Understanding the Indo-Pacific Economic Framework for Prosperity:
Examining the possible impact of digital trade-related provisions on domestic regulation of the digital economy in five select countries

By: Rishab Bailey, Public Citizen[1]
September 2023

1.0. Introduction

The growth of the digital ecosystem has brought untold benefits for people around the world. However, the proliferation of digital technology has also brought with it several problems: the spread of illicit and dangerous content, disregard of privacy norms, monopolization of the digital economy, the uneven spread of value, and so much more. Countries around the world are therefore increasingly attempting to regulate the digital ecosystem to deal with these issues.

Such attempts, however, face pushback from incumbents who rely on a relatively unregulated ecosystem to derive their profits. One area where we see such a contestation is in the context of international trade agreements. Digital trade-related chapters are now included in a variety of trade agreements – both regional and bilateral. While ostensibly included to bring in regulatory consistency, implement high-standards of consumer protection, and promote cross-border trade in digital goods and services, many fear that rather than seeking to implement regulatory regimes that advance consumer or public interest, these digital trade chapters are being used to hardcode binding rules that advance the interests of Big Tech companies.

One of the most important trade agreements currently being negotiated is the Indo-Pacific Economic Framework for Prosperity (IPEF), commonly referred to as just the Indo-Pacific Economic Framework. Driven by the United States, the effort brings together 14 countries, representing about 40% of the world's GDP. The nature of the agreement is broad, consisting of four pillars that cover a range of issues from tax and anti-corruption to clean energy and supply chains. The agreement is said to be unlike other previous trade agreements in that it does not include negotiations on issues of market access and tariffs but instead focuses on issues such as labour and the environment.

One of the key components of the agreement is a pillar on trade, which includes a chapter on digital trade. There has been a significant amount of public discussion on this chapter, though as of now, there is no clarity on the exact provisions in the agreement as the negotiating texts remain secret. Big Tech has been lobbying the U.S. government, which is drafting all the IPEF negotiating texts, to include provisions similar to that in the U.S.-Mexico-Canada Free Trade Agreement (USMCA). This agreement is commonly seen as favouring the interests of Big

[1] The author acknowledges and thanks Jane Kelsey, Emeritus Professor, University of Auckland, New Zealand; J.C. Navera, Policy Officer, IBON International, Philippines; and Wahyudi Djafar, Executive Director, Institute for Policy Research and Advocacy, Indonesia for their comments and discussions. All views expressed are personal and all errors are the author's.

Tech companies[2] by implementing liberalized rules concerning the digital ecosystem and reducing the space for domestic conversations on regulation of the digital ecosystem.

In this context, this report examines the possible impact of including USMCA-style provisions on attempts to regulate the digital economy in five countries currently negotiating the IPEF: India, Indonesia, Philippines, Australia, and Singapore.[3]

The report begins with an overview of the IPEF, its aims, and the negotiation processes. It then attempts to understand the possible nature of digital economy-related provisions in the IPEF and the demands that Big Tech has made in this regard. Through scrutiny of public comments, it is demonstrated that Big Tech companies see the USMCA as a baseline for the IPEF. Some of the critical issues highlighted in the public comments include: (a) ensuring free cross-border flows of data, (b) preventing disclosure of algorithms and source code, and (c) protection of intermediaries from liability (safe harbour for intermediaries).

The final section of the report analyses the possible impact of including USMCA-style provisions on domestic regulatory frameworks pertaining to these three issues. The case is made that implementation of "high standard" USMCA-style provisions in the IPEF could have significant consequences for regulation of the digital economy in the countries under study. Implementing USMCA-style rules in the IPEF could hurt consumer interests (such as privacy and user safety) and reduce space for domestic conversations on nascent policy issues such as the regulation of AI.

2.0. Understanding the Indo-Pacific Economic Framework

The Indo-Pacific Economic Framework (IPEF) is an initiative launched by the U.S. government in May 2022 that seeks to "advance resilience, sustainability, inclusiveness, economic growth, fairness, and competitiveness"[i] for the economies of participating countries in the Indo-Pacific region. Launched as a mechanism to curb Chinese economic influence in the region,[4] the initiative aims to enable greater "cooperation, stability, prosperity, development, and peace within the region".[ii]

The IPEF includes 14 countries – the United States of America, Australia, Brunei, Fiji, India, Indonesia, Japan, South Korea, Malaysia, New Zealand, the Philippines, Singapore, Thailand, and Vietnam.[5]

[2] The phrase is used loosely to refer to the largest and most dominant technology corporations such as Alphabet, Meta, Amazon, Microsoft, IBM, etc., all of which are U.S.-based entities.

[3] The report focuses on existing or proposed regulation in the countries under study and in the process restricts itself to an examination of statutory instruments and regulatory policy. The report also excludes from its scope regulations aimed specifically at the public sector/government.

[4] China entered into the Regional Comprehensive Economic Partnership (RCEP) with Australia, Brunei Darussalam, Cambodia, China, Japan, Lao PDR, New Zealand, Singapore, Thailand and Vietnam. It has also expressed an interest in joining the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the Digital Economic Partnership (DEPA). The U.S. is not party to any of these arrangements, thereby giving rise to fears of greater Chinese influence over economies in the region.

[5] The framework will be kept open for more participants to join in the future, subject to adherence of the agreed -upon commitments.

The proposed framework consists of four pillars or areas for discussion, each of which will constitute a separate agreement:

(i) *Trade*: This pillar seeks to find common ground on issues concerning the digital economy (potentially including issues of cross-border data flows, data localisation, online privacy, and unethical uses of AI), as well as on issues concerning labour, environmental standards, and corporate accountability.[iii]

(ii) *Supply Chains*: This pillar seeks to establish commitments that aim to prevent supply chain disruption to create more "resilient" economies. Key issues for discussion include mapping of critical mineral supply chains, improving traceability in key sectors, and coordination on the diversification of supply chains.[iv]

(iii) *Clean Energy, Decarbonisation and Infrastructure*: This pillar focuses on efforts to tackle the climate crisis, including through the use of renewable energy, imposing energy efficiency standards, and measures to combat methane emissions.

(iv) *Tax and Anti-Corruption*: This pillar attempts to enforce stringent measures concerning tax evasion, anti-money laundering, and anti-bribery regimes.

Of particular interest to this report is the Trade Pillar, as this is expected to contain detailed provisions pertaining to the digital economy.[6] There are also understood to be digital elements in each of the pillars, though at this time there is insufficient information available to analyze them. The Trade Pillar is the only one that appears to have a separate digital trade chapter.

While the U.S. Trade Representative (USTR) has said the IPEF does not constitute a traditional free trade agreement, or a replacement for other multilateral processes covering market access, tariff restrictions, and the like,[v] countries are nevertheless expected to adhere to all the commitments under any chosen pillar. It remains unclear what enforcement mechanisms the trade chapter may contain, although the U.S. will have the ability to conduct inquiries under Section 301 of the 1994 Trade Act if it believes the IPEF parties are engaged in unfair trade practices that breach their obligations.

A country can opt out of any single pillar but must agree to adhere to all commitments under any chosen pillar. Notably, India has, for the moment, opted to stay out of the Trade Pillar, ostensibly due to differences over provisions pertaining to the regulation of the digital economy and fears that the introduction of high labour or environmental standards could act as non-tariff barriers to Indian trade.[vi] The other negotiating countries have agreed to participate in all four pillars.

Pursuant to ministerial meetings conducted in the U.S. in September 2022, the scope of discussions under each pillar was announced.[vii] Further meetings have since taken place to discuss the text of the agreement, with the U.S. pressing to conclude negotiations by November 2023 to coincide with its hosting of the Asia-Pacific Economic Cooperation (APEC) summit in San Francisco.[7]

[6] The U.S. Trade Representative (who is heading negotiations on the Trade Pillar) and other IPEF partners issued a ministerial statement in September 2022, outlining the scope of the negotiations under the Trade Pillar, which is to cover discussions on: labour, environment, digital economy, agriculture, transparency and good regulatory practices, competition policy, trade facilitation, inclusivity, and technical and economic cooperation.

[7] Following the first in-person ministerial meeting in September 2022, further negotiating rounds have taken place at Brisbane in December 2022, in New Delhi in February 2023, in Bali in March 2023, in Singapore in May 2023,

3.0. ***What Are Likely Provisions Concerning the Digital Economy?***

At the outset of negotiations, the U.S. government was clear that the IPEF would seek to lay down "high standards" on cross-border data flows, data localisation, online privacy, and unethical and discriminatory use of AI.[viii] The Ministerial Statement on the text following the first in-person ministerial meeting in September 2022 notes that the IPEF would work to focus on initiatives that would, among other things, promote:

(a) trusted and secure cross-border data flows;

(b) inclusive, sustainable growth of the digital economy;

(c) responsible use and development of developing technologies; and

(d) competition and consumer protection law that ensures open, fair, transparent, and competitive markets, including digital markets.

The Ministerial Statement also recognized the need for flexible approaches to be adopted to achieve public policy goals of diverse communities.[ix]

Following the first ministerial meeting in Los Angeles, the USTR (who leads negotiations for the Trade Pillar I) published negotiating goals for that pillar, although these do not specifically mention measures pertaining to the digital economy.[x] Subsequently, while full texts for various issues under the Trade Pillar such as trade facilitation, agriculture, services domestic regulation, transparency, and good regulatory practices, have apparently been tabled, the U.S. has still not provided negotiating parties with a full draft of the text for the digital trade chapter. This is reported to reflect internal tensions within the U.S. government on core aspects of the digital trade chapter, including some of those discussed in this paper. To date, negotiations have been limited to texts that the U.S. has tabled.[xi]

While discussions on the draft text on digital trade continue, U.S. trade officials are known to have solicited the advice of lobbyists for Big Tech companies to help craft the IPEF's digital trade provisions.[xii] It appears that an initial version of the text proposed by the U.S. contained provisions that "would have effectively stymied any efforts by the countries to regulate the tech companies…".[xiii] While the USTR has commented on the need to disentangle trade negotiations from the interests of Big Tech companies, it appears that many of these companies are engaged in both public and back-door negotiations to ensure that their interests are reflected in the final text of the IPEF.[xiv] This is all the more worrying, given the relatively limited participation of other stakeholders in the negotiation processes and the corporate capture of the trade advisory system in countries such as the U.S.[8] The speed at which negotiations are being conducted also limits the ability of other non-corporate stakeholders to influence the text.

