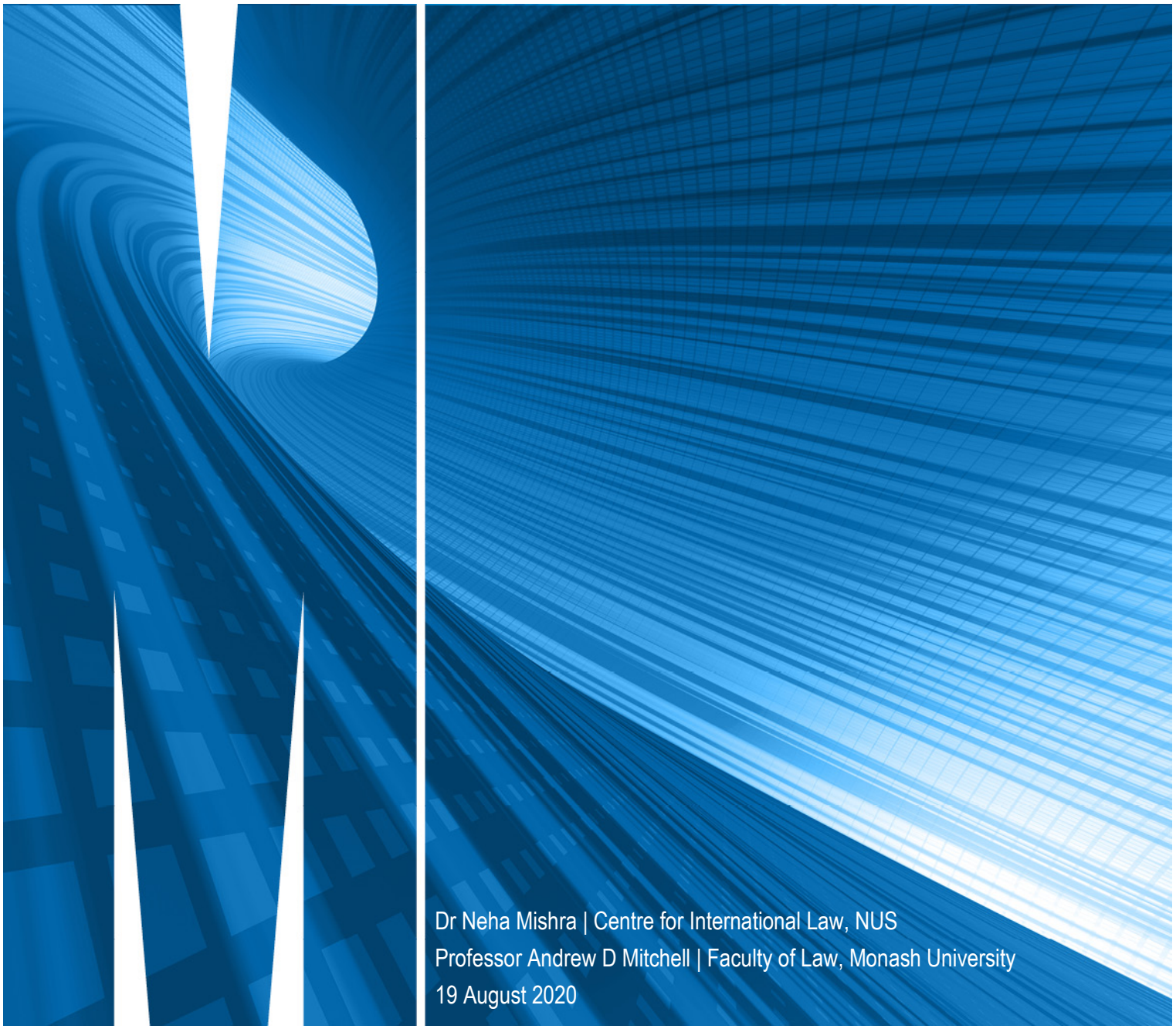
MONASH University

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

Future of Digital Trade Rules Consultation



Dr Neha Mishra | Centre for International Law, NUS
Professor Andrew D Mitchell | Faculty of Law, Monash University
19 August 2020

MONASH University

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

CONTENTS

DISCLOSURE AND ACKNOWLEDGEMENTS

This submission arises from independent research and contains the authors' own views as academics. It does not necessarily reflect the views of any past or current employer or other entity.

