New Zealand Creative Sector Submission to MFAT
Digital Economic Partnership Agreement Negotiation

This submission is made on behalf of WeCreate, whose members are listed on the WeCreate website, https://wecreate.org.nz/about-us/members/ In addition to our members we have a number of *Friends* that are businesses operating in the creative sector. WeCreate is the alliance of New Zealand's creative sector organisations and industries, incorporating over 25,000 members. Our mission is to catalyse the growth of the sector, advance its collaboration with other sectors and serve as the interaction point for Government to maximise the opportunities our creativity offers.

2 WeCreate appreciates the opportunity to be consulted on New Zealand's participation in the Digital Economy Partnership Agreement (DEPA) negotiations with Singapore and Chile. This submission focuses on cross-sectoral and general policy issues. It has been informed by engagement with the creative sector including, *inter alia*, at the 2017 and 2018 'Creative Economy Conversations' and at the 2019 'Creative Economy Digital Trade Conversation' as well as specifically in the preparation of this submission. Individual members of WeCreate may have different views on specific issues.

Summary

3 The New Zealand creative economy is increasingly dependent on, and benefits hugely from, digital technology. Digital trade – through digital channels including streaming, downloads, platforms, and licensing of digital content – and digital enablers including the digitisation of services and production, mean that there is potential for a substantial expansion in creative economy exports from New Zealand. This would generate benefits for New Zealand including an increase in export revenue and a contribution to enhanced productivity and broader competitiveness for the economy.

4 However, as is the case for other export sectors, creative economy exporters are increasingly challenged by measures in the global digital regulatory environment that add costs or difficulty to cross-border activity. WeCreate accordingly welcomes the efforts by the New Zealand Government to secure a trade-friendly "global digital marketplace", including through the WTO e-commerce negotiations and in its DEPA negotiations with Singapore and Chile. While New Zealand creative exporters have not encountered significant trade barriers in relation to exports to the latter markets, we strongly support the efforts of these three small, open, globally-oriented economies to develop a pathfinder towards a more trade-friendly digital trade environment around the world.

4 WeCreate considers that in the DEPA negotiations, New Zealand negotiators could usefully emphasise trade-friendly approaches in the following areas:

- Services trade barriers, including around cross-border financial services;
- Challenges in relation to the dominant position of platforms;
- Barriers and restrictions in relation to cross-border data flows, including compliance costs in relation to privacy regulations and local presence;
- Challenges in relation to the protection of intellectual property rights and online piracy;
- and overall, a streamlining of global regulatory approaches to digital trade, to minimise the creation of a "digital noodle bowl" of divergent or conflicting approaches.

Submission

3 Creativity is in New Zealand's DNA: we benefit from a powerful combination of unique stories, culture and values; highly-skilled creative people; a long tradition of innovative approaches, and a ready embrace of modern technologies – all of which enables us to unlock and share our creativity more broadly, including offshore. The "creative economy" spans a wide range of sectors, including publishing, recorded music, art, design, architecture and fashion, videogaming, artificial reality and virtual reality, screen, advertising and other segments. These sectors can be a powerful engine for broader New Zealand economic growth. Creative industries generate revenue themselves as well as acting as a multiplier in other sectors, helping to generate broader economic gains in terms of productivity, international competitiveness and enabling innovative new business models. The Ministry for Business, Innovation and Employment has estimated that digital goods and services are already the third-largest New Zealand export sector, and that productivity improvements in the sector have a multiplier effect on New Zealand's GDP.[1]

4 The advent of digital and telecommunications technology has meant that the way that creative content is produced, distributed and consumed has been completely transformed over the last two decades – not just in New Zealand, but globally. In many cases, creative sectors have become digitised from end to end, with some industries such as videogaming "born global", while others such as screen, music and publishing transformed through digital production, editing and distribution. The creative sector generates revenue through multiple global digital channels (streaming, downloads, other online services), e-commerce platforms, performance rights (broadcasting), licensing of digital content, goods and services and direct sales. In large part, this trade is 'weightless', helping to contribute to the transition of New Zealand to a more sustainable, low-carbon economy.

5 The digital revolution has also helped to unlock the potential of creative small businesses – the vast majority of this sector in New Zealand – to participate in cross-border trade at lower cost and with broader reach in a way that was not possible before. Physical creative exports traditionally relied on securing international distributors, territory-by-territory releases, and deep pockets to finance high legal, marketing and distribution costs. By contrast, digital creative exports can have global reach from Day One, opening up new opportunities for smaller or independent creators in a wider of markets and consumers, and enabling rapid growth. Digitisation can lower costs and help keep content more secure. It can also unlock vertical integration (notably in the gaming sector) and the potential for value-added 'spinoff' products.

6 The global appetite for creative content is growing as the number and reach of disruptive entertainment platforms increases.[2] New Zealand creative exports enjoy growing demand in large emerging markets such as India, China, South-East Asia and the Middle East. In addition to direct exports, there are also opportunities for co-production with international producers and for supplying our creative expertise and services as part of international value chains. New Zealand, as a small but sophisticated and wealthy market, can also serve as a useful 'test-bed' for global content (for example, the Pokemon Go Harry Potter app was tested here).

The Digital Economic Partnership Agreement

7 New Zealand creative economy exporters have not to date encountered significant challenges or barriers to creative digital exports to Singapore or Chile. This no doubt reflects the general openness of these economies to digital trade, as is reflected in their very high rankings in the

[1] Ministry of Business, Innovation and Employment, 'Building a Digital Nation', https://www.mbie.govt.nz/info-services/digital-economy/documents-and-images/building-a-digital-nation.pdf

[2] See UNCTAD, exports of creative services were estimated at USD$424 billion in 2005, or 3.4% of global trade, with a growth rate of nearly 9% over the period 2000-05

European Centre for International Political Economy's '*Digital Trade Restrictiveness Index*' (DTRI).[3] Chile and Singapore rank, respectively, at 56 and 57 out of 65 countries in terms of restrictiveness (New Zealand, the least-restrictive country in the Index, ranks at 65).

8 Nevertheless, WeCreate supports the DEPA as a "pathfinder" to broader plurilateral or even global rules: this becomes all the more important when considering that, in the same ECIPE Index, the top ten most restrictive countries cover nearly half of the world's population, and a number of these most-restrictive countries are important creative economy export destinations for New Zealand, including notable markets around the Asia-Pacific.[4]

9 Typically, the barriers encountered by creative economy exporters in global markets include the following broad categories: traditional "services trade" barriers; challenges in relation to the dominant "platform-based" business model for some sectors; barriers in relation to cross-border data flows; other burdensome regulatory requirements; and challenges in relation to the protection of intellectual property rights. In some cases, greater openness to trade also has implications for the sustained viability of the New Zealand domestic creative economy.

Restrictions or prohibitions on the provision of digital goods or services

10 As for other services exporters, New Zealand creative sector exporters can encounter traditional "services" trade barriers including:

- restrictions or costs in relation to financial services – including relatively high financial transfer fees, especially for very large volumes of very low value transactions, or "microtransactions", as are common in the video gaming sector;
- discriminatory rules for the provision of online retailing, local presence requirements, limitations on foreign ownership and licensing and registration requirements;
- local content requirements;
- inability to use VOIP services in some territories;
- high visa costs and processing timeframes for business travel in some markets (especially for touring performers and offshore screen production activities);
- challenges around enforcement of end-user licensing agreements (for example, liability issues in relation to end-user licences in some markets e.g. access by a child of unsuitable content).

Challenges in relation to the market power of platforms

11 Digital platforms including e-commerce sites have unlocked significant opportunities for New Zealand creative sector exporters, providing a path to market that minimises the challenges of distribution, marketing and back-office functions such as payments and cybersecurity, and enabling innovative business models that can generate significant value and scale. At the same time, however, some large platforms exercise significant control over pricing, market intelligence and engagement with customers. These storefronts may raise challenges for New Zealand creative exporters, which are often very small and lack sufficient heft to influence large global platforms or their algorithms. Challenges may include:

- high fees (with few alternatives, such as online competitors or bricks-and-mortar retail options);
- lack of independent arbiters to settle disputes – dispute terms and settlement processes are imposed by the platforms;

[3] https://ecipe.org/wp-content/uploads/2018/05/DTRI_FINAL.pdf
[4] Digital Trade Restrictiveness Index, ECIPE (2018), https://ecipe.org/dte/

- lack of access to customer- or product-related data (such information is closely-held by platforms), making it difficult for exporters to respond to market signals;
- lack of influence over platform algorithms that may be important to discoverability;
- overly-broad limitations on liability of online platforms for intellectual property rights infringement, or so-called "safe harbours"; and
- platforms may not be regulated sufficiently to safeguard creator IP.