---

and in Busan in July 2023. Ministers have met in person in Los Angeles and Detroit and several times online. U.S. Department of Commerce, *Indo Pacific Economic Framework*, https://www.commerce.gov/ipef.

[8] Civil society groups have pointed to the lack of transparency in negotiation of the IPEF, which limits stakeholder engagement. See for instance, *100+ U.S. Civil Society Organizations Call for a Transparent and Participatory Negotiating Process for the Indo-Pacific Economic Framework (IPEF) and Future Trade Negotiations*, July 22, 2022, https://www.citizen.org/wp-content/uploads/IPEF-transparency-letter-july-2022.pdf; *Civil Society Calls for Release of IPEF Pillar 2 Agreement and Current Texts*, July 6, 2023, http://aftinet.org.au/cms/sites/default/files/CSO%20IPEF%20Pillar%202%20Release%20Letter.pdf#overlay-context=; Pita Ligaiula, *Pacific groups call for greater transparency in mega-regional trade talks*, Pacific News Service, September 9, 2022, https://pina.com.fj/2022/09/09/pacific-groups-call-for-greater-transparency-in-mega-regional-trade-talks/. It has also been pointed out that corporate interests dominate the U.S. government's official trade advisory system. For instance, 84% of U.S. trade advisors – who have privileged access to

3.1. What Provisions Does Big Tech Want?

Broadly speaking, Big Tech would like the IPEF to contain binding international standards that build on previously signed agreements such as the U.S.-Mexico-Canada Free Trade Agreement (USMCA), the U.S.-Japan Trade Agreement (USJTA), the Singapore-Australia Digital Economy Agreement (SADEA) and the Australia-United Kingdom Free Trade Agreement (AUKFTA).[xv] The USMCA in particular, which is viewed as a "pro-Big Tech" agreement,[xvi] appears to form the "baseline" for binding commitments in the IPEF.[9]

The nature of the wish list sought by Big Tech interests is clarified in submissions made to public comments processes in the U.S. and Australia. Though individual submissions do raise other issues, comments from Big Tech companies and industry groups coalesce around the following three major issues:

(a) Ensuring the "free flow of data across borders," achieved by restricting the imposition of localisation norms.

(b) Establishing safeguards against forced source-code disclosure as a condition to market access.

(c) Implementing "safe harbour" provisions for intermediaries, based on Section 230 of the U.S. Communications Decency Act 1996.

Other issues raised include restrictions on market access, provisions regarding non-discrimination (though market access issues are not going to be part of the framework), greater intellectual property protections, the removal of requirements to establish local offices or local representatives to carry out business, and forced encryption key disclosure.[xvii] These issues overlap to a considerable extent with the U.S. Chamber of Commerce's Priorities for Digital Trade.[xviii] Implementing binding minimum standards on these issues is seen as key to ensuring regulatory certainty, thereby reducing costs of business and enhancing market access, which protects the economic interests of U.S.-based Big Tech companies.[xix]

Big Tech companies have also not refrained from publicizing their positions on the IPEF. For example, at the time of the IPEF's launch, IBM called for the framework to include binding commitments "to support cross-border data flows, protect source code and algorithms, and encourage the adoption of open digital architectures".[xx] More recently, an Alphabet spokesperson addressed the issue of free-flow of data clauses in the IPEF, stating: "We have very publicly advocated for the Indo-Pacific Economic Framework to include strong digital trade provisions that ensure digital technologies are widely accessible, and that support privacy, security, and trust in cross-border data flows".[xxi]

An overview of these issues and the possible impact of adopting USMCA-like provisions in the IPEF follows.

---

negotiating text – represent business interests. See Rethink Trade, *Loaded – Corporate Interests Dominate the Official US Government Trade Advisory System*, https://rethinktrade.org/ustr-advisors/

[9] See for example, Google and Microsoft comments. Google, *Comments regarding the Indo-Pacific Economic Framework*, April 11, 2022, https://www.regulations.gov/comment/ITA-2022-0001-0046; Microsoft, *Response to Office of US Trade Representative Request for Comments on the Proposed Fair and Resilient Trade Pillar of an Indo-Pacific Economic Framework and US Department of Commerce Request for Comments on the Indo-Pacific Economic Framework*, April 11, 2022, https://www.regulations.gov/comment/ITA-2022-0001-0034; Microsoft, *Indo-Pacific Economic Framework Consultation*, October 2022, https://www.dfat.gov.au/sites/default/files/ipef-submission-microsoft.pdf

4.0. Analysing the Possible Effects of IPEF on Domestic Regulation of the Digital Ecosystem

This section examines how adoption of USMCA-like provisions on the four issues highlighted previously could affect attempts at regulation of the digital economy in five of the IPEF negotiating countries. By providing examples from India, Indonesia, Philippines, Singapore and Australia, the case is made that adopting "high standard" provisions such as in the USMCA could limit domestic attempts at regulating the digital economy in public interest.[10]

4.1.1. Free Flow of Data

One of the primary issues of concern to Big Tech companies is the implementation of measures restricting the foreign transfers of data. Such measures can take a variety of forms, ranging from conditional requirements – such as the need for a finding that the foreign country will adequately protect the data or for consent of the data subject prior to a transfer – to strict requirements that mandate local storage and processing of data. For instance:

(a) The EU's General Data Protection Regulation (GDPR) permits foreign transfers of personal data only if subject to an adequacy decision[11] or other appropriate safeguards that ensure effective rights and remedies for data subjects. Such safeguards may include the use of binding corporate rules, approved data protection clauses or certification mechanisms, etc.

(b) A number of countries bar foreign transfers of data that is considered particularly sensitive, such as financial, health, or telecom data. For example, Germany restricts transfers of telecom metadata and tax accounting data, and South Korea restricts transfers of mapping data and certain types of financial data (card data of consumers).

Data localisation mandates can be used, amongst other reasons, to:[xxii]

(a) *Protect the privacy rights of users* by limiting the ability of corporations to transfer data to foreign countries where privacy standards may be lower or where individuals may find it difficult to exercise their privacy rights. Restrictions on data transfers can also enhance the ability to audit and secure data flows.

(b) *Enhance administrative efficiency and improve domestic law enforcement* by ensuring that foreign corporations comply with a variety of domestic regulations, including by making it easier for regulators and authorities to carry out their supervisory and enforcement functions.

(c) *Promote economic and strategic purposes* by requiring the building of local computing and storage facilities and enhancing domestic capacity in this respect or implementing measures to create a level playing field in the digital ecosystem through taxation and other such measures.

[10] These five countries have been selected for study based on their size and economic heft. The regulatory frameworks concerning the digital ecosystem in each of these countries is also at different stages, with Australia and Singapore having the most advanced regulatory systems. For instance, data protection legislation in these countries was passed in 1988 and 2012 respectively. In comparison, India, the Philippines, and Indonesia have far more underdeveloped regulatory frameworks pertaining to the digital ecosystem. India, for instance, has yet to enact a comprehensive data protection law, while Indonesia passed such a law in 2022.

[11] That is, pursuant to a decision by the European Commission that a foreign jurisdiction ensures an adequate level of protection to the data, taking into consideration a variety of factors such as the relevant legislation, the presence of independent supervisory authorities, rule of law, and respect for human rights among others.

However, free flow of data clauses can restrict the ability of States to implement such measures.

Article 19.11 of the USMCA provides that: "*No Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person*." This provision is subject to exceptions that permit the implementation of localisation measures that are "necessary to achieve a legitimate public policy objective" and that are not (a) applied in a manner so as to constitute an arbitrary or unjustifiable discrimination or a disguised restriction on trade, and (b) do not impose restrictions on transfer of data greater than necessary to achieve the relevant public policy objective. Further, Article 19.12 of the USMCA restricts signatories from requiring computing facilities to be located domestically as a condition to conduct business in that territory. Together these provisions act to limit the ability of signatories to decide on whether and what barriers should be created to exports of data from their territories.[12]

The scope of the permissible derogations under the USMCA provisions mentioned above is relatively narrow, setting a high standard for any domestic measure to meet to pass muster. For instance, the provisions in the USMCA are far stricter that in free trade agreements (FTAs) such as the Regional Comprehensive Economic Partnership (RCEP) and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP).[13] The RCEP and CPTPP[14] recognise that: (a) parties may have their own regulatory requirements concerning the cross-border electronic transfer of information, and (b) parties may have their own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications. These provisions provide a broader latitude for domestic measures to be adopted that may restrict cross-border data flows. Notably, Article 19.12 of the USMCA does not allow parties to invoke a legitimate public policy objective exception to impose hard localisation measures.[xxiii] The exceptions provided under the RCEP and CPTPP treaties are also broader – they explicitly permit measures to be adopted in the interests of national security, which may not be disputed by other parties to the treaty.