EXECUTIVE SUMMARY

This submission provides our views on three areas of digital trade relevant to international trade agreements:

(1) **Addressing data-related trade barriers**: Given the central role of cross-border data flows in the global economy, we are of the view that future digital trade agreements must contain provisions allowing free cross-border data flows across all service sectors and also prohibiting data localisation. These provisions must be subject to clear exceptions allowing data restrictions or localisation requirements for achieving legitimate domestic regulatory objectives, and drawing carve-outs for highly sensitive sectors, as and when necessary. Further, trade rules on data flows must be complemented by other disciplines that promote digital trust. For instance, all parties to digital trade agreements must adopt basic frameworks on data protection and privacy consistent with recognised international standards and encourage the use of mutual recognition mechanisms (eg, privacy trustmarks) for enabling cross-border data flows. Additionally, digital trade agreements must require all parties to adopt a framework on online consumer protection, with reference to relevant international frameworks developed by the UN, OECD, and other transnational bodies.

(2) **Dealing with cybersecurity and national security concerns**: In our view, future digital trade agreements must contain stronger disciplines on international cybersecurity cooperation and provide greater recognition to multi-stakeholder and market-driven cybersecurity standards to facilitate the widespread adoption of competitive and robust standards on cybersecurity. Instead of unilaterally imposing highly restrictive cybersecurity measures, especially on the grounds of national security, countries must engage meaningfully and transparently in diplomatic and policy dialogues outside trade institutions to foster stronger international consensus on dealing with conflicts over cybersecurity-related issues.

(3) **Digital development and inclusion:** Digital development and inclusion is essential to promote digital trade within Australian as well as regionally and globally. Therefore, in our view, in addition to promoting digital development and inclusion domestically to support and enable digitally excluded communities, Australia must take a stronger leadership role in promoting digital development and inclusion in the Asia-Pacific by providing greater technical assistance and capacity building support to digitally less developed countries.

In pursuing reforms of digital trade rules at the WTO and through FTAs, we believe that Australia can benefit by adopting a three-pronged strategy: (1) pushing for forward-looking rules on digital trade that are principles-based and technology neutral; (2) engaging proactively in dialogues on global cybersecurity and privacy norms, standards, and best practices in relevant international and multi-stakeholder bodies that can complement digital trade rules; and (3) ensuring that digital trade rules support an interoperable and unfragmented internet as this is an essential requirement for the sustainable growth of digital trade.

BACKGROUND

Digital trade has expanded rapidly to include not only e-commerce or the 'production, distribution, marketing, sale or delivery of goods and services by electronic means' (as defined by the World Trade Organization ('WTO')), but also a wide variety of economic activities underlying the digital economy. These developments have inspired several 'modern' international trade agreements, which contain comprehensive chapters on digital trade (eg, *Comprehensive and Progressive Agreement for Trans-Pacific Partnership* ('CPTPP') and *United States – Mexico – Canada Agreement* ('USMCA')). These comprehensive digital trade chapters can be contrasted with the more basic 'Electronic Commerce' Chapters found in the Free Trade Agreements ('FTAs') of the early 2000s. In August 2020, Australia signed the *Singapore – Australia Digital Economy Agreement* ('SADEA') which replaces the Electronic Commerce Chapter of the Singapore – Australia FTA. Another recent example of a 'digital economy' agreement is the *Digital Economic Partnership Agreement* ('DEPA'), signed by Singapore, Chile, and New Zealand in June 2020.

We welcome the various efforts of the Australian government in proactively promoting the domestic and global digital economy. At the domestic level, the Australian government has adopted a whole-of-government approach encompassing a vast range of issues including promoting digital innovation and competition, internet governance, internet trust and consumer protection, and supporting Australian businesses especially micro, small and medium enterprises ('MSMEs'). At an international level, Australia has negotiated 14 FTAs with comprehensive electronic commerce chapters, including the megaregional trade agreement, CPTPP. These agreements will play a key role in reducing digital trade barriers and promoting digital trade liberalisation. Australia has also been successfully leading the Joint Statement Initiative ('JSI') on Electronic Commerce at the WTO. Further, the Australian International Cyber-Engagement Strategy has been devised taking into account the complex relationship of the economic, political, social, and technological aspects of the internet-driven world. In our view, consolidating domestic efforts across different areas of digital trade and data and internet regulation, and a coherent, unified international strategy on digital trade and internet governance, are both essential to promote Australian interests in the global digital economy.

