CAP submission on IPEF

Digital economy-related matters

The Trans-Pacific Partnership (TPP)[1] included an electronic commerce (ecommerce) chapter. Some World Trade Organization (WTO) Members are also negotiating a plurilateral Joint Initiative (JI) on E-commerce.[2] Big tech companies such as Google, Amazon and Facebook have been aggressively pushing the ecommerce rules above,[3] including in IPEF[4] and some of CAP's concerns about the impact on consumers etc of these ecommerce provisions are outlined below.

As algorithms, big data, electronic authentication and digitalisation etc become more widely used, governments need the policy space to regulate this fast-moving area of technology. Therefore it is particularly important that the IPEF does not restrict this regulatory space since the regulations which will be needed in future are not yet known. Amending treaties such as IPEF once they are in force is a time-consuming negotiating process (as well any domestic procedural requirements), so if IPEF restricts the ability to regulate this fast-moving technological area and then its governments need to impose new restrictions on new technology that would violate IPEF, the risk is that IPEF could not be amended in time and quickly becomes out of date and problematic. This is not a hypothetical issue as can be seen by the broadening of exceptions to the source code provision in the TPP's ecommerce chapter in subsequent agreements, however these have not been reflected in amendments to the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) so CPTPP Parties are unable to implement competition law etc provisions because they are stuck with the TPP's restrictions on source code.

Electronic authentication/esignatures

The TPP[5] and the JI ecommerce[6] include provisions prohibiting governments from requiring companies and consumers to use a certain level of cybersecurity etc in their electronic authentication.

However, governments often need to regulate electronic authentication methods to protect consumers etc e.g.:[7]

- The Malaysian central bank requires two-factor authentication for internet banking transactions[8] to ensure they are secure.
- India's central bank requires mobile banking transactions to use two-factor authentication etc.
- The US Federal Trade Commission (FTC) has charged companies who fail to encrypt sensitive data such as credit/debit card information due to the large number of fraudulent purchases which occurred.
- The New York State Department of Financial Services requires certain companies to encrypt non-public information when it is in transit and at rest (unless it is unfeasible).
- Some US states such as Massachusetts and Nevada require encryption of personal information when it is being transmitted to protect privacy etc.
- To prevent identity theft etc, approximately 25 US states have passed laws specifying that social security numbers cannot be required to be transmitted unless the connection is secure/encrypted as the US Federal Trade Commission recommended in 2008 that Congress enact.

- After an intruder accessed sensitive personal information, the New York Attorney General in 2014 required Uber to encrypt GPS-based location information when in transit and the adoption of multi-factor authentication, or similarly protective access control methodologies.
- To reduce administrative costs and burdens etc, the US Patient Protection and Affordable Care Act sets requirements for electronic exchange of information as does the USA's Health Insurance Portability and Accountability Act (HIPAA). Since this is for efficiency etc reasons, this would not be saved by even an effective, easy-to-use health exception.
- Canada mandated cybersecurity standards for its petroleum and natural gas pipelines because of the critical importance of energy infrastructure.
- The Department of Homeland Security (DHS) reported ongoing cyber intrusions among U.S. natural gas pipeline operators which heightened congressional concern about cybersecurity in the U.S. pipelines sector and the White House, Congressional representatives and regulators (both Democrat and Republican) have all expressed concern at these cybersecurity risks and proposed mandatory regulations to address them. The US did not regulate and the largest US fuel pipeline was hacked in 2021 because of a failure to use multifactor authentication causing it to be shut down for the first time in its 57 year history, causing shortages across the East Coast and higher fuel prices etc as well as Colonial to pay a $4.4million ransom.[9]

Government regulation is needed in the examples above because of market failures and the inability of individual consumers to force banks etc to use more secure methods of electronic authentication etc. However the TPP and JI ecommerce do not permit the government regulation above except for 'a particular category of transactions'.[10] However as can be seen above, exceptions for more than one category of transactions are already needed, let alone in future as electronic authentication becomes more common.

IPEF should therefore not include these restrictions on electronic authentication.