[12] Separately, Article 17.18 of the USMCA, allows localisation measures to be implemented regarding financial payments in certain circumstances where sectoral regulators are not provided immediate, ongoing, and direct access to financial data required for their regulatory and supervisory roles and such failure is not remedied. This provision was apparently included in view of the difficulties of the U.S. financial regulators to access offshore financial data following the collapse of Lehman Brothers and the global financial crisis in 2008. However, one may question whether regulatory needs are met by this provision, given that a remedial process may take time, thereby delaying access to any important financial data. Jane Kelsey, John Bush, Manuel Montes, and Joy Ndubai, *How Digital Trade Rules Would Impede Taxation of the Digitalised Economy in the Global South*, Third World Network, https://www.twn.my/title2/latestwto/general/News/Digital%20Tax.pdf

[13] Article 12.15 and Article 14.11 of the RCEP and CPTPP recognise that parties may have their own regulatory requirements concerning the electronic transfer of information. The agreements require parties to allow cross-border transfers of information when this activity is for the conduct of the business of a covered person. Derogations from the provision are permissible in order to achieve a legitimate public policy objective, when such a measure is not arbitrary or a disguised restriction on trade, and where the measure is proportionate to the objective sought to be achieved. In addition, the RCEP permits derogations on national security grounds, which may not be disputed by other parties. Articles 12.14 and 14.13 of the RCEP and CPTPP recognise that parties may have their own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the secrecy and confidentiality of communications. Further, no party shall require a covered person to use or locate computing facilities within that party's territory as a condition for conducting business within that territory. However, parties are permitted to adopt measures to achieve legitimate public policy goals subject to such measures being non-arbitrary/a disguised restriction on trade and proportionate. In addition, the RCEP permits derogations on national security grounds, which may not be disputed by other parties.

[14] Amongst the countries under study in this report, the Philippines, Indonesia, Australia, and Singapore are parties to RCEP, while Australia and Singapore are parties to the CPTPP.

Under the USMCA, the cumulative impact of a domestic measure having to be both necessary and the least restrictive possible, reduces the space available to a signatory to adopt localisation-related measures.[xxiv] For instance, some have questioned whether requirements to take consent of data subjects prior to a cross-border data transfer could fall foul of these tests (in view of alternative, less restrictive measures available such as the creation of accountability mechanisms).[xxv] Indeed, these provisions could be said to favour a model of self-regulation, as such models are generally considered less restrictive that other more intrusive forms of regulation. There is also a lack of clarity on what constitutes a "legitimate public policy objective".[xxvi] For instance, would measures to enhance supervisory access of regulators, or that seek to enhance domestic sovereignty over data in the form of measures to provide a level-playing field for domestic data businesses be covered under such a flexibility? Would such a provision hamper the effective implementation of high standards of privacy protection?

In this context, it is worth noting that the EU, which also implements conditional restrictions on foreign flows of data under the GDPR regime, has been wary of the inclusion of USMCA-style free flow of data clauses in the World Trade Organisation's Joint Statement Initiative on E-Commerce, fearing that its domestic regulatory regime, which sets a high standard of data protection, may come under threat.[xxvii] The EU has instead sought to include provisions that specifically recognize the ability of countries to implement restrictions on cross-border transfers on grounds of protecting privacy.[xxviii]

Finally, it must be kept in mind that the provisions in the Digital Trade chapter of the USMCA are subject to certain general exceptions. These could, in theory, provide some flexibility to signatories to adopt contrary domestic measures. Thus, Article 19.2 (3) of the USMCA, excludes the applicability of the entire Digital Trade chapter to government procurement, or to information held or processed by or on behalf of a signatory. Further, Article 32.1(2) incorporates paragraphs (a), (b), and (c), of Article XIV of GATS into the agreement. These paragraphs provide for the application of domestic measures designed to: (a) protect public morals or public order, (b) protect human, animal, or plant life or health, and (c) enforce laws to protect safety of citizens or protect them from fraud or deceptive practices, or privacy harms. Such measures should not however be "arbitrary," "discriminate unjustifiably" between countries, or take the form of a "disguised restriction" on trade in services.

Other general exceptions under the USMCA include:

(a) *Article 32.2* which allows for measures to be taken to protect security interests.

(b) *Article 32.4* which allows for measures to ensure integrity and stability of financial systems.

(c) *Article 32.8* which requires adoption of appropriate legal frameworks concerning privacy in signatory countries.

Based on the measure at hand, these exceptions could be used to justify the imposition of domestic regulation concerning any of the four issues under study in this report. For instance, the GATS exception for privacy protection could be used to justify the imposition of domestic measures that restrict cross-border data transfers of particularly sensitive personal data such as health or payments data.

However, it is worth noting that despite the presence of the general exceptions, the successful use of these to defend domestic regulatory measures is extremely rare. Notably, only two out

of the 48 attempts to use the general exceptions under the GATT/GATS agreements have been successful over the past two+ decades.[xxix] Further, the usefulness of these exceptions has been questioned in the context of the internet economy. For instance, while the GATS agreement uses fairly broad terms (such as "public morals," "public order," or the ability to impose regulations to protect health, etc.), [xxx] these are said to be "limited in scope and do not facilitate consideration of Internet trust issues holistically".[xxxi] Thus, the exceptions provided for in the USMCA may not offer much policy flexibility for domestic regulation.[xxxii] Further, there is also a lack of clarity concerning the scope of the exemption created for the government. It is unclear to what extent the exemption applies to data held by regional/local governments, as well as public authorities. Norms concerning localisation of data held by state instrumentalities may therefore come under question.[xxxiii]

Among the countries under study, only Australia, Indonesia, and India apply any form of hard localisation norms:

(a) **Australia** requires the localisation of health data under the My Health Records system.[xxxiv] Service providers are required to store data only within Australia or face civil or criminal penalties.

(b) **Indonesia** requires all public sector data to be stored locally.[xxxv] Private electronic systems operators are permitted to transfer personal data abroad, provided the data is made available to relevant regulatory authorities to carry out their supervisory functions.

(c) **India** requires the localisation of government data, as well as digital payments data, corporate accounting data, certain types of health data, and telecom data.[xxxvi]

Each of the countries under study, however, does implement conditional restrictions on cross-border transfers of personal data, as explained below:

(a) **The Philippines'** *Data Privacy Act 2012 and Implementing Rules*[xxxvii] permit foreign transfers of personal data subject to the transferring entity retaining responsibility for ensuring security of the data. The data controller is required to ensure contractual arrangements or other reasonable means to provide a comparable level of data protection to data that is transferred to a third party.

(b) **Singapore's** *Personal Data Protection Act 2012* and *Personal Data Protection Regulations 2021*[xxxviii] prohibit cross-border personal data transfers unless the data will be comparably protected outside of Singapore.[15]

[15] Specific entities may be exempt from this requirement by the data protection authority upon request. For the purpose of a foreign transfer, the transferers of data must ensure that the recipient of the data is subject to legally enforceable obligations requiring protection of the data. This can occur through the presence of a law that protects the data, contractual provisions requiring a comparative standard of data protection, the use of binding corporate rules or similar legally binding instruments, or if the recipient holds certifications recognising that it provides a comparable degree of protection to the data. In any event, foreign transfers of personal data can also take place subsequent to consent of the individual concerned, in contexts where consent is deemed to have been provided, where the transfer is necessary to protect the vital interests of the individual and consent cannot be obtained in a timely manner and would not reasonably be withheld or if the transfer is in the national interest, the personal data is in transit through Singapore or if the personal data is publicly available in Singapore.

(c) **Australia's** *Privacy Act 1998* requires a data controller to take reasonable steps to ensure that a foreign recipient of data will not breach Australian privacy principles in handling the data.[16]

(d) **Indonesia's** *Personal Data Protection Law 2022* permits foreign personal data transfers subject to the data recipient's country having a legal framework that provides equivalent or greater protection as provided under the domestic law.[17]

Interestingly, the 2022 law does not revoke earlier regulations on data protection unless they are contrary to provisions of the new law. Thus, conditions provided in the *Law on Protection of Personal Data in an Electronic System 2016* on foreign transfers of personal data could still apply.[xxxix] This law requires transfers of personal data outside Indonesia to be coordinated with the relevant government ministry or institution, implying that relevant authorities must be informed of the proposed data transfer, including by providing details of the destination country, name of the recipient, date of transfer, and reason/purpose for the transfer.

(e) **India's** *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011* permits cross-border data transfers of sensitive personal data if the foreign jurisdiction has a similar level of data protection as provided for under the Rules. Such a transfer "may be allowed only if it is necessary" for the performance of a contract between the person to whom the information relates and the body corporate, or if the person has consented to the transfer.

Each of the countries under study allows cross-border transfers of personal data, subject to equivalent protection being afforded to the data in the foreign jurisdiction, which is usually to be enforced through the presence of binding contractual clauses or similar instruments.

However, conversations around the implementation of hard localisation norms continue. Notably, India's recently tabled *Digital Personal Data Protection Bill 2023* would permit the Central Government to notify countries to which Data Fiduciaries (data controllers) may not transfer personal data. The provision is extremely broad in that it gives the government a general power, that can be exercised for unstated reasons, to blacklist entire countries from processing Indian data.

In Australia, the *National Data Security Action Plan 2021*, a discussion paper issued by the government, has sought public comments on whether Australia needs to implement more explicit data localisation measures in view of the possible security risks to data when stored abroad.[xl] The paper recognises the need to balance free flows of data with protection of sensitive information, noting that "while data localisation laws may be justified in some

[16] This requirement is not applicable if certain conditions are met, including explicit consent of the data subject, where the transfer is required by law or an international agreement to which Australia is a party, or if the transferring entity reasonably believes that the recipient is subject to a law or binding scheme that protects the data in a way that is substantially similar to how the data is protected by the Australian Privacy Principles, and the individual concerned has the ability to access mechanisms to enforce the law or binding scheme.

[17] In the alternative, i.e. where the recipient's country does not provide a sufficiently high standard of data protection, the controller must "ensure that there is adequate and binding personal data protection." Hunter Dorwart et al., *Indonesia's Data Protection Bill: Overview, Key Takeaways and Context,* Future of Privacy Forum, October 19, 2022 https://fpf.org/blog/indonesias-personal-data-protection-bill-overview-key-takeaways-and-context/. Specifics of how this is to be achieved will be laid down in regulations to be notified subsequently. If the above two conditions are not met, personal data may be transferred abroad subsequent to consent of the data subject.

instances, widespread storage requirements can represent significant barriers to trade and economic cost." The release of the paper has apparently spurred much debate in Australia, with Big Tech companies arguing no benefit to such measures, while others have either taken more nuanced positions, or as in the case of one Australian cloud service provider, have suggested "full data sovereignty".[xli]

From the above, it is clear that while most of the jurisdictions under study employ conditional restrictions on data transfers, certain sectoral rules and regulations require localisation of specific forms of data considered particularly sensitive (such as health or payments data). While these may arguably fall under the scope of general exemptions provided for in trade law, this is subject to contestation, which would lead to legal uncertainty. In any event, as mentioned previously, the poor record of general exceptions protecting public interest-based domestic regulatory measures does not inspire confidence in the use of such measures in the context of the digital economy.