In this submission, we provide inputs on three issues that can inform Australia's position in the WTO and FTA negotiations on digital trade:

(1) addressing data-related trade barriers through international trade agreements;

(2) cybersecurity and national security concerns in digital trade; and

(3) digital development and inclusion for promoting digital trade.

We then provide our inputs on the role that Australia can play in influencing the future of digital trade rules. This submission draws from our research on digital trade, listed in Annex A.

ADDRESSING DATA-RELATED TRADE BARRIERS IN INTERNATIONAL TRADE AGREEMENTS

CROSS-BORDER DATA FLOWS

Data Flows are Critical

Data flows lie at the heart of digital trade. Even the most routine transactions on the internet require a complex web of data moving across different digital platforms and media. A general consensus exists in the international community that data flows are essential for promoting digital innovation, consumer well-being and choice, and enabling economic growth. Therefore, the debate on cross-border data flows, especially data localisation, has taken centre place in the WTO and several FTA negotiations. The issue of cross-border data flows relates to several other complex public policy concerns such as privacy protection, cybersecurity, digital trust concerns and, increasingly, national security and digital sovereignty.

Horizontal Obligations with Clear Exceptions

To promote liberalisation of digital trade, we are of the view that the WTO Members must consider adopting horizontal obligations (i.e. across all service sectors) allowing cross-border data flows and prohibiting data localisation measures. These obligations must be subject qualified by clear exceptions allowing data restrictions or localisation requirements for achieving legitimate domestic regulatory objectives. While some experts argue that the *General Agreement on Trade in Services* ('GATS') clearly applies to several restricting cross-border data flows (eg, data localisation measures), we believe that the uncertainty regarding the classification of modern-day digital services under GATS creates a high degree of legal uncertainty.

Revised CPTPP Model

In developing new WTO rules on cross-border data flows, the CPTPP is an important reference point. We believe that CPTPP art 14.11 (Cross-Border Transfer of Information by Electronic Means) and art 14.13 (Location of Computing Facilities) are good model provisions, but we suggest three modifications for future WTO rules:

(i) providing an illustrative list of policy objectives that qualify as 'legitimate' to ensure more legal certainty;

(ii) clarifying that the existing general and security exceptions in WTO law remain applicable;

(iii) ensuring that the obligations apply horizontally, with possible carve-outs for highly sensitive sectors.

However, such provisions can also raise concerns among countries regarding the loss of their regulatory space; the available exceptions (even when clear and reasonable) may not be sufficient to allay those concerns. We, therefore, suggest reforms in international trade rules to incorporate more meaningful provisions in other areas such as privacy protection and digital trust in international trade agreements. However, we do not think that the WTO or any other trade institution can or should set standards or determine benchmarks on

internet policy issues, but rather can adopt rules incorporating relevant internationally recognised norms and standards by reference.

PRIVACY PROTECTION

Different Approaches to Privacy Creates Challenges for Trade

Privacy protection and digital trade share a difficult relationship. While a minimum level of privacy protection is essential to establish and enhance trust in digital trade, different approaches to privacy protection across countries often create trade barriers. In particular, privacy frameworks pose challenges to cross-border data flows of personal data. For example, in the context of the European Union ('EU'), the recent *Schrems II* decision not only invalidates the *EU-US Privacy Shield*, but also adds new uncertainties regarding the validity of Standard Contractual Clauses and Binding Corporate Rules, standard procedures used by companies all over the world to transfer data out of the EU (including Australian companies). This approach is in contrast to the relatively open nature of cross-border data flows supported by countries such as Japan, Australia, Hong Kong, Korea, Singapore and the US. For example, the data privacy certification system provided by the Cross-Border Privacy Rules System ('CBPR') at Asia-Pacific Economic Cooperation ('APEC') can be utilised by companies from nine APEC members, including Australia.