Barriers in relation to data flows

12 Restrictions on cross-border data flows add "hassle" and cost to business activities. Barriers encountered by New Zealand creative exporters include:

- restrictions on cross-border data flows, especially in relation to some markets, notably China;
- burdensome privacy or cybersecurity requirements, especially GDPR, notably in relation to monetising content and advertising; overall, *ensuring* compliance (rather than *being* compliant *per se*) adds significant legal and other costs;
- issues around sovereignty, control and jurisdiction of data;
- forced data localisation – in some cases, business have been able to find work-arounds (e.g. via licensing) and in some cases this is encountered as a commercial/contractual requirement rather than a regulated one. But forced data localisation (and/or associated local presence requirements) add significant costs and "hassle". The alternative – treating some markets' data differently to others – would likewise add costs and difficulties, leading to a view that in some cases it is simply easier not to supply those customers/markets;
- issues around the use of data in AI; and
- data transfer costs and inefficiencies – e.g. in relation to sending large files from New Zealand screen production overseas and back to New Zealand for post-production.

Other burdensome regulatory requirements, other issues

13 Other barriers that New Zealand creative exporters have encountered, both regulatory and otherwise, include:

- regulatory compliance costs across markets – especially where regulatory approaches and standards differ across markets – work against innovative business models. Territory-specific advice (and compliance/enforcement) in relation to local regulations and negotiating and enforcing contracts is both necessary and expensive;
- issues around liability and enforcement (especially in relation to artificial intelligence activity);
- issues around establishing/verifying identity;
- tax treatment;
- legal challenges around cryptocurrency and blockchain; and
- for e-commerce in relation to creative goods, challenges around traceability in supply chain; freight costs and import duties for inputs.

New Zealand domestic considerations

- global digital distribution offers new opportunities (markets and inputs) but could also mean that the domestic New Zealand tax base and domestic market, infrastructure and skills are eroded (local suppliers become relatively less competitive and this has impacts on the sustainability of domestic businesses); and
- shortage of workers with the right skills.

Intellectual Property

14 WeCreate notes that intellectual property (IP) protection is not mentioned in the briefing provided to the Minister for Trade and Export Growth, nor in the DEPA statement by New Zealand, Singapore and Chile. As noted above, creative content is a major driver of digital trade flows and the use of internet-connective devices around the world, but the expansion of digital trade must be predicated on both robust intellectual property protections and the ability to enforce such protections. Such an environment encourages the creation of high-quality creative content because of the assurance it provides to content creators in relation to the safe dissemination of that content and their ability to extract value from it. In short, copyright and other IP protections are at the heart of a successful creative economy, at home and abroad. A recent study on business experiences in the Asia-Pacific found that 83 percent of small businesses identified enforcement of intellectual property laws as either a "major" or "minor" problem in their cross-border e-commerce activities. [5]

15 Specific IP challenges encountered by the New Zealand creative sector include:

- online piracy – New Zealand authors, musicians, filmmakers and other creators have experienced substantial erosion in the value of their work due to illegal copying via peer-to-peer or streaming sites. This is a significant issue and an impediment to realising the full value of digital exports;
- subversion of technological protection measures (TPMs);
- lack of harmonisation in certain key areas, for example New Zealand's shorter copyright term of 50 years compared to 70 years in place in Singapore, Chile and many other OECD countries;
- overly broad limitations on liability, or "safe harbours", for online platforms; and
- performance requirements including forced transfer of source code or technology – these often feature in commercial relationships (e.g. contractual obligations) and are a "business reality" in some markets – but should not be a regulated requirement.

16 WeCreate urges New Zealand to include intellectual property rights protection in the DEPA negotiations; this should build on existing approaches in the WTO TRIPS Agreement, WIPO Internet Treaties and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), including in relation to copyright-protected content, copyright term, performance rights, and enforcement procedures. With regard to cross-border data flows and a free and open internet, while restrictions can and do act as barriers to trade, provisions on cross-border data flows must not interfere with the exercise and protection of legitimate intellectual property rights.

New Zealand's objectives for DEPA

17 New Zealand's objectives for DEPA should accordingly include the establishment of a rules-based, open global trading environment that supports cross-border data and digital trade flows (while recognising the need for certain restrictions to meet legitimate objectives, including the protection of intellectual property rights). Regulation should be as light-handed as possible, non-discriminatory, least trade-restrictive, and developed using good regulatory practices and through a process of robust consultation with stakeholders, including those in the creative economy.

[5] ABAC (2015), 'Driving Economic Growth through Cross-Border E-Commerce in APEC: Empowering MSMEs and Eliminating Barriers', University of Southern California Marshall School of Business, https://www2.abaconline.org/assets/2015/4%20Manila/MSMEEWG%2035-053%20USC%20Marshall%20SMMEs%20in%20e-Commerce%20Research%20Project%20Full%20Report.pdf

18 Specifically we would endorse approaches that include:

- a permanent moratorium on tariffs on electronic transmissions
- a prohibition on data localisation requirements and other restrictions on cross border data flows, with a high threshold for any exceptions (including the concept of measures being 'no more trade-restrictive than necessary to meet a legitimate objective')
- electronic authentication and recognition of e-signatures
- adequately resourced and streamlined Customs procedures, including e-border processes and paperless trading, consistent with the obligations in the WTO Trade Facilitation Agreement, to smooth trade flows and reduce compliance costs, especially for SMEs
- a high *de minimis* threshold for e-commerce
- cooperation on global approaches to cybersecurity, privacy, access to data for law enforcement and consumer protection – seeking to align approaches where possible
- further liberalisation of trade in digital services, including through removal of market access and national treatment restrictions on digitally-provided services
- a prohibition on requirements to provide source code and forced technology transfer
- consultative processes for the development of regulations and technical standards, and mutual recognition of conformity assessment
- given the crucial role played by e-payments/fintech in e-commerce, trade-enabling approaches to cross-border financial services
- platforms to be subject to competition policy disciplines that ensure a more level playing field for SMEs
- transparency (for exporters) around laws and regulations relating to data regulation

ENDS

Recommendations to the Ministry of Foreign Affairs and Trade

19 WeCreate recommends that the Ministry:

a. note WeCreate's support for the negotiation of an ambitious and trade-friendly global rules framework for digital trade, based on the approach taken in CPTPP, and drawing on APEC and ABAC Principles for Non-Tariff Barriers;
b. continue to consult widely with sectors likely to be impacted directly by the negotiations, and with other stakeholders

WeCreate Inc.
June 2019

For further information:
Paula Browning
Chair, WeCreate
[redacted]
Email: paula@wecreate.org.nz

NEW ZEALAND COUNCIL OF TRADE UNIONS
Te Kauae Kaimahi

Submission of the New Zealand Council of Trade Unions Te Kauae Kaimahi

to the

Ministry of Foreign Affairs and Trade

on the

proposed Digital Economy Partnership Agreement

P O Box 6645
Wellington
1 July 2019

Table of Contents

1. Introduction

1.1. This submission is made on behalf of the 27 unions affiliated to the New Zealand Council of Trade Unions Te Kauae Kaimahi (CTU). With over 310,000 members, the CTU is one of the largest democratic organisations in NewZealand.

1.2. The CTU acknowledges Te Tiriti o Waitangi as the founding document of Aotearoa New Zealand and formally acknowledges this through Te Rūnanga o Ngā Kaimahi Māori o Aotearoa (Te Rūnanga) the Māori arm of Te Kauae Kaimahi (CTU) which represents approximately 60,000 Māori workers.

1.3. While the digital economy, or electronic commerce, can have many benefits, it raises numerous difficult problems, many of which have only become apparent with time and experience. They range from privacy and labour rights through to economic development and taxation of multinationals. By addressing such issues in a trade negotiation, the emphasis is on commercial advantage rather than taxation or labour, democratic, consumer or human rights. This submission outlines the issues as we see them, and states the CTU's position.

1.4. "The digital economy" is a very broad term, but many (including the Productivity Commission) see it as difficult to define and it will become increasinglymeaningless.

As MFAT says in its outline of the proposal for a Digital Economy Partnership Agreement (DEPA)[1], quoting the Commission, "there is little to differentiate the digital economy from the broader economy; in other words, the digital economy is the economy". The title of this proposed agreement therefore does nothing to clarify its purpose. All parts of the economy already contain some digital elements, even if it is only the use of email and a website. Some are much more sophisticated even though their end products are not digital. Some are producing "digital" products, but the issues of the "digital economy" are not simply about them. We are not sure why this term has been used in preference to "E-commerce" which has been used in other negotiations (and MFAT says they are used "interchangeably"), nor how it might differ in practice. We will use the term here for the purposes of the consultation, and hope that our meaning is clear from the context.

1.5. We note that the start of negotiations towards a Digital Economy Partnership Agreement with Chile and Singapore was announced on 16 May 2019. The CTU is represented on the board steering the current trade policy review. We are disappointed that negotiations such as this are being initiated while that process continues. The continuation of such negotiations appears to pre-empt any recommendations the review that will make.

2. The objectives of an agreement on the digital economy

2.1. In broad terms, we see the digital economy presenting opportunities and threats, which we will outline below. It is growing rapidly. If we consider the objectives of a DEPA in a wellbeing context (such as the Government has used in the 2019 Budget) they should encompass not only growth in international trade but other impacts including people's rights to privacy and freedom from personal attack (physically or otherwise), good employment relationships and fair pay, the health and ability of New Zealand news media to provide good quality information and analysis, and the ability of our government and other governments to raise revenue. In these circumstances, "barriers" to a thriving trade are secondary. The most pressing need is to find ways to regulate to diminish the threats. Yet MFAT gives the primary objective as being to combat "barriers to digital trade", and the examples of these barriers include the very regulation that is urgently needed.