Further, measures such as those proposed in India's *Digital Personal Data Protection Act 2023* could fall foul of requirements of proportionality and necessity included in free flow of data clauses due to the broad nature of the localisation requirement. Even provisions in domestic law that permit conditional transfers of personal data could be subject to question under free flow of data clauses in trade agreements, due to the high bar required to meet the necessity and least restrictive measure tests, as well as ambiguity over the scope of permissible derogations on grounds of pressing public policy concerns. For instance, some have pointed to how the imposition of consent requirements for cross-border transfers of personal data "could be regarded as imposing restrictions greater than required to achieve the objective of privacy protection…".[xlii] Thus, a number of the cross-border data transfer measures discussed above could be subject to contestation on the grounds of being unnecessary and disproportionate. This could take on added importance as more and more sectors of the economy become data driven. Measures aimed at ensuring security/privacy of the data, as well as appropriate regulatory access to the data, may be hampered by inclusion of broad free flow of data provisions in FTAs.

4.1.2. Disclosure of Algorithms and Source Code

Software plays an increasingly integral part of our lives today, with the growth of the AI ecosystem in particular implying that algorithms and the software (or source code underlying the software)[18] will be used in virtually every area of our lives, from the judiciary and policing to consumer products. However, software can be programmed to serve illicit purposes or can have unintended consequences ranging from promoting/enhancing discriminatory treatment to misappropriating and misusing user data.[xliii]

Ensuring that software "does what it says" or acts within acceptable legal and ethical bounds, can be important to prevent harms ranging from a loss of life and property to illegal surveillance and discrimination.[xliv]

[18] A simple way of understanding source code is that this is the series of instructions that a computer program uses to perform a particular task. In more complex systems, based on machine learning and other newer forms of computing, the source code may provide guidance on how the program is to go about 'learning.' Algorithms are a set of instructions that are used to perform a specific task. Cosmina Dorobantu, Florian Ostmann, and Christina Hitrova, *Source Code Disclosure: A Primer for Trade Negotiators*, Chapter 4 in Addressing Impediments to International Trade, Alan Turing Institute, 2021, https://www.turing.ac.uk/sites/default/files/2021-06/dorobantu_ostmann_hitrova_2021_1.pdf

While regulatory responses to risks arising from deployment of AI systems are still being developed, an increasing number of international and domestic regulatory policies have sought to implement measures to enhance the transparency of AI-related products.

For example:

(a) The OECD's AI Principles recognise the need for transparency, explainability, accountability, robustness, security and safety of AI tools.[xlv]

(b) In the U.S., the Blueprint for an AI Bill of Rights calls for pre-deployment testing, risk identification and mitigation, and ongoing monitoring to ensure that AI systems are not unsafe, discriminatory, or inaccurate, as confirmed by independent evaluation.[xlvi]

(c) A number of proposed data protection and other laws seek to ensure that software is safe to use by requiring pre- and post-deployment algorithmic impact assessments and algorithmic audits.[19]

However, clauses in free trade agreements can limit the ability of regulators and independent entities to conduct *a priori* investigations of the source code/algorithms used in software.

Article 19.16 of the USMCA limits the ability of signatories to require disclosure or access to the source code of software/algorithms as a condition precedent to the import, sale, use or distribution of the relevant software or products containing the software. The agreement provides a limited exception that permits disclosure of source code to a regulatory or judicial body for the purposes of a specific investigation or proceeding, and subject to implementation of safeguards against unauthorised disclosure. The limitation of disclosure only to instances where a specific investigation has been launched can be extremely restrictive. It may be difficult to establish bona fide grounds for an investigation without access to the source code or algorithm itself. This also limits the ability for external or independent audit of algorithms and software systems, which could be critical in jurisdictions with low regulatory capacity.

While such clauses have been included in trade agreements ostensibly on the basis that corporations need to protect their intellectual property from disclosure (and copying), provisions that bar scrutiny of source code/algorithms prior to deployment can enhance the "black box" nature of AI and software tools, thereby enhancing risks associated with such systems. Ex-ante evaluations of algorithms/source code - whether by regulators or independent entities – can highlight problems with AI and software systems before harm occurs. The ability to access to algorithms appears to be of particular interest in the context of competition and consumer protection, with several competition authorities the world over increasingly seeking to examine the anti-competitive harms caused by algorithms used by big digital platforms. As noted by the UK's Competition Markets Authority, "Having access to the data and/or the code means it is possible to audit a decision-making system through a comprehensive regulatory inspection in a more thorough manner than a 'black-box' approach."[xlvii] The OECD, citing several instances of competition authorities examining algorithms for anti-competitive

[19] See for instance, the American Data Privacy and Protection Act (HR 8152), the Facial Recognition Act, 2022 (HR 9061), the Justice in Forensic Algorithms Act, 2021 (HR 2438), Platform Accountability and Transparency Act (S 5339), and the Facial Recognition and Biometric Technology Moratorium Act, 2021 (HR 3907/S 2052), *cf.* Daniel Rangel and Lori Wallach, *International Pre-emption by "Trade" Agreement: Big Tech's Ploy to Undermine Privacy, AI Accountability, and Anti-Monopoly Practices*, Rethink Trade, March 2023, https://rethinktrade.org/wp-content/uploads/2023/03/International-Preemption-by-Trade-Agreement.pdf.

outcomes, also recognises the importance of algorithmic auditability to protect consumer interests.[xlviii]

In any event, it is worth noting that the RCEP does not contain an analogous clause (restricting the disclosure of source code or algorithms), while Article 14.17 of the CPTPP applies only to source code and not algorithms. Further, the provision in the CPTPP does not specifically limit access to source code to instances where an investigation has been initiated. Indeed, the provision recognises that parties may require the modification of source code to enable compliance with domestic regulation. The power to require correction/modification of source code is done away with the in the USMCA, thereby limiting the ability of parties to require changes to algorithms/source code that could be found to be biased or otherwise harm individuals.[xlix]

The extension of treaty provisions to restrict access to algorithms is particularly worrying given that very few states, if any, have reached consensus on whether and how to regulate the AI ecosystem. While jurisdictions such as the EU and the U.S. have proposed various regulatory interventions in this space, in the countries under study, only Singapore appears to have a reasonably advanced policy framework pertaining to AI.

As part of its AI Strategy, 2019, Singapore recognises the need for a "progressive and trusted" environment to be created for the deployment of AI systems. To this end, it has adopted a largely self-regulatory/voluntary framework consisting of:

(a) *Principles to Promote Fairness, Ethics, Accountability and Transparency in the Use of Artificial Intelligence and Data Analytics in the Financial Sector 2018*: This document contains a set of principles that seek to promote fairness, ethics, accountability and transparency in the use of AI in financial systems. The document seeks to provide guidance to firms on ethical uses of AI and how to strengthen internal processes around data management and use. The document, however, does not refer to the need for any external testing or audit of AI systems.

(b) *Model AI Governance Framework 2020*: This voluntary code is intended to provide guidance to the private sector on deployment of AI systems. The document stresses that human well-being and safety should be a primary consideration in designing, developing, and deploying AI systems, and it recognises the need for organisations using AI in decision making processes to ensure that those processes are explainable, transparent, and fair. It highlights the importance of auditability, explainability, accountability, and fairness in the AI ecosystem, noting that evaluation of an AI product by internal or external auditors can contribute to the trustworthiness of an AI system and demonstrate the responsibility of design and justify outcomes. However, the document also notes that auditability does not entail making information about business models of intellectual property related to the AI system publicly available. The document therefore recommends a risk-based approach to auditability, with such practices to be adopted where necessary or where required for an organisation to align itself with regulatory requirements or industry practice.[20]

[20] Annexure B to the document notes that algorithmic audits would have to be carried out at the request of a regulator. Carrying out an audit may require engaging external experts. The document notes that an algorithmic audit can be an expensive tool, and therefore recommends only carrying out such an assessment when it is clear that such an exercise will yield a "clear benefit" for an investigation.

(c) *An AI governance testing framework known as AI Verify*: Launched in 2022 by the Infocomm Media Development Authority, the project seeks to enable AI developers to demonstrate their claims about performance of their systems by enabling voluntary self-assessment of their systems. The system is designed to preclude organizations from unintentionally divulging sensitive information from their AI systems (such as their underlying code or training data).[l]

Singapore, therefore, does not explicitly require any disclosure or audit of source code in its AI regulatory framework.[21]

The other countries under study—Australia, India, Indonesia and the Philippines—do not implement any specific AI-related regulations, though each has in place high-level AI-related policies and ethics-related guidelines.

For instance:

(a) **Australia** has developed an AI Ethics Framework, released in 2019, which consists of 8 principles which AI developers may use (voluntarily) to ensure their products/systems are safe, secure, and reliable.[li] These principles include those of transparency and explainability, which require responsible disclosure so people can understand when they are being impacted by AI and can find out when they are using an AI system. The principle of accountability recognises the need for human oversight of AI.

(b) The National AI Strategy of the **Philippines** recognises a variety of harms that could be caused by the unrestricted development and use of AI systems and therefore recognises the need for regulation of AI systems, noting in particular that AI-driven platforms may need to be audited to ensure that biases are not amplified or further propagated. [lii] The policy also recognises the need for proper appraisal of algorithms in cases where interpretability may be critical such as where decisions of AI systems impact humans.