Privacy Trustmarks and Data Certification Mechanisms

Privacy trustmarks and data certification mechanisms can play a critical role in enabling digital trade and cross-border data flows. For instance, while negotiating the EU-Australia FTA, Australia should consider the continuity of Australia – EU data flows, especially since Australia has failed so far to achieve an adequacy finding from the European Commission. In this regard, Australia can explore adopting provisions in the FTA recognising data protection trustmarks or other certification mechanisms that are mutually recognised by both Australia and the EU. Such data certification mechanisms are feasible under the General Data Protection Regulation ('GDPR') (art 46(2) and art 42) but remain unexplored. The compatibility of the mechanisms available under the GDPR and the APEC CBPR could also be further explored. Further, Australia should promote stronger recognition of APEC CBPR in its FTAs, especially with APEC members, something visibly missing in the CPTPP (USMCA art 19.8.6 provides that the parties 'recognize that the APEC CBPR is a valid mechanism to facilitate cross-border information transfers while protecting personal information'). Finally, the use of mutual recognition mechanisms (eg, data trustmarks) is supported by GATS art VII. It has also been included in some existing Australian FTAs in the context of provisions on personal information protection. Therefore, Australia may also consider introducing a relevant provision in the WTO JSI negotiations.

Facilitating a Basic Framework to Address Digital Trust Concerns

International trade agreements can facilitate a basic framework on privacy/data protection and online consumer protection to enable more trust in the digital ecosystem. This means that international trade agreements could incorporate relevant international standards on privacy and online consumer protection by reference. As discussed earlier, a clear divide exists regarding the appropriate benchmark for privacy and data

protection with some countries supporting the APEC or Organisation for Economic Cooperation and Development ('OECD') Privacy Frameworks, while others preferring a GDPR-like approach. Recent years have also seen the rise of information security laws aimed at data protection in countries such as China and Vietnam. We believe that the most reasonable option (especially at the WTO, where the divide is glaring given the wide membership at the JSI initiative) is to require countries to adopt a basic privacy framework consistent with the principles and guidelines of relevant international bodies, including transnational bodies such as the Global Privacy Assembly. Such an open provision will enable participating countries to continuously discuss and accommodate evolving norms in the global data privacy and data protection framework. This approach has been followed in some Australian FTAs. In FTAs negotiated with like-minded partners, Australia could however also agree upon a common framework such as the OECD Privacy Guidelines.

Low levels of cross-border trust also arise from divergence or absence of adequate online consumer protection laws in foreign markets, resulting in reduced export opportunities especially for MSMEs and loss of revenue for e-commerce platforms, logistics services, and e-payment service providers. We recommend that international trade agreements must contain obligations requiring all parties to adopt a basic framework and establish a mandatory cooperation mechanism for online consumer protection. In this regard, recognising the international convergence on online consumer protection in other fora is also important, for example, under the UN, OECD, and International Competition Network. The SADEA recognises the possibility of using alternative dispute resolution for e-commerce services, which could include dispute resolution mechanisms provided by e-commerce platforms. Especially, in data-driven sectors, Australia must continue to incentivise provisions in FTAs that facilitate the adoption of robust frameworks on privacy and online consumer protection to ensure that digital services provided within Australia comply with the Australian Trust Principles developed by the Australian Data and Digital Council.

CYBERSECURITY, NATIONAL SECURITY AND DIGITAL TRADE

STRENGTHEN INTERNATIONAL CYBERSECURITY COOPERATION

Several international trade agreements treat cybersecurity as a side-issue and include weak provisions on international cooperation on cybersecurity. We are of the view that these provisions must be strengthened, and an established mechanism in FTAs should enable international cybersecurity cooperation. Especially concerning the development of cybersecurity frameworks and standards, governments must proactively work alongside the private sector, especially given their predominant role in devising and implementing cybersecurity standards and solutions.

USE CYBERSECURITY STANDARDS RATHER THAN UNILATERAL MEASURES

International trade agreements must encourage countries to adopt international cybersecurity standards and best practices rather than unilateral measures. For instance, concerns have already been raised at the WTO regarding the imposition of domestic standards in the Chinese and Vietnamese cybersecurity laws. Research has also indicated the adverse security implications of indigenous cybersecurity standards, especially when they are not transparent and interoperable with global standards. However, to date, most FTAs remain largely silent on this issue. Further, cybersecurity standards for digital services developed by multi-stakeholder internet institutions and private industry bodies are unlikely to recognised under GATS (art VI:5 read with art VI:4; only standards developed by traditional multilateral institutions fall within the scope of GATS art VI).