[1] https://www.mfat.govt.nz/en/trade/free-trade-agreements/digital-economy-partnership-agreement-depa-negotiations/

2.2. We do not consider that the appropriate context for such an agreement is a trade agreement. If trade can be enhanced without compromising the need for regulation, well and good. But the primary objective should be to ensure that the digital economy is used to enhance New Zealanders' wellbeing. The methods may include the regulation of the use of digital technologies; whether or not those are a "barrier to trade" is secondary. An equal consideration is whether some forms of expansion of international digital trade may reduce New Zealanders' wellbeing, for example by compromising their privacy or their security of employment.

2.3. By way of example of the problems of a trade-focussed approach, the CPTPP Chapter 14 on Electronic Commerce prevents customs duties on electronic transmissions. It is not clear what that means for services transmitted electronically and whether it impacts on the ability to tax the services or the suppliers of those services. It confers a right on businesses to transfer information, including personal information, across borders by electronic means, allowing regulation only if it is in a form least restrictive to trade. Recent events, such as incitements to violence and election interference using digital economy businesses, show that that the transfer of information should not be regarded as an absolute right, and that constraints on it may unavoidably be restrictive of trade because the greater public good lies in that direction. It requires at least as favourable treatment for digital products and services from another CPTPP country as for local ones, removing options for supporting the development of our products and services. It bans a country from requiring suppliers to locate computing facilities (such as storage of personal information) in its own territory, again allowing only regulation which is least restrictive to trade, putting protection of privacy out of practical reach for many purposes, removing options for the development of our own storage-based industries. It prevents governments from requiring access to software source code from suppliers in another country, even when that access may be essential to determining whether suppliers are obeying New Zealand laws (including distributing objectionable materials or discriminating on a racial or religious basis).

2.4. It requires each country to adopt and maintain consumer protection laws, but sets no standards for such rules and does not strengthen cross-border enforcement of them. Similarly it requires them to have a legal framework for the protection of the personal information of the users of electronic commerce, but again sets no standards nor does it provide for international enforcement. This approach is highly problematic given that the US, for example, regards privacy as a consumer issue,

'agreed' when purchasing a product or service, or governed by voluntary industry codes, rather than a right such as here and in the EU. It requires each country to have measures to control unwanted messages (spam).

2.5. These cover many areas of human activities and values including privacy, security, fair treatment free from arbitrary discrimination, effective and adequately-resourced government, intellectual property rights and local economic development. We submit that the cart has been put before the horse: a wide ranging discussion is needed rather than one focussed on enhancing trade.

3. Some of the issues that require consideration

Employment

3.1. Digital systems are being used in ways that cover every part of our lives. We are of course particularly concerned about employment.

3.2. The online 'platform economy' (such as Uber) undermines employment relationships, increasing insecurity, weakening minimum wage laws, making collective bargaining difficult or impossible, and increasing the likelihood of discrimination.

3.3. Increasing use of 'artificial intelligence' or computer algorithms in hiring, firing, monitoring workers and customers, and automating tasks has profound implications for work. For example, the algorithms used for "artificial intelligence" can have in-built gender, racial or other bias ("Algorithmic prejudice: Facebook's ad system seems to discriminate by race and gender," 2019; "Facebook charged with discrimination by US Department of Housing," 2019; Hatton, 2019; Keogh,2019).

3.4. This needs greater regulation and oversight, but the e-commerce rules do not help and in a number of ways make it more difficult (including preventing access to the code of such algorithms). This requires consideration not only of ensuring the applicability and enforcement of privacy and other human rights laws but also of reconsidering intellectual property rights rules that may govern access to algorithms.

3.5. The reach and the enforcement of employment laws across borders requires international agreement to prevent the use of digital commerce in undermining the viability of existing good jobs, intensifying work, or making work more insecure. Current models of labour chapters (such as in the CPTPP) do not address these issues.

3.6. Using social media to judge performance ("likes" and "dislikes") opens the door to prejudice in ways that can be very harmful to the target's current and future employment with none of the usual protections of requiring robust evidence and fair process.

Competition

3.7. Some of these corporations have grown to become the largest in the world with monopolies over major areas of commerce. They are a force in growing inequality. The need for regulation and competition will grow. The growth in technology, because of its capital intensity and network effects may lead to greater industry concentration and increased monopsony power of employers (e.g. Autor, Dorn, Katz, Patterson, & Reenen, 2017; Mitchell, 2018; Naidu, Posner, & Weyl, 2018). Competition chapters in current international agreements typically deal only with domestic competition. The need is for international rules that regulate international anti-competitive behaviour.

Offensive and harmful use

3.8. Personal data has become very valuable to companies like Google and Facebook yet has been used in intrusive, anti-social or anti-democratic ways and the companies are becoming de facto regulators of what is offensive and what is 'fake news'. Increasingly countries are trying to regulate this, but it is made more difficult or unlawful by rules that restrict regulation of electronic data flows, where computer facilities are located, and the ability to inspect the algorithms used by these companies. We need international agreement on ways to regulate such activity under the various countries' laws rather than leaving it to corporate censors acting under a particular country's law which may or may not govern international activities.

Protection of personal information and privacy

3.9. There is insufficient protection for personal information and privacy. This concerns both our daily lives (such as use of social networks) and employers' use of our personal data. As noted above, in some countries such as the US, the regulation of privacy and use of data may be regarded as 'consumer' issues rather than as a right as in New Zealand's privacy laws. In such circumstances, the privacy and proper use of individuals' information is not protected by international agreements that assume that each country has adequate laws for this purpose. International agreement on minimum standards for such laws is needed.

3.10. In addition, if personal data is stored in a country with weak privacy or intrusive surveillance laws then the rights of users of such services in New Zealand are curtailed either by law or by difficulties in enforcement of rights. Providers of digital services may be subject to requirements by governments (such as the US or China) to provide information or allow access to the information of individuals or organisations using their services. It may not be clear to individuals which suppliers are providing such services (particularly for example if they are subcontracted out) and where storage is located. It may not be their choice if the data is held by an employer. If international agreements continue to outlaw government requirements to provide services locally then users are unable to be sure that their information is protected.

3.11. Before making agreements that encourage these circumstances to intensify, the priority should be to reach international agreement on minimum standards (such as the European Union's General Data Protection Regulation) at least consistent with New Zealand law.

Taxation

3.12. Taxation of corporations like Google, Apple, Facebook and Amazon is already difficult, heavily constrained by existing trade rules. An international agreement on their taxation is being discussed at the OECD under an extension of the Base Erosion and Profit Shifting (BEPS) process, and this would be the best outcome. However this may be a long time coming because the countries in which these corporations are based (primarily the US, but possibly also China) will be unwilling to reduce their rights to taxation and to reduce the competitive advantage of under-taxation given to "their" corporations. We are therefore likely to depend on a digital services tax which the Government is currently consulting on.

3.13. The ability to levy such a tax is wedged between double taxation treaties which prevent new approaches to corporate income taxation, and trade (such as WTO) rules which prevent the use of other forms of tax that might be interpreted as tariffs. The space is narrowed further by National Treatment requirements that require overseas suppliers to get no less favourable treatment than local companies. National Treatment prevent policies that stop double taxation of local companies who would otherwise be required to pay both company income tax and the digital services tax. A further constraint is provisions in agreements such as the CPTPP preventing any requirement for a physical presence in New Zealand. Aphysical

presence is a requirement for corporate taxation under current double taxation treaties. It may be that tariffs on digital trade may have to be considered if other options are not possible, but that has been ruled out too.

3.14. It is not sufficient to say, as is stated in some government material, that “This agreement will not affect New Zealand's tax settings nor prevent us from imposing domestic taxes (e.g. GST or income tax) on electronically-transmitted content” (New Zealand Government, 2019) when there are such barriers to good tax policy. Positive action is required to enhance the government’s ability to tax and enforce its collection. While international agreement at the OECD would be the best outcome, regional agreements could build towards that outcome and agreements covering the digital economy should include enhanced rights to tax suppliers and for mutual enforcement of such rights.

Economic development

3.15. The rules make it more difficult to develop local digitally-based services competing with large multinationals, limiting our economic development and that of developing countries.

Impact on local news services

3.16. Meanwhile, corporations such as Google and Facebook undermine the financial viability of local news media without contributing to local professional news gathering or taxes. There is a strong case to tax their activities on the grounds of their impact on local news services, in order to fund local news gathering and investigative reporting. This is over and above the need to tax their income as for any other company active in New Zealand. The right to exact such a tax should be recognised in international agreements.

Cross-border enforcement

3.17. Enforcement of New Zealand law against the increasing numbers of cross-border online employers and service providers (a current example being Switzerland-based ticket reseller Viagogo) is difficult or impossible. The problem of cross-border enforcement is not new, but it is multiplied many times by the ease with which electronically based business can work across borders. It is worsened by provisions in agreements such as the CPTPP preventing any requirement for a physical presence in New Zealand which would make consumer and other complaints easier to bring and enforce. This is likely to prove important in areas like provisionof

medical treatment across borders. Agreement is needed to make international enforcement much easier.