Cross-border data flows and data localisation

The TPP[11] and JI ecommerce[12] include that Parties must allow data (including personal information) to flow out of their countries to anywhere in the world, including to non-Parties or countries with no privacy protection and no copy being stored locally. Governments require data to be stored locally for a number of reasons including:[13]

- For privacy reasons. E.g.:
  - one data broker has data on more than 820 million consumers[14] and a US Senate report noted this data can be organised in lists such as "'Rural and Barely Making It,' 'Ethnic Second-City Strugglers,' 'Retiring on Empty: Singles,' 'Tough Start: Young Single Parents,' and 'Credit Crunched: City Families.'" So these 'lists enable marketers to identify vulnerable consumers with ease. . . precision targeting of vulnerable groups also carries a risk of harm.'[15]
  - the FTC flagged that certain companies may obtain lists of consumers which are more receptive to certain forms of enticements or "suffering seniors" who have Alzheimer's or other such conditions to target them with toxic financial products'[16] and Equifax has already been convicted in the US for selling consumer data to predatory lenders.[17]
  - 5% of patients account for almost half of health costs, so health insurance companies want to avoid insuring these sick people, or charge them more. Therefore, companies were gathering records from pharmacies and selling them to health insurers who could use the information to reject health insurance applications from those with pre-existing conditions or charge them more.
  - Therefore Australia requires health data to remain in Australia where it has strong privacy protection, rather than allowing it to go offshore to countries with no privacy protection and Malaysia restricts the transfer of personal data outside Malaysia[18].
- To prevent tax evasion. E.g. New Zealand requires a copy of tax records that are stored on the cloud to be stored on a New Zealand server so that they can be checked by tax authorities without having to rely on a mutual legal assistance treaty (MLAT) which can be slow and uncertain (if they exist with the country storing the data).

- For effective financial regulation including in crises such as the 2008 global financial crisis when Lehman Brothers positions needed to be unwound after it collapsed, but its data was held in Hong Kong and US regulators found it difficult to access.
- For security reasons. E.g. the USA requires all cloud computing service providers that work for the Department of Defense (DOD) to store DOD data within the USA and South Korea restricts the cross-border transfer of mapping data.

In addition, the Organisation for Economic Co-operation and Development (OECD) noted the problems with getting evidence from abroad via MLATs where delays mean illicit funds in corruption cases can be lost, documents can be destroyed etc.[19] E.g. Singapore did not receive an answer via an MLAT so had to release money laundering funds which it had seized, Australia noted the difficulty in getting material via an MLAT in a form admissible in its courts and even Australia had resource challenges in using MLATs.[20] This indicates that digital economy provisions in IPEF could undermine other IPEF areas of interest such as anti-corruption[21] by prohibiting requirements to store data locally and therefore making law enforcement in a variety of areas more difficult.

The TPP[22] and JI ecommerce[23] include an exception for legitimate public policy objectives (LPPO) as long as they pass a necessity test and are also not arbitrary/unjustifiable discrimination/disguised restriction on trade ('chapeau'). However governments have failed to pass the necessity test at the WTO 61% of the time and failed to pass an easier-to-satisfy[24] version of the chapeau 86% of the time.[25] Since the TPP had a specific additional exception to data localisation for financial institutions (see below), presumably US financial regulators did not think that this general LPPO exception was sufficient.

IPEF should therefore not include provisions on cross-border data flows or location of computing facilities/data localisation.

Source code and algorithms

The TPP[26] and JI ecommerce[27] include provisions restricting the ability of Parties to require access to or transfer of source code (and algorithms[28] in the case of the JI ecommerce). However, governments often require:[29]