ENCOURAGE THE DEVELOPMENT OF INTERNATIONAL CYBERSECURITY STANDARDS

In light of the weak international consensus on cybersecurity standards, we believe that Australia must continue to proactively engage in the development of internationally competitive and transparent cybersecurity standards in all relevant international and multi-stakeholder fora. The Australian International Cyber Engagement Strategy recognises the importance of internationally competitive and innovative cybersecurity standards. A stronger consensus in the international community on standard-setting will eventually facilitate the adoption of provisions in international trade agreements recognising a broader range of internationally competitive and market-relevant transnational and multi-stakeholder cybersecurity standards.

DISCOURAGE MISUSE OF THE NATIONAL SECURITY EXCEPTION

Recent years have seen a change in the relationship between economics and public/national security in the context of digital trade. Several governments now impose measures restricting digital applications and products on the grounds that it is necessary for national security. Some governments also argue that these restrictions qualify under the security exception. In our view, the security exception available in WTO treaties and FTAs applies only in very limited circumstances. Further, recent WTO panel reports have also clarified that these exceptions are not entirely self-judging; rather, the Panel can objectively examine if the measure relates to specific circumstances listed in the exception and that the measure is implemented in good faith.

Therefore, the majority of such measures will not satisfy the threshold under GATT art XX or GATS art XIVbis or equivalent provisions in FTAs as they affect day-to-day commercial transactions. These exceptions may be available when cyber-weapons are used in a war or where a cyber-attack can be considered to be equivalent to a 'war' or 'emergency in international relations'. However, the lack of international consensus on this subject is likely to cause uncertainty, if and when countries chose to evoke the security exceptions to defend their restrictions on digital trade.

Australia can partner with like-minded trading partners at the WTO and other relevant for a to advocate that the security exception must not be invoked to address commercial threats in digital trade and reserved for use in exceptional cases in compliance with the principle of good faith. Further, as discussed earlier, Australia can also seek stronger cooperation mechanism for cybersecurity governance (through FTAs or otherwise) to contain commercial threats (e.g. data breaches) as well as resolve cybersecurity-related disputes. Nonetheless, protecting critical sectors such as defence and public health (especially during the ongoing pandemic) from advanced persistent threats, malware attacks, etc. remains necessary and judicious.

ENGAGING IN DIALOGUES OUTSIDE TRADE BODIES

The relationship between national security, cybersecurity and digital trade is undoubtedly becoming complex, especially as foreign interference through digital products and services becomes easier. In this regard, Australia must proactively engage in cybersecurity dialogues outside trade bodies, especially in the UN. In our view, Australia must also support timely and relevant norm entrepreneurship by the private sector such as the Cybersecurity Tech Accord and the Charter of Trust for a Secure Digital World. Australia is already a supporter of the multi-stakeholder declaration, Paris Call for Trust and Security in Cyberspace. Domestically, co-regulation initiatives and aligning with the private sector could pave the path for more regulatory and industry sandboxes to test the security impact of new technologies for digital trade.

DIGITAL DEVELOPMENT AND INCLUSION INITIATIVES

ENHANCE DIGITAL EDUCATION AND SKILLS NATIONALLY

Digital development and inclusion remain essential to promote digital trade within Australian as well as regionally and globally. The Australian Digital Inclusion Index indicates a digital divide within Australia, primarily due to differing income and education levels. Further, factors such as age, gender, geography, and cultural background also affect digital inclusion. These factors also impede the development of digital entrepreneurship initiatives by people coming from disadvantaged backgrounds or communities. To strengthen its position on digital trade, the Australian government should foster initiatives to enhance digital education and skills within the country and continue providing adequate support to MSMEs.