Public services

3.18. Our longstanding concerns about the potential impact of trade in services and investment agreements on public services should be well known to MFAT.

3.19. An example relevant to digital services is the cross-border provision of education services into New Zealand by electronic means. These raise again the important questions of quality assurance, competition for government funding, cherry-picking of courses, and undermining of the viability of our public institutions and local content essential for New Zealand's economic, social and cultural development and for the protection of our environment. The growth of large-scale free online courses (MOOCs or Massive Open Online Courses) is an illustration of the threats and opportunities, but our concerns would be further intensified if the large technology companies began provision of courses, either directly or through subsidiaries.

3.20. As with the other matters we have discussed in this submission, the primary need and priority is for suitable regulation of such activities to ensure that they increase New Zealand's wellbeing rather than treating them primarily as trade and commercial opportunities.

4. Conclusion

4.1. We agree that international agreements on the digital economy (e-commerce) are urgently needed. However their focus should be to assist international regulation of employment practices, protect privacy and consumer rights, and encourage the development in all countries of digitally based services and industry while helping authorities break up and regulate international monopolies, gather revenue from these companies, and enforce our laws.

4.2. The current model of E-Commerce agreements, such as in the CPTPP, often work against these needs.

4.3. The government should recognise that digital economy agreements have broad social and developmental impacts that are not predominantly commercial and should consult broadly on them before developing an acceptable human-centred model. They should not be part of free trade and investment agreements.

5. References

Algorithmic prejudice: Facebook's ad system seems to discriminate by race and gender. (2019, April 4). *The Economist*. Retrieved from https://www.economist.com/business/2019/04/04/facebooks-ad-system-seems-to-discriminate-by-race-and-gender

Autor, D., Dorn, D., Katz, L. F., Patterson, C., & Reenen, J. V. (2017). *The Fall of the Labor Share and the Rise of Superstar Firms* (Working Paper No. 23396). https://doi.org/10.3386/w23396; NBER: http://www.nber.org/papers/w23396

Facebook charged with discrimination by US Department of Housing. (2019, March 29). *Stuff.Co.Nz*. Retrieved from https://www.stuff.co.nz/technology/social-networking/111638395/facebook-charged-with-discrimination-by-us-department-of-housing

Hatton, E. (2019, May 23). Truckies leaving job over poor pay, driver-facing cameras. *RNZ News*. Retrieved from https://www.rnz.co.nz/news/national/389844/truckies-leaving-job-over-poor-pay-driver-facing-cameras

Keogh, B. (2019, May 27). Independent watchdog needed to probe Government's use of AI: law, computer science experts. *Stuff.Co.Nz*. Retrieved from https://www.stuff.co.nz/technology/112954104/independent-watchdog-needed-to-probe-governments-use-of-ai-law-computer-science-experts

Mitchell, S. (2018, February 15). *Amazon Doesn't Just Want to Dominate the Market—It Wants to Become the Market*. *The Nation*. Retrieved from https://www.thenation.com/article/amazon-doesnt-just-want-to-dominate-the-market-it-wants-to-become-the-market/

Naidu, S., Posner, E., & Weyl, G. (2018). *More and more companies have monopoly power over workers' wages. That's killing the economy*. Retrieved from Vox website: https://www.vox.com/the-big-idea/2018/4/6/17204808/wages-employers-workers-monopsony-growth-stagnation-inequality

New Zealand Government. (2019). *Digital Economy Partnership Agreement - TPs and Q&A*. New Zealand Government.

A Sleeping Giant: New Zealand's Obligations on Electronic Commerce and Digital Services[1]

Electronic commerce, or digital trade, is the newest and most far-reaching of the 21st century 'new issues' in international trade negotiations. Digital technologies are transforming the world around us at a breathtaking pace, offering huge advantages to first movers and posing massive challenges for regulators and for countries seeking to catch up. There are strong parallels to the bonanza of riches that financial innovators secured in the 1990s and 2000s, thanks to a void in understanding of their services and products, especially by financial regulators. In both cases, the mega-corporations that control the technologies and dominate the markets have sought and secured 'trade' rules that protect their positions and will constrain new regulation once the risks and negative consequences of their activities are betterunderstood.

Prior to the Trans-Pacific Partnership Agreement (TPPA) New Zealand had adopted very few obligations on electronic commerce in its free trade agreements (FTAs), and almost all of them were unenforceable. There were also little-known restrictions on the regulation of cross-border and technology-related services under the World Trade Organization's (WTO) General Agreement on Trade in Services (GATS) and cross-border services chapters in FTAs. The TPPA's electronic commerce chapter has introduced unprecedented, extensive and enforceable constraints on New Zealand's ability to regulate the digital domain. The original TPPA chapter remains unchanged in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) or TPPA-11. According to government documents, that is now considered to be the standard template for future bilateral, regional and multilateral negotiations.[2]

This paper describes the new digital trade regime as a sleeping giant, which will at worst prevent, and at least have a chilling effect on, moves by future governments to regulate the digital domain in the public interest. The basis for this claim is articulated through three levels. At a meta-level, the disciplines being developed extend far beyond any legitimate notions of trade. They seek to impose global rules on governance of the digital domain - arguably one of the most complex, multi-dimensional and hence controversial subjects confronting states and societies this century, alongside climate change. That portends a contest over their legitimacy that rivals the current crisis confronting the international investment regime and is centred around development asymmetries, public interest, wealth distribution, corporate capture, geopolitics and foreignpolicy.

At a meso-level, the location of these rules within a trade liberalisation paradigm prescribes a particular ideology, historically derived institutional context, legal form and meaning, inclusion and exclusion. Specifically, it means they are: framed by concepts that privilege market and commercial interests over all else; devised in undemocratic, usually secretive, trade negotiations to which

[1] Professor Jane Kelsey, Faculty of Law, University of Auckland

[2] Hon David Parker to Jane Kelsey, 9 February 2018, Singapore-New Zealand Closer Economic Partnership Upgrade Negotiations: Closing mandate (undated). Released under the Official Information Act, February 2018. (MFAT OIA)

industry lobbyists have privileged access; located within the prescriptive legal form, drafting and interpretation precedents, and enforcement mechanisms of free trade agreements; and constructed by trade officials whose inclination, training and mandates are to bring negotiations to a successful conclusion through trade-offs, subject to the *real politik* of the deal.

The final part of the paper applies this argument at the micro-level, reviewing how the New Zealand government has approached the novelty of trade rules on e-commerce, principally in the TPPA. Using heavily redacted documents released under the Official Information Act by the Ministry of Foreign Affairs and Trade (MFAT) and by the Privacy Commission, I try to assess how the meta-level factors play out in practice and the problems that creates for public interest-based approach to regulating the digital domain. The analysis uses three quite different examples: privacy, source codes, and Maori data sovereignty.

I conclude that New Zealand urgently needs to liberate the rules governing the digital domain from the closed confines of the trade rubric and control of the trade bureaucracy, and conduct an open, informed debate about what values, priorities and interests should inform our approach as the technology, our understanding, and its impacts evolve over time. The entry into force of CPTPP has partly pre-empted our ability of this and for future governments to apply the promised 'inclusive and progressive' strategy to rules on e-commerce. But we can still play an important, critical role in the regional and multilateral context. Unless we do, the government and our trade negotiators risk leading the country down a cul-de-sac from which there are very limited options for regulatory exit, and which will have serious, as yet unforeseen, consequences in the future.

A brief historical context

Electronic commerce appeared as a 'trade' issue on the agenda of the WTO in 1998,[3] when the US tabled a proposal to make permanent the moratorium on customs duties on electronic transmissions adopted at the 1st ministerial meeting in 1996. That was genuinely about trade. Subsequent discussions at the General Council led to the adoption of a Work Programme on Electronic Commerce in September 1998, to be conducted through the WTO's committees on trade in goods, trade in services, intellectual property, and trade and development.[4] The mandate defined electronic commerce as the 'production, distribution, marketing, sale or delivery of goods and services by electronic means'. The Work Programme has been renewed at each ministerial conference, without making significant progress on developing newrules.[5]

[3] General Council, 'Global Electronic Commerce. Proposal by the United States', WT/GC/W/78, 9 February 1998

[4] Work Programme on Electronic Commerce. Adopted by the General Council on 25 September 1998, WT/L/274, 30 September 1998, pursuant to the Ministerial Declaration on Global Electronic Commerce, adopted on 20 May 1998, WT/MIN(98)/DEC/2.