(c) In **India**, the government's apex think tank, the Niti Aayog, has released a National Strategy for AI 2018, which identifies key opportunities and challenges for AI development and lays down a high-level roadmap for AI development.[liii] It has also developed Principles for Responsible AI, which lay down broad ethical guidelines and considerations for regulating the AI ecosystem.[liv] In addition to recognising the need for ethical uses of AI, and the possibility of various harms such as bias and discrimination arising from the unregulated use of AI, the document recognises seven principles to guide the adoption of AI in a responsible manner. While recognising that AI systems should be based on principles of equality, safety, reliability, inclusivity, non-discrimination, privacy, and security, the document highlights two vital principles: transparency and accountability. The principle of transparency implies that the design and function of AI systems should be recorded and made available for scrutiny and audit, to the extent possible, so as to ensure that deployment of a system is fair, honest, impartial, and guarantees accountability. The principle of accountability, amongst other things, requires stakeholders involved in design, development and deployment of AI

[21] Its privacy law too does not specifically require auditing of algorithms in the form of privacy impact assessments, though organisations are required to develop and implement policies and practices that are necessary for the organisation to comply with the PDPA. Organisations are therefore "encouraged" to conduct privacy impact assessments. Personal Data Protection Commission Singapore, *Guide to Data Protection Impact Assessments*, 2021, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/DPIA/Guide-to-Data-Protection-Impact-Assessments-14-Sep-2021.pdf

systems to set up auditing processes, either internal or external, to oversee adherence to relevant AI principles.

(d) In **Indonesia**, the government's National AI Strategy, the Stranas KA, recognises the need for development of ethics-based regulatory frameworks as a key focus area. The document therefore includes plans for "national standards, regulations and an ethics board to ensure that usage of AI is in accordance with the country's Pancasila values system".[lv]

While each of these countries has not yet implemented regulatory frameworks concerning the use of AI, the conversations around regulation of this space are growing. For instance, the Australian government released a discussion paper in June 2023 seeking public comment on the need for and methods of regulation within the AI ecosystem.[22] Separately, a report by the former House of Representatives Select Committee on Social Media and Online Safety makes various recommendations on the use of algorithms by digital platforms, which include greater examination of the harms caused by the use of algorithms as well as potential mechanisms to require platforms to report on their use of algorithms.[lvi] In its response, the Government of Australia has broadly agreed with the need for better understanding of how digital platforms use algorithms in their operations. It has also noted that various government departments are looking into various regulatory options concerning AI.[lvii]

India's proposed Digital India Act is likely to implement regulation over the AI ecosystem, in particular rules pertaining to quality testing, algorithmic accountability, and vulnerability assessment.[lviii] While the draft law is not yet available to the public, it is possible that it may require some measure of ex-ante disclosure to, or assessment of, algorithms/source code by the government/regulators.

From the above, it is clear that while each of the countries under study has recently recognised the need for development of AI systems based on sound ethics, regulatory frameworks in this regard are still to be fully developed. While many of the high-level policy documents in these countries recognise the need for greater transparency and auditability of AI systems, they remain unclear about the mechanisms to achieve these ends. While self-regulatory models are unlikely to fall foul of USMCA-style provisions, the use of more intrusive regulatory options that mandate disclosure or audit of source code/algorithms is likely to be problematic despite the presence of general exceptions (as discussed previously).

At the same time, there is growing public disquiet around the use and deployment of AI products and the lack of transparency over algorithms. For instance, in Indonesia, Gojek, a popular ride-sharing app, has faced calls for scrutiny over its algorithms from drivers who allege that the app's algorithms have "increasingly squeezed and exploited" their working conditions.[lix] Similar protests have been seen in India in the context of Zomato—a food delivery app—tweaking its algorithms to unilaterally impose more onerous working conditions on riders.[lx] In Australia, the "robo-debt" scandal demonstrated the need for greater

[22] The document notes the various harms that are made possible due to the use of AI systems (ranging from the spread of misinformation to discrimination) and lays down various options for regulation of the AI ecosystem (ranging from self-regulatory models such as that employed in Singapore to more interventionist regulation such as in the form of the EUs proposed AI Act). Department of Industry, Science and Resources, *Safe and Responsible AI in Australia: Discussion paper*, Government of Australia, June 2023, https://storage.googleapis.com/converlens-au-industry/industry/p/prj2452c8e24d7a400c72429/public_assets/Safe-and-responsible-AI-in-Australia.pdf

transparency and oversight of the use of AI and algorithmic systems, particularly where this could have significant impacts on people's lives.[23]

In other contexts, such as Europe's AI Act, similar interventionist regulatory approaches have faced significant pushback from Big Tech and industry lobbies.[lxi] The establishment of international rules that mandate deregulation in the AI space only aids such efforts. Under these circumstances, signing up to IPEF provisions that limit the ability of regulators or external experts to audit AI systems (through access to source code or underlying algorithms) would be, at the very least, premature.

4.1.3. Safe Harbour

The concept of "safe harbour" was first seen in the American Communications Decency Act, 1996 ("CDA"). Section 230 of CDA provides that "interactive computer services"[24] cannot be treated as the publisher or speaker of third-party information carried on their platforms.[25] Thus, the provision provides immunity from prosecution to platforms for carrying/distributing potentially harmful third-party content, and in the process seeks to encourage self-regulation (content moderation) by digital platforms. Crucially, the provision protects platforms from liability in circumstances where they have knowledge of harmful content being circulated.

A number of countries across the world have introduced laws that borrow from the CDA in insulating digital platforms from claims that could arise as a result of carrying illicit/illegal content. However, the safe harbour frameworks in many jurisdictions do not extend as far as the protection afforded by Section 230 CDA. Instead, many jurisdictions implement a functional differentiation between different types of intermediaries and only protect intermediaries from liability from third-party content if they are acting as passive transmitters (or distributors) of content. This entails that if knowledge of illegal content can be ascribed to the intermediary, it cannot avail of safe harbour. Thus, the safe harbour provided under these laws is of a far more limited nature than under American law under the CDA. For instance, the European Union's E-Commerce Directive distinguishes between intermediaries providing caching, hosting, and conduit services, with different obligations imposed on each type of intermediary.[26]

---

[23] The "robo debt" scandal arose out of the use of AI-based systems to calculate and recover welfare overpayments, thereby defeating welfare fraud. The system was however shown to use faulty data and was barred by the Australian Federal Courts in 2019. Mark Brogan and Mark Arratoon, *Robodebt, algorithmic accountability and the law of averages*, The Mandarin, January 19, 2023, https://www.themandarin.com.au/209861-robodebt-algorithmic-accountability-and-the-law-of-averages/; Peter Whiteford, *Debt by Design: The anatomy of a social policy fiasco – or was it something worse?*, AJPA Volume 80, Issue 2, June 2021, pp 340-360, https://onlinelibrary.wiley.com/doi/10.1111/1467-8500.12479; Centre for Responsible Technology, *I, Robodebt*, Submission to the Australian human Rights Commission discussion paper on human rights and technology, March 2020, https://humanrights.gov.au/sites/default/files/2020-07/50_-_the_australia_institutes_centre_for_responsible_technology_1.pdf

[24] Defined as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions."

[25] The provision is subject to certain exceptions created for enforcement of (a) federal criminal laws, (b) intellectual property laws, (c) certain state laws, (d) electronic communication related privacy laws, and (e) knowingly hosting content that promotes sex trafficking.

[26] In order to avail of the safe harbour, mere conduit intermediaries must not initiate the transmission, select the receiver of the transmission, and select or modify the information contained in the transmission. Cache providers must not modify the information, must comply with conditions on access to the information, must comply with rules regarding the updating of the information, must not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information, and they must act to expeditiously

While many point to how a safe harbour provision is essential to protect online speech, others argue that limiting the liability of platforms has resulted in the creation of an online ecosystem where harmful acts (ranging from the spread of disinformation to cyber bullying as well as terrorist and other extremely dangerous content) are rife, given that platforms have no incentive to moderate content.[lxii] Some have viewed safe harbour as a subsidy, which seeks to enable growth of platforms by insulating them from large damage claims.[lxiii]

In view of the significant harms seen in the online ecosystem, often occasioned by the platforms themselves, a number of countries have imposed or are considering imposing obligations on various types of intermediaries to ensure the digital ecosystem is safe.

For example:

(a) The **UK**'s Online Safety Bill seeks to create a new "duty of care" for online platforms that would require them to take action against illegal/harmful online content or face significant fines (and in some cases criminal action).

(b) The German Network Enforcement Act in **Germany** requires large social media platforms to put in place processes to disable or block access to content that is manifestly unlawful within a stated time period.[lxiv] The law also requires platforms to maintain robust grievance redress processes and imposes various reporting/transparency requirements.

(c) A number of jurisdictions, notably **Japan and the U.S.** (in the context of copyright content), only exempt intermediaries from liability for third-party content in the event they do not have knowledge thereof. These countries apply the general concepts behind distributors' liability to the Internet, implying that should any illegal/illicit content be brought to the attention of the platform concerned, and they fail to take appropriate remedial action, they could be held liable for the spread of the content.[lxv]

(d) The Digital Services Act in the **EU** establishes requirements for platforms to improve their content moderation practices. The law maintains immunity from prosecution to intermediaries (for carrying illegal third-party content) but establishes a variety of obligations that intermediaries are required to follow, which include the establishment of grievance redress mechanisms, and obligations aimed at enhancing the transparency of platforms towards users.

Such laws, while subject to criticism (usually on grounds of disproportionately restricting speech) pose a significant threat to the business models of large digital platforms, who can currently not just evade responsibility for harmful activities but are often alleged to actively enhance the spread of harmful content. Implementation of greater duties of care on platforms could lead to greater economic costs (in terms of operating costs occasioned by the need to implement content moderation practices or purchasing liability insurance) for platforms. It could also reduce online engagement, thereby reducing revenues.[27]

---

remove or to disable access to the information it has stored upon obtaining actual knowledge that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement. Finally, in order to claim safe harbour, hosts should not have actual knowledge of the illegal act and, as regards claims for damages, should not be aware of facts or circumstances from which the illegal activity or information is apparent; and upon obtaining such knowledge or awareness, must act expeditiously to remove or to disable access to the information.