PROMOTE DIGITAL DEVELOPMENT AND INCLUSION INTERNATIONALLY

Australia can also be an important leader in promoting digital development and inclusion regionally and globally. Most FTAs have weak provisions (if at all) on digital development and inclusion (including FTAs between developed and developing countries). Digital inclusion must be viewed not only as a moral imperative (for eg, for achieving the Sustainable Development Goals), but also as being essential for improving opportunities for Australian businesses in the region, especially in the Asia-Pacific. For instance, Australia can play an important role in promoting digital development and inclusion in the developing countries of the Asian region by providing technical assistance and capacity-building support to developing countries and Least Developed Countries. Similarly, in addition to FTAs, Australia can also promote other regional initiatives with ASEAN and APEC to improve digital connectivity and digital adaptation in the Asia-Pacific region. Given that these issues are relatively uncontroversial, achieving consensus remains likely, including in the WTO JSI discussions.

ROLE OF AUSTRALIA IN SHAPING FUTURE DIGITAL TRADE RULES

Digital trade stands at a critical juncture. While it remains important to promote digital innovation and economic opportunities (especially for economic stability during the Covid-19 pandemic), the policy and technology risks associated with digital and data-driven technologies services are also increasing rapidly. Further, due to the unpredictable nature of digital innovation, digital trade rules must remain future-forward i.e. relevant to future technologies such as Artificial Intelligence, Internet of Things, and digital currencies. It also remains essential that Australia can balance conflicting geopolitical interests in digital trade in the Asia-Pacific region and beyond. To counter such conflicts, Australia can consolidate its position by negotiating comprehensive and deeper chapters on digital trade such as the recent SADEA with other like-minded and trusted partners. However, such high-quality agreements may be challenging to negotiate with digitally less developed countries as they often do not have the required regulatory frameworks and resources to support digital trade. Therefore, the JSI negotiations remain critical for advancing Australian interests in digital trade at the global level. Australia must also continue using multiple fora in representing and advocating for digital trade liberalisation such as the G20, OECD and APEC. We discuss three ideas below that can shape Australia's role in its FTA and WTO negotiations on digital trade:

(1) pushing for forward-looking rules on digital trade;

(2) promoting global cybersecurity and privacy norms that complement FTAs and WTO law; and

(3) aligning trade rules with an interoperable and unfragmented internet.

FUTURE FORWARD RULES ON DIGITAL TRADE

In our view, the recently signed SADEA marks an important change in Australian strategy towards digital trade in FTAs. We welcome the holistic initiatives in this agreement, including new provisions relevant to the digital economy not found in other Australian FTAs on electronic invoicing, online safety, data innovation and regulatory sandboxes, electronic payments, artificial intelligence, open government data and digital identities. Australia must continue entering into such comprehensive agreements with like-minded trading partners, as long as it can continue to protect its economic and policy interests. Where such agreements are negotiated with developing countries, Australia must include provisions facilitating digital development and inclusion (especially providing assistance to develop domestic regulatory frameworks), incorporating adequate digital trade facilitation measures, and boosting prospects for meaningful regulatory cooperation. In order to ensure that digital trade rules continue to be future-forward, Australia must also encourage a principles-based and technology-neutral approach in regulating digital trade to the greatest extent possible. Cross-border data flows is at the heart of competitiveness in digital economy. Thus, while negotiating future FTAs, Australia must facilitate the use of APEC CBPR and other data trustmarks/certifications and promote the free flow of data.

PROMOTING GLOBAL PRIVACY AND CYBERSECURITY NORMS

The development of privacy and cybersecurity norms primarily happens outside trade institutions in international/regional organisations such as the UN, OECD, APEC, International Telecommunications Union, and G20, and other multi-stakeholder and transnational organisations such as Global Privacy Assembly, International Competition Network, and Internet Governance Forum. However, these norms also play a vital role in creating a trustworthy environment for digital trade. Therefore, we are of the view that Australia must advocate for global privacy and cybersecurity standards that complement their FTAs and WTO law in all relevant fora. Some of the relevant issues related to privacy and cybersecurity are topical (eg, regulating digital surveillance during Covid-19). In contrast, others are broader (eg, standard-setting for privacy-enhancing technologies and security-by-design). Further, Australia must pay close attention to relevant developments outside state-based institutions in evolving policy areas such as AI ethics and IoT security. Another important multi-stakeholder initiative is the Blue Dot Network, established to develop shared standards for global infrastructure development, including digital infrastructure.

Finally, we recommend that establishing a single coordination body under PTAs will help reach a consensus among parties on relevant international standards and best practices in different aspects of digital trade, as well as evaluate and modify digital trade agreements from time to time. A committee on electronic commerce can play a similar role in the WTO.