[5] Jane Kelsey, 'The development implications of TPP-style e-commerce rules for the GATS acquis', 21:2 *Journal of International Economic Law* 273-295

In parallel, e-commerce has incrementally become more prominent in free trade agreements (FTAs), with US FTAs taking the lead.[6] Its scope has moved far from that early definition to now impose disciplines on broad matters of internet governance, secrecy of source codes and algorithms, offshore transfer and processing of data, spam, e-signatures for transactions, net neutrality and access to the internet, and public telecommunications networks. These chapters are complemented by more expansive chapters on trade in services, financial services and telecommunications.[7]

Chapter 14: Electronic Commerce in the Trans-Pacific Partnership Agreement (TPPA) 2016 set the precedent and the basic template. Negotiations were contested, but within narrow US-defined parameters. As a signal of discomfort, it was not agreed that some of all of the chapter would be subject to dispute settlement until the end. The recently revised North American Free Trade Agreement (NAFTA), the US Mexico Canada Agreement 2018 (USMCA), hosts the most comprehensive 'digital trade' chapter to date,[8] eclipsing the TPPA. Japan has also become a leading proponent. The Japan Mongolia Economic Partnership Agreement 2016 largely replicated the TPPA. The final text of the EU Japan Economic Partnership Agreement that entered into force in January 2019 is almost as extensive, aside from the provision on cross-border data flows.[9] The European Union has been developing its own model, different in form but substantially the same in substance, aside from provisions on privacy of personal information.

There was never a leak of the TPPA e-commerce chapter. The first developed text that became publicly available for analysis was a leak of the e-commerce proposals in the now moribund Trade in Services Agreement (TiSA),[10] which was based on the TPPA. It took several iterations of leaks and quite extensive debate among academic, legal and technology experts to identify the key questions, let alone the economic, social, cultural and regulatory implications.[11] By that time the TPPA's e-commerce chapter had been concluded, with some safeguards inserted into the rules demanded by

[6] The pre-cursor to the TPPA was Chapter 15 of the US Korea Free Trade Agreement 2012, which covers electronic supply of services (technological neutrality); non-discrimination and no customs duties on digital products; electronic authentication and signatures; online consumer protection; paperless trading; principles of access to and use of the Internet for electronic commerce; and cross-border information flows. The Australia US Free Trade Agreement 2005 did not include access to and use of the Internet or cross-border information flows. Notably none of these FTAs included non-disclosure of source code, which was a Japanese initiative in the TPPA.

[7] See similar proposals in TiSA, Jane Kelsey (2017), *TiSA: Foul Play,* UNI Global Union, Brussels: telecommunications 58-62, 111-124; financial services 125-133.

[8] The Chapter 19 provisions cover: 1. Definitions; 2. Scope and General Provisions; 3. Customs duties; 4. Non-discriminatory treatment of digital products; 5. Domestic electronic transactions framework; 6 Electronic authentication and electronic signatures; 7. Online consumer protection; 8. Personal Information Protection; 9. Paperless trading; 10. Principles on access to and use of the Internet for digital trade; 11. Cross-border transfer of information by electronic means; 12. Location of computing facilities; 13. Unsolicited commercial electronic communications; 14. Cooperation; 15. Cybersecurity; 16. Source code; 17. Interactive computer services; 18. Open government data.

[9] Chapter 8, Section F, esp Article 8.81.

[10] See https://wikileaks.org/tisa/ecommerce/

[11] Jane Kelsey and Burcu Kilic, 'Briefing on US TiSA Proposal on E-Commerce, Technology Transfer, Cross-Border Data Flows and Net Neutrality', 17 December 2014, <http://cdc-ccd.org/IMG/pdf/Briefing_on_TISA_E-Commerce_Final.pdf> ; Tamir Israel, Tisa Annex on Electronic Commerce, https://wikileaks.org/tisa/ecommerce/analysis/Analysis-TiSA-Electronic-Commerce-Annex.pdf; Jane Kelsey (2017) *TiSA: Foul Play,* 33-46, 94-106

the US and subsequently Japan.[12] As the negotiations entered their end game, it was impossible to generate an effective informed public debate to get the text reopened. Meanwhile, Japan was vigorously promoting the same text through the RCEP, where it met stronger resistance. Not only was China a party, but more information was available to inform developing countries especially of the implications. Similar engagement was occurring internationally level, including through the trade and development division of UNCTAD, and the South Centre in Geneva. In other words, the e-commerce chapter in the TPPA slipped through largely unnoticed, but it is now highly contested.

New Zealand's e-commerce obligations have followed a rapid trajectory. Elements such as paperless trading, and electronic notifications and tendering, were dispersed through various chapters of the Trans-Pacific Strategic Economic Partnership Agreement or 'P-4'. The agreement with Thailand in 2005, and those with Hong Kong and with Australia and ASEAN in 2010, had electronic commerce chapters,[13] but the obligations were flexible and, aside from a moratorium on customs duties in the Thai FTA, were not subject to dispute settlement. The TPPA was a massive step up in both substance and enforceability. Since agreed to, it has become the new norm. The recent upgrade of the agreement with Singapore (a party to CPTPP) is apparently incorporating the TPPA model, with officials describing it as

> an exemplar for subsequent efforts towards e-commerce trade liberalisation, including in future FTA negotiations and within the World Trade Organization (WTO). Many "core" components of the chapter are based on the CPTPP and *consistent with New Zealand's standard approach* … .[14]

The European Union (EU) has tabled an electronic commerce text in its negotiations with New Zealand that takes a different form but covers the same ground,[15] and includes a broad definition of 'computer and related services' the EU has been promoting for some years to update the classification of those services that is used in the GATS.[16]

New Zealand has also joined a breakaway minority of WTO Members who, unable to secure a mandate for negotiations on e-commerce at the 11th ministerial conference in December 2017,[17] announced their intention to pursue an agreement among themselves.[18] During 2018 they held several meetings in Geneva which were co-chaired by Australia, Singapore and Japan – all TPPA-11 parties. At a side-meeting at the World Economic Forum in Davos in February 2019, trade ministers

[12] The e-commerce chapter was reportedly one of the first to be closed, in mid-2014.
[13] Chapter 10 of each agreement.
[14] Parker to Kelsey, 9 February 2018, page 9 of 20 para 47 (MFAT OIA)
[15] EU-New Zealand Free Trade Agreement, Title [ ] Digital Trade, 25 September 2018
[16] Communication from the European Communities and their Member States, 'Coverage of CPC 84 – Computer and Related Services', TN/S/W/6, S/CSC/W/35, 24 October 2002.
[17] The Ministerial Statement only reaffirmed continuation of the moratorium on customs duties. WTO Ministerial Conference, Eleventh Session, Buenos Aires, 10-13 December 2017, Work Programme on Electronic Commerce. Ministerial Decision of 13 December 2017, WT/MIN(17)/65, 18 December 2017
[18] WTO Ministerial Conference, Eleventh Session, Buenos Aires, 10-13 December 2017, Joint Statement on Electronic Commerce, WT/MIN(17)/60, 13 December 2017

from over seventy countries[19] reaffirmed their intention to launch negotiations for a plurilateral agreement on electronic commerce.[20]

The WTO move raises are many complexities, not least how they will conduct negotiations and secure adoption of any agreement within the legal parameters of the Marrakesh Agreement.[21] Pushing negotiations without a mandate and spurning the Doha round is also highly divisive, and bound to have a further corrosive impact on an already fractured WTO – a crisis which New Zealand has vowed to help fix, not exacerbate. Members from the global South are split.[22] A group of Friends of E-commerce for Development, including China, are promoting the new agenda with support from well-funded think tanks and the divisions of UNCTAD on logistics and trade.[23] Major developing countries like the African group,[24] the group of Least Developed Countries, and India, supported by a different UNCTAD department,[25] supported a continuation of the existing work programme. They insist that digital industrialisation requires policy space and that the outstanding development agenda from the Doha round must be addressed before any new issues are negotiated.[26] China decided at the last minute to sign on to this breakaway group, even though – or because - the TPPA rules were ultimately targeted at China's digital industrialisation and security strategies. The Regional Comprehensive Economic Partnership (RCEP) negotiations show there are clear base lines beyond which China will not go, including at the WTO. These are crucial questions, some of which are addressed below.