[27] It is commonly stated that social media platforms for example, profit from hateful content by promoting such content in order to garner engagement. Tom Bateman, *Facebook profits off hate and that's why it won't change,*

Accordingly, Big Tech is pushing for the introduction of USMCA-like provisions in the IPEF, aiming to extend the broad protection afforded by U.S. law on intermediaries to other countries.

Article 19.17 of the USMCA mandates that signatories should not adopt 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.*" Parties are barred from imposing liability on suppliers of interactive computer services for taking action to moderate content on their platforms in good faith.[28]

This provision therefore replicates the CDA position under which platforms are (a) not to be held liable for third party content on their platforms (even if the platform is aware of the harmful content), and (b) encouraged to self-regulate. Notably, both the RCEP and CPTPP do not contain an analogous provision.

Inclusion of a USMCA-like provision in the IPEF could significantly affect the ability of signatories to implement duties on platforms to make the online ecosystem safer and more secure.[29] As with the previously discussed provisions, deregulation of the platform economy would largely benefit incumbent players in the ecosystem.

This would also threaten a number of domestic policy initiatives in countries that are negotiating the IPEF. For instance, Australia, India, the Philippines, and Singapore all confer safe harbour on intermediaries in the event they do not have "actual knowledge" of the offending third-party content. Each of these countries, together with Indonesia, requires intermediaries to take down illicit content once informed of the same. Indeed, many jurisdictions are seeking to increase the scope of the obligation on platforms to not just take down content once it is notified, but also to proactively filter their platforms for illegal content.

While requirements for proactive filtering of content have been criticized by many due to possible negative effects on civil liberties, the spread of a various types of harmful content on digital platforms—ranging from fake news to terrorist and other extreme forms of violent content—have created a situation where all the jurisdictions under study are looking at implementing greater state control over the social media space.

Some of the initiatives in this regard are:

(d) The **Australian** *Online Safety Act 2021*, which requires intermediaries to establish grievance redress mechanisms for users, ensuring proactive filtering to reduce access to illicit content and empowering the e-safety commissioner to issue notices directing removal, blocking, or link-deletion notices. A failure to comply with a notice can lead to fines being imposed on the intermediary.

---

says whistleblower Frances Haugen, *EuroNews*, *October 4, 2021*, https://www.euronews.com/next/2021/10/04/facebook-profits-off-hate-and-that-s-why-it-won-t-change-says-whistleblower-frances-haugen; Kris Shaffer, *The Business of Hate Media*, Medium.com, April 24, 2017, https://medium.com/data-for-democracy/the-business-of-hate-media-47603a5de5f4

[28] Exceptions to the provision are provided for enforcement of intellectual property and criminal law.

[29] One may note that various members of the U.S. Congress sought to have Article 19.17 of the USMCA removed, as it was felt this may limit the ability of the U.S. legislature to amend Section 230 of the CDA at a subsequent point of time. *Supra* Note xxiii.

(e) The **Australian** *Criminal Code Amendment (Sharing of Abhorrent Violent Materials) Act 2019* requires intermediaries to expeditiously remove certain types of illegal content, failing which they can face civil or criminal punishment. Similarly, the *Enhancing Online Safety Act 2015* establishes the office of the eSafety Commissioner, which is responsible for ensuring safety of the online ecosystem. The authority can issue removal notices for various types of illicit online content (cyber bullying, cyber abuse, non-consensual intimate images, Class 1 and Class 2 content under the Broadcasting Services Act).

(f) The proposed *Digital India Act* in **India** is expected to cast obligations on intermediaries to prevent various harms to users, such as the spread of revenge porn, cyber-bullying, etc.

(g) The **Indian** *Information Technology Act 2000* and rules issued thereunder require intermediaries to "make reasonable efforts" to prevent users from publishing illicit content. They also require intermediaries to establish grievance redress processes that are overseen by a government-appointed committee. Significant social media intermediaries are also required to "endeavor to deploy technology-based measures" to proactively identify particularly egregious types of illicit content.

(h) **Indonesia's** *Ministerial Regulation 5/2020* requires electronic service operators to proactively monitor and take down prohibited information and/or documents, as well as any information that could "inform ways or provide access" to such documents.

(i) **Singapore** has proposed two codes of practice for online social media services that require platforms to take various ex-ante measures to regulate content, including through proactive filtering of content, providing users tools to report illegal content, and implementing grievance redress mechanisms. *The Protection from Online Falsehoods and Manipulation Act 2019* enables a regulator to issue various directions to intermediaries to fact-check and disable access to false information. The regulator can also issue codes of practice that can require intermediaries to carry out certain forms of due diligence, identify locations from where false information is being spread, and prevent the use of bots from circulating such information.

While the content and effects of these regulations could be debated, what is clear is that each of the jurisdictions under study is attempting to put in place measures that cast greater obligations on intermediaries (particularly platforms) to make the online ecosystem safer and more transparent towards users. This represents a clear move away from the position adopted in the CDA. It is to be noted that the utility of the safe harbour provision in the CDA is increasingly being questioned, even in the U.S.[lxvi] The growing use and impact of social media in particular has brought about a realization that self-regulation of platforms is insufficient to promote a safe and trustworthy online ecosystem. Implementation of retrograde safe harbour provisions in the IPEF could therefore scuttle any such attempts at regulation. While such measures could possibly be defended using general exemptions that permit domestic measures to protect public morals, health and safety, etc., as discussed previously, the use of such exceptions has proven difficult in practice. Given the significantly different legal regimes used by the countries under study (and the pushback against S 230, CDA in the U.S.), it appears unlikely that, despite the wishes of Big Tech, that the IPEF will include a safe harbour provision modelled on Section 230 of the CDA.

5.0. Conclusion

The IPEF is an ambitious attempt at seeking regulatory alignment between the signatory countries on a host of issues, including pertaining to the digital economy. While the text of the digital trade chapter is not yet public, there has been intense lobbying in the U.S. Government for IPEF to contain provisions that advance Big Tech's interests.

Big Tech companies have been clear in seeking to include "high standard" USMCA-style provisions regarding a number of issues, including the free cross-border flows of data, limitations on access to source code, anti-discrimination measures, and limited liability of intermediaries. However, codification of USMCA-like provisions on these issues could limit the regulatory options available to signatories to implement public or consumer interest regulation over the digital ecosystem.

Specifically:

(a) Free flow of data clauses could limit the ability of countries to implement localisation norms or even conditions on foreign transfers of data. Such measures can be used for a variety of reasons ranging from the protection of personal data to ensuring a level playing field in the digital ecosystem or securing regulatory access to important data.

(b) Provisions restricting access to source code and algorithms could limit the ability of regulators or independent entities to scrutinize software products prior to their deployment. This reduces accountability and transparency while also enhancing the possibility of harms occurring to individuals and societies from the use of such products/services.

(c) Limited liability clauses modeled on the American CDA would limit the obligations cast on intermediaries (including platforms) to make the digital ecosystem safer.

Each of these provisions would directly impact a variety of regulatory and policy frameworks in the countries under study. For instance:

(a) Australia, India, and Indonesia apply hard data localisation norms to certain types of data, which may be subject to challenge. Even provisions pertaining to conditional foreign transfers of data, seen in the data protection laws of each of the five countries under study, could be challenged under the extremely strict free flow of data provisions used in the USMCA. In essence, the inclusion of such clauses would allow for the continued flow of data to the U.S., where it would be subject to its (relatively low standard) data protection norms.

(b) Each of the countries under study has recognised the need for development of AI systems based on sound ethics. Regulatory frameworks in this regard are still to be fully developed. While many of the high-level policy documents in these countries recognise the need for greater transparency and auditability of AI systems, they remain unclear about the mechanisms to achieve these ends. In the circumstances, it appears that signing up to IPEF provisions that limit the ability of regulators or external experts to audit AI systems (through access to source code or underlying algorithms) may be premature.

(c) Each of the jurisdictions under study has moved away from the American CDA position of providing intermediaries with virtual blanket immunity for carrying third-party content. In a recognition of the fact that self-regulation of the digital ecosystem has not

> led to optimal results, each of the countries under study has or is considering the implementation of laws that cast a variety of content moderation and related obligations on intermediaries. These would all be subject to challenge under USMCA-style safe harbour provisions if included in the IPEF. The inclusion of such a provision in the IPEF therefore appears unlikely, given the significant differences between extant models of safe harbour in these countries and the CDA position (as well as the increasing calls for amendment of Section 230 in the U.S. itself).

While the USMCA does contain various specific and general exemptions, commentators have questioned their utility in the context of the digital ecosystem. The specific exemptions built into the provisions are limited in scope. Further, it appears that the use of general exemptions in trade law is not a common practice. Thus, the agreement provides the illusion of flexibility while actually acting to restrict domestic policymaking in a significant manner.

Overall, it is clear that implementation of USMCA-style provisions in the IPEF would lead to an erosion of the ability of signatories to implement domestic regulations pertaining to the digital economy. This would entrench the status quo in the digital ecosystem and limit the ability of states to regulate the space in order to prevent harms to individuals and societies.

The three issues under study in this report all relate to areas where there is a need for nuanced policy conversations. For instance, there is no universal acceptance of the American model of safe harbour, with debates ongoing even in the U.S. as to the wisdom of continuing with the CDA framework. However, the adoption of binding international rules, which preclude any discussions at the domestic level on these issues.

It is also worth noting that the USMCA goes well beyond (the also controversial) agreements such as the RCEP and CPTPP (which have been signed by a number of IPEF negotiating countries) by restricting disclosure of algorithms (in addition to source code), imposing stricter requirements pertaining to free cross-border flows of data, and by adopting provisions requiring safe harbour to be provided to intermediaries.