ALIGNING TRADE RULES WITH AN INTEROPERABLE AND UNFRAGMENTED INTERNET

Australia must take a leadership role in promoting trade rules that promote an interoperable and unfragmented internet, especially in light of the growing geopolitical tensions in digital trade. An open, interconnected internet is essential for digital trade. Especially for open economies such as Australia, digital isolation is counterproductive. In addition to advocating cross-border data flows in FTAs and JSI negotiations, Australia must also focus on encouraging global standard-setting in digital trade and developing domestic regulatory disciplines on e-commerce. Several Australian FTAs already strive to balance digital trade liberalisation with the domestic policy space essential to regulate the digital sector. The SADEA, in particular, provides clear exceptions for restricting cross-border data flows, which can be instrumental in promoting an interoperable and unfragmented internet.

Unfortunately, most trade rules do not provide sufficient avenues for participation by or collaboration with multi-stakeholder and internet technical bodies. However, given the central role of these bodies in devising protocols and standards of the internet, trade institutions must learn from their expertise, whether at the stage of negotiating new digital trade rules or implementing them. Therefore, Australia should play an active role in relevant multi-stakeholder internet dialogues to remain abreast of policy developments on internet governance and regulation of data-driven technologies, including by inviting experts to provide their inputs on relevant issues, as and when required. This expertise can also be instrumental in deciding complex digital trade disputes likely to arise in the coming years.

APPENDIX A - RESEARCH ON DIGITAL TRADE

Neha Mishra and Andrew Mitchell, 'Understanding the Role of International Investment Agreements in the Digital Economy' (forthcoming, 2021).

Neha Mishra, 'When International Trade Law Meets Data Ethics: A Brave New World', *NYU Journal of International Law & Policy* (Vol 53:2, 2021 (Forthcoming)).

Andrew Mitchell and Neha Mishra, 'Digital Trade Integration in Preferential Trade Agreements' *UNESCAP ARTNeT Working Paper Series*, no. 191 (2020).

Neha Mishra, 'Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation?' (2020) 19(3) *World Trade Review* 341-364.

Neha Mishra, 'The Trade -(Cyber)security Dilemma and its Impact on Global Cybersecurity Governance', (2020) 54(4) *Journal of World Trade* 567-590.

Andrew Mitchell, Tania Voon and Jarrod Hepburn, 'Taxing Tech: Risks of an Australian Digital Services Tax under International Economic Law' (2019) 20(1) *Melbourne Journal of International Law* 88–124.

Andrew Mitchell and Neha Mishra, 'Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute' (2019) 22(3) *Journal of International Economic Law* 389–416.

Neha Mishra, 'Building Bridges: International Trade Law, Internet Governance and the Regulation of Data Flows' (2019) 52(2) *Vanderbilt Journal of Transnational Law* 463-509.

Andrew Mitchell and Neha Mishra, 'Data at the Docks: Modernising International Trade Law for the Digital Economy' (2018) 20(4) *Vanderbilt Journal of Entertainment & Technology Law* 1073–1134.

Andrew Mitchell and Neha Mishra, 'International Trade Law Perspectives on Paperless Trade and Inclusive Digital Trade', *UNESCAP ARTNeT Working Paper Series*, No. 170 (2017).

Neha Mishra, 'The Role of the Trans-Pacific Partnership in the Internet Ecosystem' (2017) 20(1) *Journal of International Economic Law* 31-60.

Andrew Mitchell and Jarrod Hepburn, 'Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer' (2017) 19 *Yale Journal of Law & Technology* 182-236.

MONASH University

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

Further information

Dr Neha Mishra
Postdoctoral Fellow
Centre for International Law
National University of Singapore
469A Bukit Timah Road, Tower Block, #09-01
Singapore 259770

T: +65 8297 5403
E: cilnm@nus.edu.sg; mishra.neha@gmail.com

cil.nus.edu.sg

Professor Andrew D Mitchell
Faculty of Law
Monash University
Wellington Road
Clayton, Victoria 3800
Australia

T: +61 3 9905 3086
E: andrew.mitchell@monash.edu

monash.edu.au

CRICOS provider: Monash University 00008C