The Meta-level: Wrong Arena, Wrong Agenda, Wrong Goals

E-commerce is shaping up to be the next battleground in the turbulent international trade law arena. Much of the resistance mirrors the objections that have plunged the international investment regime into a crisis of legitimacy – development asymmetries, ideological closure, pro-corporate bias, industry capture, exclusion of affected interests from negotiations and disputes, fetters on regulatory sovereignty, among others. But unlike foreign investment, the dynamic transformation of the digital domain is rapid, unpredictable and harmful in as-yet-unforeseen ways, making policy

[19] This number includes the European Communities, plus all the EU Member States.
[20] Joint Statement on Electronic Commerce, WT/L/1056, 25 January 2019
[21] Ravi Khanth, 'Intention to launch e-com pluri talks announced at Davos' Published in SUNS #8833 dated 28 January 2019; Ckakravarthi Raghavan and Jomo Sundaram, 'Beware Proposed E-Commerce Rules', *IPS News, 5 February 2019* http://www.ipsnews.net/2019/02/beware-proposed-e-commerce-rules/
[22] South Centre, 'The WTO's Discussions on Electronic Commerce', SC/AN/TDP/2017/2, January 2017
[23] The WTO lists the members as Argentina, Chile, China, Colombia, Costa Rica, Kazakhstan, Kenya, Mexico, Moldova, Montenegro, Nigeria, Pakistan, Sri Lanka and Uruguay and the MIKTA group (Mexico, Indonesia, Korea, Turkey and Australia); https://www.wto.org/english/thewto_e/minist_e/mc11_e/briefing_notes_e/bfecom_e.htm. See also Second Meeting of Friends for E-Commerce for Development Held in Argentina, Ministry of Commerce, People's Republic of China, 12 December 2017, http://english.mofcom.gov.cn/article/newsrelease/significantnews/201712/20171202688768.shtml
[24] General Council, 'Work Programme on Electronic Commerce. Communication from the African Group. Draft Ministerial Decision on Electronic Commerce', JOB/GC/155, 21 November 2017
[25] The Division on Globalization and Development Strategies. See South-South Digital Cooperation, a Regional Integration Agenda, 2018, UNCTAD/GDS/ECIDC/2018/1, and the critique in the *Trade and Development Report 2018,* Chapter III.
[26] Ravi Khanth, 'India rejects WTO push for new global e-commerce rules', *LiveMint,* 17 October 2017, https://www.livemint.com/Industry/tRCUKDsTGvnQUpVyVTLmhJ/India-rejects-WTO-push-for-new-global-ecommerce-rules.html

space all the more imperative. On top of this, there is a fraught history of moves in other international institutions and multi-stakeholder forums to develop agreement, or at least principles, on Internet regulation that have largely been blocked by the proponents of digital trade rules.

The advent of this new 'trade' agenda has been heavily contested from within and outside the international trade regime. The issue has divided developing countries and development-oriented international organisations. While proponents hail the potential for developing countries to leapfrog the development divide,[27] others warn that the proposed rules will deepen the development asymmetry beyond the current digital divide and herald a new form of colonialism.[28] These tensions are evident in regional moves to develop e-commerce strategies and associated rules.[29]

The UNCTAD Trade and Development Report 2018 articulated why many developing countries are opposed to e-commerce negotiations in the WTO:

> Among the most critical additional policy challenge(s) is that of adopting competition and regulatory frameworks to address potential adverse effects on market structure, innovation and the distribution of gains from digitalization. The combination of network effects and rent-seeking behaviour associated with the digitization of data that transcend borders, must also be closely monitored and carefully managed. Accordingly, developing countries will need to preserve, and possibly expand, their available policy space to effectively manage integration into the global digital economy.[30]

The report goes on to caution against 'a premature commitment by developing countries to trade and investment rules driven by one-sided interests and with long-term impacts'. It recommends instead the pursuit of South-South digital cooperation, including through their regional integration agendas.[31] That critique contrasts with numerals panels at UNCTAD e-commerce week in 2017 and 2018 pushing for the launch of negotiations.[32]

Similar divisions are evident between internet governance and digital rights groups, on one hand and the industry lobby and its allies on the other. The US industry has aggressively positioned itself since the late 2000s, pressing a consistent set of demands through industry specific organisations,[33]

---

[27] Director-General Azevedo, Remarks at the Launch of WTO-eWTP-WEF Enabling E-commerce, 11 December 2017, https://www.wto.org/english/news_e/spra_e/spra206_e.htm

[28] Parminder Jeet Singh, 'Digital Industrialisation in Developing Countries – A Review of the Business and Policy Landscape', *IT for Change,* December 2017, http://itforchange.net/digital-industrialisation-developing-countries-%E2%80%94-a-review-of-business-and-policy-landscape

[29] South-South Digital Cooperation, a Regional Integration Agenda, 2018, UNCTAD/GDS/ECIDC/2018/1,; Jane Kelsey, (2017) *The Risks for ASEAN of Mega-FTAs that Promote the Wrong Model of e-Commerce*, Economic Research Institute for ASEAN and East Asia (ERIA)

[30] UNCTAD *Trade and Development Report 2018. Power, Platforms and the Free Trade Delusion*, UNCTAD/TDR/2018, 69

[31] Ibid, 70

[32] For example, Catherine Saez, 'Panel: E-commerce crucial for development, some eager to negotiate at WTO', *Intellectual Property Watch,* 18 April 2018, http://www.ip-watch.org/2018/04/18/panel-e-commerce-crucial-development-eager-negotiate-wto/ ; see 2017: https://unctad.org/en/conferences/e-week2017/Pages/default.aspx; 2018: https://unctad.org/en/conferences/e-week2018/pages/default.aspx?Ne=10,3,,

[33] An open letter dated 17 October 2016 was signed by seven groups: the *Internet Association*, C*omputer and Communications Industry Association*, *Information Technology Industry Council, BSA/Software Alliance*, *ACT/The App*

and broader industry lobby groups. The massive influence of the Big Tech lobby on US trade strategy since the late 2000s[34] was evidenced in the USTR's 'digital 2 dozen' principles[35] and codified in the TPPA.[36] The deputy USTR responsible for e-commerce had spent the previous 23 years as chief executive of the Software Alliance (BSA). The tech lobby made up fully one-third of the corporate members of 'Team TiSA', hosted by the Coalition of Services Industries (which includes Business NZ). [37] The industry was very active in many guises during the Davos 2019 meeting, where the 'fourth industrial revolution' was the theme. [38]

The digital rights groups object that these rules extend far beyond 'trade' or even electronic commerce in scope, involving matters of Internet governance and the rules that govern the digital domain, and should not be made in a trade liberalisation arena. An international coalition of digital rights groups, calling itself JustNet,[39] rejected the intention announced at Davos to develop e-commerce rules through the WTO and FTAs 'a global blue-print of a whole new digital social order which is a form of neo-colonialism that will favour only big business and not ordinary citizens anywhere'. They called out the hypocrisy of those who were advocating a binding e-commerce agreement at the WTO, but who long rejected the development of binding intergovernmental agreements for these matters and blocked initiatives in international organisations with more relevant mandates, such as the International Telecommunications Union (ITU).[40] These same governments who once insisted that all discussions on Internet governance must take place in multi-stakeholder forums were now proposing 'closed and non-transparent pluri-lateral intergovernmental discussions (with business lobbying encouraged)'.

Their statement invoked the Tunis Agenda for the Information Society, agreed at the ITU's World Summit on the Information Society in 2005, for 'enhanced cooperation in the future, to enable governments, on an equal footing, to carry out their roles and responsibilities, in international public policy issues pertaining to the Internet, but not in day-to-day technical and operational matters, that do not impact on international public policy issues'.[41] That would not happen in the WTO. They called instead for a new UN based global mechanism to pursue the Tunis mandate, whichwas

---

Association, *Consumer Technology Association*, https://internetassociation.org/tisa101716/. Another open letter from the Internet Association to Hon Robert Lighthizer was dated 16 May 2017, https://cdn1.internetassociation.org/wp-content/uploads/2017/05/Lighthizer-Letter-5.16.pdf.

[34] Jane Kelsey, *TiSA: Foul Play,* 16-21

[35] USTR, The Digital 2 Dozen, 13 April 2016, https://ustr.gov/sites/default/files/Digital-2-Dozen-Final.pdf

[36] Nick Deardon, Press Statement, *Global Justice Now*, 25 January 2019, https://www.globaljustice.org.uk/blog/2019/jan/25/big-tech-should-be-taxed-and-regulated-%E2%80%93-davos-elite-wants-give-amazon-and-facebook

[37] The website, hosted on the Coalition of Services Industries' website, is defunct. The membership is analysed in Kelsey, *TiSA: Foul Play*, 20, Table 2.2.

[38] Brad Stone, 'Stuck in a Trade War, Tech Pitches Davos on Innovation', *Bloomberg,* 25 January 2019, https://www.bloomberg.com/news/articles/2019-01-24/tech-optimism-at-davos-tempered-by-trade-anxiety-and-regulation

[39] JustNet Coalition Statement on the Hypocrisy of Proposed Internet and Data Governance in the Name of E-Commerce Rules, January 2019 https://justnetcoalition.org/2019/WEF_and_e-com_hypocrisy.pdf

[40] Richard Hill (2013) *The New International Telecommunications Regulations and the Internet: A Commentary and Legislative History,* Schulthess/Springer: New York

[41] http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html, Para 69

'languishing due to stone-walling by the very governments that now plan to undertake Internet governance at closed inter-governmental forums involving select governments or at the WTO'.