- Access to source code e.g.:
    - Canada and Malaysia's competition laws allow the competition authority to access/seize/inspect anything including source codes and algorithms. This is needed because as a law professor noted, algorithms etc can be anticompetitive.
    - Tax authorities in countries such as the USA have the authority to access source code in software used for accounting, tax return preparation or compliance, or tax planning.
    - The US Securities and Exchange Commission and Commodity Futures Trading Commission have access to high frequency trading (HFT) source code since HFT can destabilise the stock market by exacerbating flash crashes etc
    - For car safety reasons. E.g. when the brakes in Toyota cars suddenly stopped working causing fatal crashes, a US government agency enlisted experts to check the software and the plaintiff's experts in a court case against Toyota also examined the source code and found the problem that caused the fatal crashes
    - In court cases e.g. to check if source code has been stolen or infringes intellectual property (IP) or in criminal cases or to determine breathalyser accuracy etc.
    - By gambling regulators. E.g. the Nevada gambling regulator requires access to source code of gaming machines
    - In government procurement
- Transfer of source code e.g.:
    - As a remedy for anticompetitive conduct e.g. as the FTC has required in the past or as a condition of a merger/acquisition etc.
    - By tax authorities e.g. in the US
    - In government procurement so governments are not locked into the original supplier for upgrades and modifications etc.

In future, regulators may wish to check:[30]

- The source code in cars to ensure manufacturers are not using software to defeat emissions tests again.
- the source code of medical devices such as pacemakers and insulin pumps etc before they are approved since they are vulnerable to hacking
- source code and algorithms for discrimination

The TPP's source code provision only had exceptions for critical infrastructure and patents, so did not permit any of the above (unless they could use one of the TPP' general exceptions etc e.g. for health/environment etc, but see difficulties below). After the TPP, free trade agreements (FTAs) included broader exceptions to the source code provision:

- in the Trade In Services Agreement (TISA) for LPPO provided they met the chapeau[31] then
- in some EU FTA proposals for LPPO and to **remedy** competition law violations as well as re IP and military procurement[32] then
- in the US-Mexico-Canada Agreement for regulators and courts to be able to require source code/algorithms to be made available to **regulatory bodies** for investigations, enforcement, judicial proceedings etc.[33] Then
- in the US-Japan Digital Trade Agreement for regulators/courts to be able to require source code/algorithms to be made available for investigations, enforcement, judicial proceedings etc[34]

However, the source code provision in the TPP has come into force unchanged in the CPTPP,[35] without these broader exceptions in later FTAs. This is a real life example of how quickly these provisions become out of date and how the speed of change in the digital sector means that new exceptions are rapidly needed and not possible (without going through long negotiations and domestic procedures) once the regulatory space has been restricted by treaties such as IPEF.

IPEF should therefore not include provisions restricting the ability of Parties to require: access to, disclosure of or transfer of source code or algorithms.

Ban on customs duties on electronic transmissions

The TPP bans customs duties on electronic transmissions between persons of the Parties[36] and the JI ecommerce includes a proposed ban on customs duties on electronic transmissions between persons of Members[37].

A ban on customs duties on electronic transmissions between IPEF Parties would reduce the ability of IPEF governments to collect revenue from this fast growing area. E.g. a United Nations Conference on Trade and Development (UNCTAD) paper calculated that Vietnam could lose US$51.6million/year and India US$497million/year due to a WTO moratorium on customs duties on electronic transmissions.[38] Developing[39] country governments need this revenue for healthcare etc including to pay for COVID-19 therapeutics, diagnostics and vaccines given the lack of a broad and easy-to-use waiver of IP on all COVID-19 technologies.

IPEF should therefore not include any provisions restricting the ability to impose customs duties on electronic transmissions.

Customs and trade facilitation issues

At the WTO, many developing countries still have much needed transition periods before they are required to make the costly and difficult changes needed for them to implement the Trade Facilitation Agreement (TFA).[40]

Given developing country budgetary constraints (including because of requirements to buy COVID-19 treatments, diagnostics and vaccines without a comprehensive and easy to use waiver of the intellectual property on them), the IPEF should not:

- undermine existing TFA flexibilities (including transition periods)
- include obligations beyond those in the TFA (including requirements to give up any TFA transition periods).

Environment and climate-related matters

The IPEF should not make it more difficult for IPEF governments to be able to take measures to address environmental problems, including climate change. I.e. it should not restrict environmental regulatory or policy space. This is not a mere hypothetical since IPEF provisions on the digital economy etc could restrict environmental and climate change regulations.