Such issues are particularly concerning in the context of regulation of new and emerging technologies, such as in the context of AI, where there is still no consensus as to what forms of regulation are best suited to a particular context. The democracy deficit inherent in international trade negotiation processes is also a matter of concern. Not only do Big Tech interests appear to have preferential access to trade representatives and negotiators, but public consultations on the agreement have only been conducted in two of the negotiating countries—Australia and the United States—and even then, without access to the negotiating text.

Thus, inclusion of broad USMCA-style provisions in the IPEF is likely to significantly hamper how the digital ecosystem is governed in the countries under study.

Endnotes

[i] Office of the United States Trade Representative, *Indo-Pacific Economic Framework for Prosperity*, https://ustr.gov/trade-agreements/agreements-under-negotiation/indo-pacific-economic-framework-prosperity-ipef

[ii] *Supra* Note i.

[iii] The White House, *Fact Sheet: In Asia, President Biden and a Dozen Indo-Pacific Partners Launch the Indo-Pacific Economic Framework for Prosperity*, May 23, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/23/fact-sheet-in-asia-president-biden-and-a-dozen-indo-pacific-partners-launch-the-indo-pacific-economic-framework-for-prosperity/

[iv] *Ibid.*

[v] Saptaparni Ghosh, *Explained: What is the Indo Pacific Economic Framework for Prosperity?*, The Hindu, May 28, 2022, https://www.thehindu.com/news/international/explained-what-is-the-indo-pacific-economic-framework-for-prosperity/article65460071.ece.

[vi] Amiti Sen, *Opting out of the IPEF Trade Pillar was necessary*, The Hindu Business Line, September 26, 2022, https://www.thehindubusinessline.com/opinion/opting-out-of-ipef-trade-pillar-was-necessary/article65938850.ece; Saurabh Sinha, *India Stays out of Indo-Pacific Trade* Pillar, The Times of India, September 10, 2022, https://timesofindia.indiatimes.com/business/india-business/why-india-opted-out-of-joining-trade-pillar-of-ipef-for-now/articleshow/94106662.cms

[vii] Office of the United States Trade Representative, *Trade Pillar*, https://ustr.gov/trade-agreements/agreements-under-negotiation/indo-pacific-economic-framework-prosperity-ipef/trade-pillar

[viii] *Supra* Note iii.

[ix] Office of the United States Trade Representative, *Ministerial Text for Trade Pillar of the Indo-Pacific Economic Framework for Prosperity*, https://ustr.gov/sites/default/files/2022-09/IPEF%20Pillar%201%20Ministerial%20Text%20(Trade%20Pillar)_FOR%20PUBLIC%20RELEASE%20(1).pdf

[x] Office of the United States Trade Representative, *The Indo-Pacific Economic Framework for Prosperity: Biden-Harris Administration's Negotiating Goals for the Connected Economy (Trade) Pillar*, September 23, 2022, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2022/september/indo-pacific-economic-framework-prosperity-biden-harris-administrations-negotiating-goals-connected

[xi] Office of the United States Trade Representative, *Joint USTR and Department of Commerce Readout of the First Indo-Pacific Economic Framework Negotiating Round*, December 15, 2022, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2022/december/joint-ustr-and-department-commerce-readout-first-indo-pacific-economic-framework-negotiating-round; Office of the United States Trade Representative,

Joint *US Department of Commerce and USTR Readout from the Second Indo-Pacific Economic Framework Negotiating Round*, March 19, 2023, https://www.commerce.gov/news/press-releases/2023/03/joint-us-department-commerce-and-ustr-readout-second-indo-pacific

[xii] Anonymous, *Google, Amazon Lobbyists helped US shape new Indo-Pacific Trade Framework*, Communications Today, May 3, 2023, https://www.communicationstoday.co.in/google-amazon-lobbyists-helped-us-shape-new-indo-pacific-trade-framework/; Emily Birnbaum and Leah Nylen, *Google, Amazon Lobbyists Helped US Shape New Indo-Pacific Trade Framework*, Business Standard, May 2, 2023, https://www.business-standard.com/world-news/google-amazon-lobbyists-helped-us-shape-new-indo-pacific-trade-framework-123050201296_1.html; Elizabeth Warren, *Big Tech's Big Con: Rigging Digital Trade Rules to Block Anti-trust Regulation*, May 2023, https://www.warren.senate.gov/imo/media/doc/USTR%20REPORT.pdf

[xiii] Emily Birnbaum and Eric Martin, *Tech Giants Play Too Big a Role in US Indo-Pacific Trade Talks, Critics Say*, Bloomberg, July 10, 2023, https://www.bloomberg.com/news/articles/2023-07-10/critics-slam-lobbying-by-tech-giants-in-us-indo-pacific-trade-talks#xj4y7vzkg; Elizabeth Warren, *Big Tech's Big Con: Rigging Digital Trade Rules to Block Anti-trust Regulation*, May 2023, https://www.warren.senate.gov/imo/media/doc/USTR%20REPORT.pdf

[xiv] Emily Birnbaum and Eric Martin, *Tech Giants Play Too Big a Role in US Indo-Pacific Trade Talks, Critics Say*, Bloomberg, July 10, 2023, https://www.bloomberg.com/news/articles/2023-07-10/critics-slam-lobbying-by-tech-giants-in-us-indo-pacific-trade-talks#xj4y7vzkg

[xv] Microsoft, *Response to Office of US Trade Representative Request for Comments on the Proposed Fair and Resilient Trade Pillar of an Indo-Pacific Economic Framework and US Department of Commerce Request for Comments on the Indo-Pacific Economic Framework*, April 11, 2022, https://www.regulations.gov/comment/ITA-2022-0001-0034; Microsoft, *Indo-Pacific Economic Framework Consultation*, October 2022, https://www.dfat.gov.au/sites/default/files/ipef-submission-microsoft.pdf; and BSA, *Comments on Indo-Pacific Economic Framework Negotiations*, October 28, 2022, https://www.dfat.gov.au/sites/default/files/ipef-submission-bsa.pdf

[xvi] Daniel Rangel and Lori Wallach, *International Pre-emption by "Trade" Agreement: Big Tech's Ploy to Undermine Privacy, AI Accountability, and Anti-Monopoly Practices*, Rethink Trade, March 2023, https://rethinktrade.org/wp-content/uploads/2023/03/International-Preemption-by-Trade-Agreement.pdf; Jeanne Whalen, *Trump's USMCA delivers big wins to drugmakers, oil companies and tech firms*, The Washington Post, October 2, 2018, https://www.washingtonpost.com/business/economy/trumps-usmca-delivers-big-wins-to-drugmakers-oil-companies-and-tech-firms/2018/10/02/2d68ad10-c66f-11e8-b1ed-1d2d65b86d0c_story.html

[xvii] Sarah Grace Spurgin, *Public Submissions to US Government Reveal Corporate Wishlist for IPEF: More Power at Our Expense*, Public Citizen, May 20, 2022, https://www.citizen.org/news/public-submissions-to-u-s-government-reveal-corporate-wishlist-for-ipef-more-power-at-our-expense/

[xviii] US Chamber of Commerce, *The Digital Trade Revolution*: *How Workers and Companies Can Benefit from a Digital Trade Agreement*, February 2022, https://www.uschamber.com/assets/documents/Final-The-Digital-Trade-Revolution-February-2022_2022-02-09-202447_wovt.pdf

[xix] Google, *Comments regarding the Indo-Pacific Economic Framework*, April 11, 2022, https://www.regulations.gov/comment/ITA-2022-0001-0046

[xx] *IBM Statement on Launch of IPEF*, IBM, May 23, 2022, https://www.ibm.com/policy/ipef-gary-cohn/

[xxi] Emily Birnbaum and Eric Martin, *Tech Giants Play Too Big a Role in US Indo-Pacific Trade Talks, Critics Say*, Bloomberg, July 10, 2023, https://www.bloomberg.com/news/articles/2023-07-10/critics-slam-lobbying-by-tech-giants-in-us-indo-pacific-trade-talks#xj4y7vzkg

[xxii] Rishab Bailey and Smriti Parsheera, *Data Localisation in India: Questioning the Means and Ends*, NIPFP Working Paper No. 242, September 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3356617

[xxiii] M Giest, *Data Rules in Modern Trade Agreements: Towards Reconciling an Open Internet with Privacy and Security Safeguards*, in CIGI (ed), Special Report: Data Governance in the Digital Age, Waterloo, CIGI, 2018, *cf.* Patrick Leblond, *Uploading CPTPP and USMCA Provisions to the WTO's Digital Trade Negotiations Poses Challenges for National Data Regulation*, in Mira Burri (Ed), Big Data and Global Trade Law, Cambridge University Press, July 2021, https://www.cambridge.org/core/books/big-data-and-global-trade-law/uploading-cptpp-and-usmca-provisions-to-the-wtos-digital-trade-negotiations-poses-challenges-for-national-data-regulation/59483E5412CA936C31F6EBCF9CD97FDF

[xxiv] *Ibid.*

[xxv] *Ibid.*

[xxvi] Rashmi Banga, *Joint Statement Initiative on E-Commerce: Economic and Fiscal Implications for the South*, UNCTAD Research Paper No. 58, February 2021, https://www.twn.my/announcement/UNCTAD%20Re%20Paper%2058_022021.pdf; Patrick Leblond, *Uploading CPTPP and USMCA Provisions to the WTO's Digital Trade Negotiations Poses Challenge for National Data Regulation*, in Global Perspectives on Digital Trade Governance, Mira Burri (Ed)., Cambridge University Press, July 2021, https://www.cambridge.org/core/books/big-data-and-global-trade-law/uploading-cptpp-and-usmca-provisions-to-the-wtos-digital-trade-negotiations-poses-challenges-for-national-data-regulation/59483E5412CA936C31F6EBCF9CD97FDF

[xxvii] Yasmin Ismail, *E-Commerce Joint Statement Initiative Negotiations among World Trade Organisation Members: State of Play and the Impact of COVID-19*, IISD and CUTS International, 2021, https://www.iisd.org/system/files/2021-04/e-commerce-negotiations-wto-members-covid-19.pdf; European Parliament, *At a Glance: WTO Ecommerce Negotiations*, 2020, https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/659263/EPRS_ATA(2020)659263_EN.pdf

[xxviii] *Joint Statement on Electronic Commerce: EU Proposal for WTO Disciplines and Commitments relating to Electronic Commerce*, World Trade Organisation, April 26, 2019, https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=253698,253697,253696,253560,252791,252624,252622,252611,252627,252625&CurrentCatalogueIdIndex=0&FullTextHash=&HasEnglishRecord=True&HasFrenchRecord=True&HasSpanishRecord=True

[xxix] Daniel Rangel, *WTO General Exceptions: Trade Law's Faulty Ivory Tower,* Public Citizen, February 2022, https://www.citizen.org/wp-content/uploads/WTO-General-Exceptions-Paper_.pdf

[xxx] *Supra* Note xxiii.