Another significant group of stakeholders, the Trans-Atlantic Consumer Alliance led by Consumers International, insists any international discussion on digital trade must be transparent, open and inclusive; puts consumer interests at the centre; and recognises that topics such as cybersecurity, internet of things, artificial intelligence, net neutrality and data protection do not belong in trade agreements.[42] The rationale for the new 'trade' agenda has also been questioned from the 'right'. Simon Lester for Cato Institute obligations noted TPPA rules on online consumer protection and spam 'are not about reducing trade barriers, but rather about encouraging governments to adopt particular domestic policies', then asked what they were actually intended to do?[43]

The e-commerce agenda has also generated a broader civil society campaign. The international movement of trade unions and non-government organisations have long criticised free trade and investment agreements as partisans of capital that fuel inequalities and work for the 1%. Big Tech is the latest iteration. Post-Davos, civil society groups warned that 'threats to economic sovereignty … will be greatly amplified if the rapidly evolving digital economic space is governed by rules that were developed by transnational corporations (TNCs) for their own profit-making around the world.'[44] The International Trade Union Congress stressed the need to safeguard governments' space to regulate as the tech giants consolidate their power: 'Algorithmic bias, workplace surveillance, electronic union blacklisting are realities and workers need their governments to protect them. We must not allow for a future in which working people's ability to hold the giants of the digital economy accountable is limited by trade agreements. Our governments must have full power to regulate.'[45]

These challenges are overlaid by rising geo-political and strategic tensions, being played out in both the digital and trade arenas between the US and China as the old and new hegemons.[46] China's aggressive digital strategy challenges the technological and commercial dominance of US and European states and the first mover benefits of their tech-related industries. The recent moves by the Five Eyes governments and their allies to exclude Huawei commercially and operationally from the telecommunications networks is accelerating these tensions.[47] Digital trade rules are seen as a

[42] Trans-Atlantic Consumer Dialogue (TACD) Resolution on Digital Trade, 28 January 2019, http://tacd.org/tacd-urges-wto-negotiators-not-to-interfere-with-digital-rights

[43] Simon Lester, 'What are trade rules on e-commerce supposed to do?', *World Trade Law Blog,* 27 January 2019, https://worldtradelaw.typepad.com/ielpblog/2019/01/what-are-trade-rules-on-e-commerce-supposed-to-do.html

[44] 'Civil society calls on governments to reject WTO e-commerce talks', 25 January 2019, https://www.downtoearth.org.in/news/economy/civil-society-calls-on-govts-to-reject-wto-e-commerce-talks-62968

[45] International Trade Union Congress ' "E-commerce" push at WTO threatens to undermine labour standards', 25 January 2019, https://www.ituc-csi.org/e-commerce-push-at-wto-undermines-workers

[46] Jane Kelsey, 'The Trans-Pacific Partnership Agreement and The Regional Comprehensive Economic Partnership: a battleground for competing hegemons?', M. Perry (ed) *Perspectives on Free Trade: Hegemony or Harmony*, New York: Springer, 11-34; Henry Gao (2018), 'Digital or Trade? The Contrasting Approaches of China and the US to Digital Trade', 21:2 *Journal of International Economic Law* 297-321

[47] Nick Beams, '"Five Eyes" Intelligence Agencies Behind Drive Against Chinese Telecom Giant Huawei', *Global Research,* 14 December 2018, https://www.globalresearch.ca/five-eyes-intelligence-agencies-behind-drive-against-chinese-telecom-

means of accessing the massive Chinese market on their own terms and neutralising Chinese competition in third countries - China was the ultimate, although not only, target of the TPPA's e-commerce rules. This context also explains China's decision to join the breakaway negotiations at the WTO, and why it will never agree to a TPPA-style outcome there, in the RCEP or any other negotiation.

Despite the focus on inter-state tension, the oligopoly of the private tech giants poses an equally fraught foreign policy and national security challenge. The risks of global cyber-warfare, and the abuses of data and technology, and covert political interference, span the tech giants, foreign states and private actors.

There is a common misconception that security concerns can be set aside because international trade agreements give states a self-judging right to breach their trade obligations on the grounds of national security. To date, the cyber-security provisions in e-commerce texts contain minimalist promises of cooperation.[48] The national security exception is based on Article XIV*bis* of the GATS, which is in turn based on Article XXI of the General Agreement on Tariffs and Trade 1944 (GATT). There is some scholarly dissension over whether objective tests might be applied to its self-judging elements.[49] Much less attention is paid to fact there is a closed list of criteria on which governments can rely. These are essentially procurement to provision a military establishment; actions related to nuclear materials; war or 'another emergency in international relations'; or pursuit of obligations under the UN charter for the maintenance of international peace and security. States taking retaliatory or pre-emptive action, for example in requiring disclosure of source codes or use of local computing facilities and servers, may struggle to establish that they are responding to an 'emergency in international relations', which the term 'another' implies is of severity akin to awar.

The TPPA and USMCA have recognised and resolved this problem by replacing the old provision with a simple carve-out that gives states carte blanche to invoke national security as a reason for non-compliance with the agreement, including the e-commerce rules.[50] Presumably they would want the same in the WTO, for their own defensive reasons – something similar was proposed by the US, Australia, Pakistan and Mauritius for the e-commerce annex in TiSA[51] - but that would require

giant-huawei/5662933; Fran O'Sullivan, 'Power of the Five Eyes in Huawei Ban', *New Zealand Herald,* 19 December 2018, https://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=12179007

[48] Eg TPPA Article 14.16, and USMCA Article 19.15

[49] Akande, D. and Williams, S. (2003) 'International Adjudication on National Security Issues: What Role for the WTO?', *Virginia Journal of International Law*, 43: 365-404; Hahn, M.J. (1991) 'Vital Interests and the Law of GATT: An analysis of GATT's security exception', *Michigan Journal of International Law*, 12: 558-620; Zillman, D.N. (1994) 'Energy Trade and the National Security Exception to the GATT', *Journal of Energy and Natural Resources Law*, 12: 117-27; Cann, W.A. (2001) 'Creating Standards and Accountability for the Use of the WTO Security Exception: Reducing the role of power-based relations and establishing a new balance between sovereignty and multilateralism', *Yale Journal of International Law*, 26: 413-85.

[50] TPPA Article 29.2; USMCA Article 32.2

[51] TiSA, Annex on Electronic Commerce, July 2016, Article 13

acceptance of separate chapter or amendments to the GATS. However, that sweeping provision would be available to any signatory to the agreement, including China!

The Straitjacket of the Trade Paradigm

That overview of meta-level issues indicates some of the reasons why the recent negotiation of digital trade rules is so controversial. The mesa-level question is how the choice of the trade arena frames and constrains digital governance rules. In particular, are trade ministers, officials and negotiators sufficiently aware of the implications of these new rules for the government's ability to regulate the digital domain in the future, and if they are, do the parameters and priorities of trade negotiations ensure they are giving them sufficient weight? Further, does the secrecy that has enveloped negotiations, especially the TPPA, preclude consideration of the broader ramifications and testing of the advice provided by and to officials in theshadows?

The sweeping catchment of rules in e-commerce chapters mirrors that of trade in services: the disciplines apply to measures, defined inclusively as any law, regulation, procedure, requirement, or practice,[52] that already exist or are adopted in the future by a Party that *affect* trade by electronic means.[53] As Simon Lester of the Cato Institute observed, the rules may apply to general policies, not just to trans-border activities. Likewise, the requirement of unfettered transfer of information across borders applies 'where the activity is for the conduct of a business'[54], and is agnostic about the value or otherwise of that business.

A trade paradigm privileges market and commercial considerations over other factors. New Zealand's policy briefs on e-commerce were consistently framed in economic terms of contributing to economic growth, and avoiding or minimising barriers to its use and development.[55] The TiSA consultation document on e-commerce asked submitters only to identify barriers, restrictions, burdens, and risks from an industry perspective.[56] Competing public policy priorities, other economic, social, cultural or considerations, and constitutional, indigenous, human rights and international treaty obligations are not just subordinated in the consultation process, they are invisible. Where they do appear in other documents, they follow a template of safeguards, exceptions and defences that are subject to formulaic chapeaux and contingent language, such as 'necessary', 'legitimate public policy objectives' and 'arbitrary or unjustifiable discrimination', whose meaning is derived through a trade-liberalisation lens. For example, New Zealand's approach to TiSA was to facilitate trade by seeking rules that support information technology services trade and restrict 'trade protectionist' rules, while ensuring that exporters can deliver in the manner oftheir

[52] TPPA Article 1.3
[53] TPPA Article 14.2.2
[54] TPPA Article 14.11.2
[55] TPP Negotiating Mandate, 9 September 2010; 'Trans-Pacific Partnership: Updated Mandates, 31 March 2012 (MFAT OIA)
[56] Information technology services and agreements on services trade, 8 March 2016, (MFAT OIA)

choosing, and 'future proofing' in a fast-moving area by seeking flexibility to respond to 'legitimate public policy issues'.[57]

The driving presumption of trade *liberalisation* militates against the protection of policy space to re-regulate in a more restrictive way. When converting into legal text, it is rare to find policy space preserved for the future; concessions like non-conforming measures for services and investment chapters apply only to some provisions, may apply a standstill and ratchet, and are heavily negotiated. General exceptions apply only to certain public policy objectives (for example, not explicitly to labour or human rights), most are subject to a necessity test, and all are governed by the chapeau. It is rare for officials to point out to lay people, including ministers and the public, that the ordinary meaning of these words is constrained by trade jurisprudence.