Other measures or practices - exceptions

As can be seen above, TPP-style ecommerce etc provisions can harm the health and privacy of consumers as well as the environment.

The standard **environmental** exception at the WTO[41] has proven to be difficult to use[42] and so would be insufficient to protect environmental regulatory and policy space from other relevant IPEF provisions.

The standard **health** exception at the WTO[43] has proven to be difficult to use[44] and so would be insufficient to protect the health of consumers in IPEF countries from other relevant IPEF provisions.

The **privacy** exception at the WTO, in addition to having the difficult-to-satisfy criteria of the health and environment exceptions above, also appears to be self-cancelling (it can only be used for measures 'necessary to secure compliance with laws or regulations **which are not inconsistent** with the provisions of this Agreement'),[45] so is clearly inadequate to address the privacy concerns above if other IPEF provisions undermine privacy.

If IPEF includes provisions which undermine the ability of its Parties to prevent **tax** evasion etc (e.g. see comments on digital-economy above), then IPEF needs an effective and easy-to-use tax exception that applies to all IPEF provisions to ensure that IPEF governments can continue to collect the taxes needed to fund healthcare and environmental protection etc.

The WTO's **prudential** defence appears to be self-cancelling[46] and although it applied to the ecommerce chapter in the TPP,[47] US financial regulators still excluded financial institutions from the ban on keeping a copy of data stored locally,[48] so they did not appear to think the prudential defence would be sufficient in the TPP to allow them to require banks to store a copy of their data locally. Financial crises cause unemployment[49] and other problems for consumers, so governments need the policy space to prevent financial crises and deal with them once they occur. Therefore merely copying the WTO's prudential defence would be insufficient to ensure that IPEF Parties can do the financial regulation that they need, including during financial crises.

The **security** exception at the WTO is only for the circumstances listed,[50] which does not include cybersecurity in times of peace and recent WTO jurisprudence indicates that it is not self-judging.[51] A security exception such as the one found in some US free trade agreements (FTAs)[52] which remove the exhaustive list of situations where the security exception can be used and include a footnote ('For greater certainty, if a Party invokes Article 22.2 in an arbitral proceeding initiated under Chapter Ten (Investment) or Chapter Twenty-One (Dispute Settlement), the tribunal or panel hearing the matter shall find that the exception applies.') would be more effective.

In conclusion, CAP does not believe the IPEF is necessary.

[1] https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text

[2] https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm . The JI ecommerce has not officially released its negotiating text, but the September 2021 version is available at https://www.bilaterals.org/?wto-plurilateral-ecommerce-draft-45155

[3] E.g. see https://ourworldisnotforsale.net/2017/Kelsey_E-commerce.pdf

[4] E.g. see comments by The Software Alliance (BSA): https://downloads.regulations.gov/ITA-2022-0001-0004/attachment_1.pdf which includes Microsoft etc: https://www.bsa.org/membership

[5] Art 14.6.2a)

[6] This appears to have already been agreed in A.1.2.4a) since it has no substantive [ ] and has been cleaned and endorsed according to the text.

[7] https://www.twn.my/announcement/TWN_esignatures2018-9.pdf published in 2018

[8] https://www.bnm.gov.my/documents/20124/856401/cp04.pdf/9bb7f8cd-00c0-c138-1539-97e53be6a8d3?t=1585799603437

[9] https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

[10] E.g. Art 14.6.3 TPP and A.1.2.5 JI ecommerce

[11] Art 14.11 and 14.13

[12] Proposed in B.2

[13] Page 9-12 of https://www.twn.my/MC11/briefings/BP3.pdf

[14] https://privacyinternational.org/advocacy-briefing/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad

[15] https://bigdata.fairness.io/

[16] https://www.esma.europa.eu/file/21667/download?token=RuKkSJxJ

[17] https://www.worldprivacyforum.org/2013/03/public-comments-letter-to-ftc-re-equifax-sales-of-consumer-info-to-predatory-lenders/

