁶ This raises concerns that the National Data Strategy, which government is presenting as a wholly benign domestic initiative, is in fact part of a predetermined shift of the UK's high standards of data protection to the self-regulatory Asia-Pacific model, using the UK-Japan trade deals as a means to legally cement that shift without public consultation or adequate Parliamentary scrutiny.

6. The UK-Japan deal includes measures which ban restrictions on the free flow of personal data, restrictions which clash with the safeguards UK and European data protection law requires of international transfers. These clauses, in Articles 8.80 and 8.84⁷, and their direct endorsement of lower data protection standards such as APEC-CBPR, would be a direct obstacle to the UK receiving EU data protection adequacy once implemented. By accepting these kinds of standards, the UK-Japan data deal commits

¹ <https://www.openrightsgroup.org/publications/what-the-uk-japan-trade-deal-means-for-digital-rights/>

² <https://www.openrightsgroup.org/blog/leaked-uk-us-trade-talks-risk-future-flow-of-data-with-the-eu/>

³ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019D0419&from=EN>

⁴ https://www.europarl.europa.eu/doceo/document/B-8-2018-0561_EN.html

⁵ <https://iapp.org/news/a/analysis-of-japans-approved-bill-to-amend-the-appi/>

⁶ <https://trade-knowledge.net/commentary/the-japan-uk-comprehensive-economic-partnership-agreement-cepa-running-to-stand-still-or-stepping-stone/>

⁷ https://wiki.openrightsgroup.org/wiki/UK-Japan_Comprehensive_Economic_Partnership_Agreement

to create a legal mechanism to allow data about both UK and EU citizens to enter the UK, and then be sent onwards to Japan, and then to the US, with limited safeguards and oversight. Personal data originating in the UK could then be used under US legal terms, meaning the APEC-CBPR contractual arrangements are the only significant legal safeguard. It would also establish the UK as a potential hub for “data laundering” of personal data into these more lax legal regimes – a form of innovation no government should wish to encourage.⁸

7. It is unclear whether the Government intends to align with the Japan-US APEC-CBPR system in the forthcoming Japan adequacy decision for January 2021, or at a later date; but Parliament needs to understand the ramifications of making this decision to align with APEC-CBPR for UK-EU data transfers. The first and simple risk is that the UK has to “account” for EU data as Japan does currently, by marking all European data as “not for transfer under APEC CBPR”. The prospects for UK-EU adequacy are already incredibly fragile. A Japan adequacy agreement that aligns with APEC-CBPR would remove any prospect of EU adequacy until additional data segregation measures are put in place.⁹ *Parliament should ascertain from Government that the Treaty creates an obligation to align with APEC-CBPR or similar ‘voluntary but enforceable’ standards, and ask when this alignment is expected.*

8. Government has not, to our knowledge published any assessment of APEC-CBPR, and how it would impact UK data protection. As we noted, the EU regards the framework as incompatible with GDPR rights. It recognises voluntary arrangements made under contract law as sufficient for data protection. This removes the need for a regulator, with rights of inspection and audit, and for dedicated data protection courts, thus it is likely to reduce independent scrutiny and individual rights of recourse significantly.

9. Given that APEC-CBPR and the UK’s GDPR are likely to be incompatible, in order for the UK to comply with the terms of the trade agreement, it will need to rewrite portions of the agreement to remove UK data protection rights in order to align the two regimes. This may cause *more* problems for EU adequacy, even if data auditing is in place, as it currently does for Japan, whose general regime is again being reviewed for improvements. There are significant concerns for Japan that current EU adequacy agreements would not survive a legal challenge. The UK would place itself in a similar dilemma: it either reduces protections to meet the standards of the trade agreement and APEC-CBPR, in which case it risks legal challenges domestically or in Europe for UK adequacy, or it keeps standards high, in which case adequacy with Japan and transfers to APEC-CBPR are open to legal challenge. If a domestic court cancelled UK-Japan adequacy or refused to permit transfers under APEC-CBPR, this would open the UK to challenge for breach of the trade agreement. *Parliament should ask for an assessment of these issues.*

DATA LOCALISATION

8. Separately from data flows, the UK-Japan deal contains a ban on the forced localisation of computing facilities as a condition to carry out business in the country. It is unclear to what extent this could require NHS sensitive data to be transferred to Japan and, as previously discussed, onwards to the US, given the complex public-private partnerships in place. Parliament should ask for clarification.

ALGORITHMS, SOURCE CODE, AND CRYPTOGRAPHY

9. Both the UK and EU deals with Japan contain provisions which ban the transfer of, or access to, algorithms and source code as a condition for trade. There is a growing demand for systems to become accountable through scrutiny of algorithms and source code, including from Parliament. Restrictions on access to algorithms and source code will block these policy objectives. Parliament should ask for clarification.

10. Additionally, the UK-Japan deal introduces a specific exception for law enforcement to demand access to encrypted communications and for financial regulation. The implications of bringing cryptography into these

⁸ <https://www.theguardian.com/commentisfree/2020/oct/17/uk-tax-brexit-data-haven-britain>

⁹ <https://www.ianbrown.tech/2020/10/09/the-uks-inadequate-data-protection-framework/>

trade deals have not been explored properly, including how it may interact with other regulations on privacy, export controls, cybercrime, or access to justice. Parliament should ask for clarification.

INTELLECTUAL PROPERTY ENFORCEMENT

11. The treaty departs from the EU-Japan agreement in the enforcement of intellectual property infractions. The text contains articles tackling the circumvention of technical protection measures (TPM) and rights management information (RMI). These anti-circumvention measures could hamper the nascent movement for the “right to repair” digital technology, which ranges from personal mobile phones to agricultural machinery programmed by software. *Parliament needs to establish under what conditions the UK can establish circumvention of TPMs.*

12. Additionally, some text engages on the intellectual property issues created the EU Copyright Directive, which could require sites to proactively scan user uploads for copyrighted content. While the UK has already confirmed that it will not transpose that directive, this suggests that the trade deal is being used to bring those provisions into force through the back door. *Parliament needs to establish what duties flow from these provisions.*