[xxxi] *Supra* Note xxiii.

[xxxii] Daniel Rangel, *WTO General Exceptions: Trade Law's Faulty Ivory Tower,* Public Citizen, February 2022, https://www.citizen.org/wp-content/uploads/WTO-General-Exceptions-Paper_.pdf

[xxxiii] Patrick Leblond, *Uploading CPTPP and USMCA Provisions to the WTO's Digital Trade Negotiations Poses Challenges for National Data Regulation*, in Mira Burri (Ed), Big Data and Global Trade Law, Cambridge University Press, July 2021, https://www.cambridge.org/core/books/big-data-and-global-trade-law/uploading-cptpp-and-usmca-provisions-to-the-wtos-digital-trade-negotiations-poses-challenges-for-national-data-regulation/59483E5412CA936C31F6EBCF9CD97FDF

[xxxiv] My Health Records Act, 2012, https://www.legislation.gov.au/Details/C2021C00475

[xxxv] Government Regulation No. 71/2019, Concerning Implementation of Electronic Systems and Transactions, https://jdih.kominfo.go.id/produk_hukum/view/id/695/t/peraturan+pemerintah+nomor+71+tahun+2019+tanggal+10+oktober+2019; and Regulation on Protection of Personal Data in an Electronic System, 2016, https://www.dataguidance.com/sites/default/files/data_privacy_english_-_permenkominfo_no_20_of_2016.pdf

[xxxvi] *Supra* Note xxii.

[xxxvii] Data Privacy Act, 2012, https://privacy.gov.ph/data-privacy-act/

[xxxviii] Personal Data Protection Act, 2012, https://sso.agc.gov.sg/Act/PDPA2012; Personal Data Protection Regulations, 2021, https://sso.agc.gov.sg/SL/PDPA2012-S63-2021?DocDate=20210930

[xxxix] Soemadipradja and Taher, *Client Update: Technology, Media and Telecommunications Law*, November 2022, https://www.soemath.com/public/images/page/download1_485_Client%20Update%20-%20Indonesia%20Data%20Protection%20Law(2).pdf

[xl] Department of Home Affairs, *National Data Security Action Plan*, Government of Australia, December 2021, https://www.homeaffairs.gov.au/reports-and-pubs/files/data-security/nds-action-plan.pdf

[xli] Justin Hendry, *Tech Giants Rally Against Data Localisation in Australia,* InnovationAus, September 7, 2022, https://www.innovationaus.com/tech-giants-rally-against-data-localisation-in-australia/

[xlii] *Supra* Note xxiii.

[xliii] Melinda St Louis, *Opportunities and Challenges for Trade Policy in the Digital Economy*, Written Statement before Subcommittee on International Trade, Customs and Global Competitiveness, US Senate Finance Committee, US Congress, December 14, 2022, https://www.citizen.org/wp-content/uploads/Trade-Policy-in-Digital-Economy-Hearing-Public-Citizen-Statement-for-Record-Dec-14-2022.pdf; Rick Claypool and Cheyenne hunt, *Sorry in Advance: Rapid Rush to Deploy Generative AI Risks a Wide Array of Automated Harms*, April 18, 2023, https://www.citizen.org/article/sorry-in-advance-generative-ai-artificial-intellligence-chatgpt-report/

[xliv] Digital Trade Alliance, *Source Code Disclosure and Trade Agreements*, Augusts 2023, https://dtalliance.org/wp-content/uploads/2023/08/Source-Code-and-Free-Trade-Agreements.pdf?utm_source=substack&utm_medium=email

[xlv] OECD AI Observatory, *OECD AI Principles Overview*, https://oecd.ai/en/ai-principles

[xlvi] White House, *Blueprint for an AI Bill of Rights*, https://www.whitehouse.gov/ostp/ai-bill-of-rights/

[xlvii] Competition and Markets Authority, *Algorithms: How they can reduce competition and harm consumers*, 2021,https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/954331/Algorithms_++.pdf

[xlviii] OECD, *Algorithmic Competition: OECD Competition Policy Roundtable Background Note,* 2023, https://www.oecd.org/daf/competition/algorithmic-competition-2023.pdf

[xlix] *Supra* Note xxiii.

[l] Josh Lee Kok Thong, *AI Verify: Singapore's AI Governance Testing Initiative Explained,* Future of Privacy Forum, June 6, 2023, https://fpf.org/blog/ai-verify-singapores-ai-governance-testing-initiative-explained/

[li] Department of Industry, Science and Resources, *Australia's AI Ethics Principles,* Government of Australia, https://www.industry.gov.au/publications/australias-artificial-intelligence-ethics-framework/australias-ai-ethics-principles

[lii] Department of Trade and Industry, *National AI Strategy for the Philippines*, Government of Philippines, 2021, https://innovate.dti.gov.ph/wp-content/uploads/2021/05/National-AI-Strategy-Roadmap-May-2021.pdf

[liii] NITI Aayog, *Responsible AI #AIFORALL Approach Document for India*, Government of India, February 2021, https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf

[liv] *Ibid.*

[lv] Asia AI News, *Indonesia National AI Strategy Published this Month*, Medium.com, August 21, 2020, https://medium.com/@asiaainews/indonesia-national-ai-strategy-published-this-month-6eaeb3d76224#:~:text=Stranas%20KA%20aims%20to%20tie,governance%20and%20technology%20development%20strategy.

[lvi] Department of Industry, Science and Resources, *Safe and Responsible AI in Australia: Discussion paper*, Government of Australia, June 2023, https://storage.googleapis.com/converlens-au-industry/industry/p/prj2452c8e24d7a400c72429/public_assets/Safe-and-responsible-AI-in-Australia.pdf

[lvii] Government of Australia, *Response to the House of Representatives Select Committee on Social Media and Online Safety Report*, March 2023, https://www.infrastructure.gov.au/sites/default/files/documents/australian-gov-response-to-house-of-reps-select-committee-on-social-media-and-online-safety-report-march2023.pdf

[lviii] Ministry of Electronics and Information Technology, *Proposed Digital India Act, 2023*, Digital India Dialogues, Bangalore, March 9, 2023, https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf

[lix] Elina Noor and Mark Bryan Manatan, *Raising Standards: Data and Artificial Intelligence in Southeast Asia*, Asia Society Policy Institute, July 2022, https://asiasociety.org/sites/default/files/inline-files/ASPI_RaisingStandards_report_fin_web_0.pdf

[lx] Nilesh Christopher, *A tiny tweak to Zomato's algorithm led to lost delivery riders, stolen bikes and missed wages*, Rest of World, October 7, 2021, https://restofworld.org/2021/how-a-small-change-to-zomatos-algorithm-created-havoc-for-delivery-riders/, Nilesh Christopher, *India: Delivery riders protest after algorithm tweak of food delivery platform led riders exposed to crime and missing wages*, Business and Human Rights Resource Centre, https://www.business-humanrights.org/en/latest-news/india-algorithm-tweak-of-food-delivery-platform-led-to-lost-delivery-riders-stolen-bikes-and-missed-wages/; Varsha Bansal, *Gig workers in India are uniting to take back control from algorithms*, Rest of World, November 14, 2022, https://restofworld.org/2022/gig-workers-in-india-take-back-control-from-algorithms/

[lxi] Billy Perrigo, *Big Tech is Already Lobbying to Water Down Europe's AI Rules*, Time, April 21, 2023, https://time.com/6273694/ai-regulation-europe/; Camille Shyns, *The Lobbying Ghost in the Machine: Big Tech's Covert Defanging of Europe's AI Act*, Corporate Europe Observatory, February 223, https://corporateeurope.org/en/2023/02/lobbying-ghost-machine

[lxii] Rishab Bailey, Smriti Parsheera and Faiza Rahman, *Comments on the (Draft) Information Technology [Intermediary Guidelines (Amendment) Rules, 2018,* January 31, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3328401

[lxiii] T Prashanth Reddy, *Back to the Drawing Board: What Should be the New Direction of the Intermediary Liability Law?*, NLUD Journal of Legal Studies, Volume 1, 2019, https://nludslj.webs.com/Prashant%20reddy.pdf

[lxiv] Network Enforcement Act, https://germanlawarchive.iuscomp.org/?p=1245

[lxv] Ashley Johnson and Daneil Castro, *How Other Countries have Dealt With Intermediary Liability*, ITIF, February 22, 2021, https://itif.org/publications/2021/02/22/how-other-countries-have-dealt-intermediary-liability/

[lxvi] John McKinnon and Brody Mullins, *Nancy Pelosi Pushes to Remove Legal Protections for Online Content in Trade Pact*, Wall Street Journal, December 4, 2019, https://www.wsj.com/articles/nancy-pelosi-pushes-to-remove-legal-protections-for-online-content-in-trade-pact-11575503157 and Taylor Hatmaker, *Nancy Pelosi warns tech companies that Section 230 'is in jeopardy',* Tech Crunch, April 13, 2019, https://tinyurl.com/23p7pt67