[18] s129 https://www.pdp.gov.my/jpdpv2/laws-of-malaysia-pdpa/personal-data-protection-act-2010/?lang=en

[19] https://www.oecd.org/corruption/ADB-OECD-Mutual-Legal-Assistance-Corruption-2017.pdf

[20] https://www.oecd.org/corruption/ADB-OECD-Mutual-Legal-Assistance-Corruption-2017.pdf

[21] https://www.regulations.gov/document/ITA-2022-0001-0001

[22] Art 14.11.3 and 14.13.3

[23] Proposed in B.2

[24] Since in the WTO the comparison to determine whether there is discrimination is between countries where the same/like conditions prevail, https://www.wto.org/english/docs_e/legal_e/gatt47_02_e.htm#articleXX and https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm#articleXIV

[25] https://www.citizen.org/wp-content/uploads/WTO-General-Exceptions-Paper_.pdf

[26] Art 14.17

[27] Proposed in C.3.1

[28] See http://unbias.wp.horizon.ac.uk/wp-content/uploads/2018/12/AlgorithmicTransparencyBriefingNotes_final.pdf for some examples of why access to, disclosure and transfer of algorithms may be needed

[29] https://www.twn.my/MC11/briefings/BP4.pdf

[30] https://www.twn.my/MC11/briefings/BP4.pdf

[31] Art 6 http://bilaterals.org/?tisa-draft-annex-on-electronic-32465

[32] https://trade.ec.europa.eu/doclib/press/index.cfm?id=1395

[33] https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between

[34] https://ustr.gov/countries-regions/japan-korea-apec/japan/us-japan-trade-agreement-negotiations/us-japan-digital-trade-agreement-text

[35] https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/comprehensive-and-progressive-agreement-for-trans-pacific-partnership-cptpp/comprehensive-and-progressive-agreement-for-trans-pacific-partnership-text-and-resources/

[36] Art 14.3

[37] B.3

[38] https://unctad.org/en/PublicationsLibrary/ser-rp-2019d1_en.pdf

[39] For the purposes of these comments ‘developing’ includes any least-developed countries joining IPEF

[40] E.g. see https://tfadatabase.org/ . E.g. Vietnam has only implemented 41% of its TFA obligations: https://tfadatabase.org/members/viet-nam and Vietnam’s GNI/capita is only 4% of the USA’s, https://data.worldbank.org/indicator/NY.GNP.PCAP.CD so it should not be required to take on the same obligations as the USA in IPEF or other international negotiations

[41] https://www.wto.org/english/docs_e/legal_e/gatt47_02_e.htm#articleXX and https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm#articleXIV

[42] E.g. see https://www.citizen.org/wp-content/uploads/WTO-General-Exceptions-Paper_.pdf

[43] https://www.wto.org/english/docs_e/legal_e/gatt47_02_e.htm#articleXX and https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm#articleXIV

[44] E.g. see https://www.citizen.org/wp-content/uploads/WTO-General-Exceptions-Paper_.pdf

[45] Art XIV.c)ii) GATS: https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm#articleXIV

[46] https://www.wto.org/english/docs_e/legal_e/26-gats_02_e.htm#annfin

[47] Art 11.11

[48] Art 14.13 applies to a ‘covered person’ and the definition of ‘covered person’ in Art 14.1 excludes ‘a “financial institution” or a “cross-border financial service supplier of a Party” as defined in Article 11.1’. While

Section B of Annex 11-B TPP includes a requirement to allow financial institutions to transfer copies of information out of the country, Parties can still require a copy of the data to be kept locally.

[49] E.g. see https://www.twn.my/title2/ge/ge26.pdf and https://www.adb.org/sites/default/files/publication/156003/adbi-wp148.pdf

[50] E.g. https://www.wto.org/english/docs_e/legal_e/gatt47_02_e.htm#articleXXI and https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm#articleXIVb

[51] https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds512_e.htm, https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds567_e.htm

[52] E.g. those with Colombia, Republic of Korea, Panama and Peru, https://ustr.gov/trade-agreements/free-trade-agreements