The National Interest Analysis was required to address advantages and disadvantages of the ecommerce chapter. It extolled the potential for e-commerce to generate economic growth and development, while offering no evidence that the *new rules* would bring any tangible economic benefit to New Zealand firms.[58] On the disadvantages, it downplayed new obligations. While acknowledging there were new areas that went beyond the 'specifically trade' focus of New Zealand's earlier agreements, it portraying them as consistent with internationally developed frameworks and reciting the bland assurances on legitimate public policy, consistency with international model frameworks, and supporting consumer confidence.[59] Potential impacts on the creative sector of non-discrimination on digital products (not dealt with in this paper) were glossed over. There was no explicit reference to rights to transfer information offshore until the more detailed discussion later in the NIA.[60] These are omissions which technical experts can fault, but no general reader or even person from the sector would know. Further on, there are unsubstantiated claims that the chapter is expected to support New Zealand's digital culture, with an assurance that the government has secured current policy settings. These assertions can be made with complete confidence that even if they are exposed there will be no consequence.

More frank exchanges may occur between officials – for example, a privacy official's record of advice from MFAT, although heavily redacted, appears to show a reservation that 'arbitrators are too quick to find' arbitrary or unjustifiable discrimination, a standard term in the chapeau.[61]

Very rarely, there may be genuine carve-outs, but even here the scope needs to be read very closely – for example, an exclusion for 'government procurement' in an e-commerce chapter may only

[57] Information technology services and agreements on services trade, 8 March 2016
[58] Trans-Pacific Partnership National Interest Analysis, 25 January 2016, 66-68, 169-71, 258-
[59] MFAT, *CPTPP National Interest Analysis*, February 2018, 50-52
[60] Trans-Pacific Partnership National Interest Analysis, 25 January 2016, 170
[61] Noted in Blair Stewart to Marie Shroff, 13 August 2013, Released under the Official Information Act 1982 on 31 January 2019 (Privacy Commissioner OIA)

apply to the procurement process, not to the substance and terms of performing the contract.[62] Does the exclusion for 'Information held or processed by or on behalf of a Party, or measures related to such information, including measures related to its collection'[63] extend to requirements relating to information made by central or local government under statutes, by-laws or other measures, but are not on their behalf?

The liberalisation presumption commonly informs governments' negotiating mandates, which set current policy and regulatory settings as the base line. The possibility that governments may need to regulate in ways that impose new constraints on commercial interests is rarely considered. The implications of a standstill are reasonably predictable for goods, although questionable for policies like country of origin labelling or alcohol health warnings. Applying a regulatory status quo to government procurement or investment is more controversial, but the constraints and consequences are still largely foreseeable. For governments to bind themselves to current regulatory and policy settings for digital technologies, products and related services, especially cross-border services, is reckless.

New Zealand's negotiating mandate for the TPPA on e-commerce began in September 2010 as 'consistent with current policy settings' and 'we should resist the inclusion of provisions that go beyond our current policy settings'.[64] However, there was mandate creep even within that framing. By March 2012 they were 'working to keep within current policy settings', with a redaction that presumably put a caveat on that.[65] A year later there was concern about the breadth of the provision banning requirements to use local computer facilities, including servers, because the 'possible future applications and public policy dimensions remain unclear'.[66] Two months later, officials were signalling issues where outcomes could fall outside current mandates and where New Zealand would need to signal flexibilities (details redacted). As the e-commerce negotiations intensified in September 2013 work on 'newer and more controversial proposals' on cross-border transfer of information, location of computing facilities, and non-discriminatory treatment of digital products was proving complex, due to their cross-cutting nature and different regulatory approaches of countries. None, as then drafted, 'were identified as requiring any changes to New Zealand's applicable regulatory settings'. Some issues remained for the chief negotiators. Other topics, notably e-signatures, are so heavily redacted that I am unable to tell what wasdiscussed.

The function of trade officials also needs to be de-constructed in a de-personalised way. Their inclination, training and mandates are to bring negotiations to a successful conclusion, with

[62] TPPA Art 14.2.3(a) needs to be read in light of the Article 1.3 definition that is confined to the 'process' of obtaining goods or services for governmental purposes, and with a view to commercial sale or re-sale or use in production of goods or services for sale or re-sale – concepts which are undefined.
[63] TPPA Art 14.2.3(b)
[64] 'TPP Negotiating Mandate', 9 September 2010, 14 and 22 (MFAT OIA)
[65] Cabinet Economic Growth and Infrastructure Committee, 'Trans-Pacific Partnership: Updated Mandates', 31 March 2012, para 7 (MFAT OIA)
[66] 'E-commerce: Issues Outstanding on Draft Articles 12 and 14', 5 May 2013 (MFAT OIA)

concessions and trade-offs that reflect the relative power of individual countries and alliances and the significance of the issue vis-à-vis others of greater or lesser importance. The officials can only operate within the scope of negotiations agreed to at a political level on the advice of senior trade officials. As negotiations roll, their options are necessarily couched in trade concepts and legal terminology, however inappropriate that may be to the matters at hand. When they communicate with outsiders who oppose elements of that agenda, and sometimes ministries whose mandates require primacy to other policy objectives, they necessarily talk past each other, unless the latter are prepared to accommodate to the trade liberalisation paradigm.

Negotiators themselves are often stuck in chapter silos where they are not privy to or do not understand the cross-cutting implications of different chapters, or have a technical function to ensure legal consistency and coherence across the entire text. Turnover of officials and parallel negotiations adds to incoherence and loss of institutional knowledge. It was disturbing to read one communication on the TiSA e-commerce rules in September 2015 that said: 'what we need to begin doing is to build up our understanding of the proposals as they relate to our domestic policy settings, and to work out whether there are any potential fishhooks for us' – followed by redactions.[67]

Institutional relationships reflect the hierarchy of trade ministry and like-minded economic ministries over others, aside from peak agencies such as the Department of Prime Minister and Cabinet and possibly Treasury and the Reserve Bank. Sectoral or subject ministries and outside agencies are at particular disadvantage, suffering from a knowledge deficit on trade concepts and language, as well as being bit players in broader negotiations.

These problems are seriously exacerbated by the undemocratic, usually secretive, approach to trade negotiations, to which industry lobbyists have privileged access.[68] Even after the fact it has proved impossible for me to access the substantive advice provided by and to MFAT on e-commerce negotiations in the TPPA and TiSA. The request made in November 2017 was finally responded to in June 2018. The request for review of that has been with the Ombudsman since July 2018 and I have been told not to expect a draft response to respond to until March 2019. Under the Official Information Act it is impossible to seek judicial review of the original response until the Ombudsman's review is complete.

Micro-level: Three examples of how this played out

(i) Source code

[67] Email from TND to various agencies, all redacted, subject: Re: Trade in Services Agreement: Proposals on Local Content, Local Technology and Cross Border Data Flows', 3 September 2015 (MFAT OIA)

[68] For example, an email from MBIE to MFAT dated 21 September 2015 noted that MFAT met with InternetNZ, IITP, and TechNZ met with MFAT on the TPPA. (MFAT OIA)

Source code is the version of software that is written in programming language that humans can read which is then transformed into a machine code that can be understood by a computer. Article 14.17 of the TPPA imposes a sweeping ban on requirements to disclose source code:

> (1) No Party shall require the transfer of, or access to, source code of software owned by a person of another Party, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory.

Japan tabled this proposal, not the US, so it did not appear until after Japan joined the negotiations after the July 2013 round. This is fundamentally a trade secrets provision that belongs to the intellectual property chapter. It has been suggested that it appeared in the e-commerce chapter because intellectual property negotiators would never have agreed.[69] By this time the e-commerce text was largely concluded, aside from several key issues. The proposal was discussed at the ministerial meeting in February 2014.

The ban applies to mass-market software of products or products containing such software. That includes coding platforms like Microsoft's GitHub, smart products like refrigerators, fit bits, baby monitors or cars, and software for checking safety and emissions (as in the Volkswagon software emissions scandal in 2015). All raise issues of consumer protection, human rights, privacy and competition. There is serious concern that the ban prevents relevant regulatory authorities from requiring disclosure of course code to ascertain compliance with national laws. The EU-Japan FTA made an inept response to this by inserting an exception for 'requirements by a court, administrative tribunal or competition authority to *remedy a violation* of competition law', but not for an investigation to establish a violation.[70] NAFTA-II addressed the issue directly after it was pointed out to US negotiators by preserving the ability of a regulatory body or judicial authority to require that a source code or algorithm is made available for an investigation or judicial proceeding, subject to safeguards against unauthorised disclosure.[71] Matters other than competition, such as a breach of anti-discrimination laws, would need to rely on the general exceptions.

At the time of the TPPA's release, it was unclear whether source codes included the algorithms that they communicate. The US later specified algorithms[72] in the equivalent provision in the USMCA, so makes it possible to argue it is not covered in TPPA, depending on the travaux. Once algorithms are included, the implications of the ban are huge. It would apply to practises like targeted advertising, dynamic pricing, race and class profiling, employee surveillance, psychometric testing, insurance risk assessments, and much more.

The MFAT documents reveal no discussion of these implications during the TPPA negotiations. When briefing the incoming Minister in December 2017, officials assured him that the source code ban

[69] Private communication with a senior negotiator, not from New Zealand.

[70] Agreement between the European Union and Japan for an Economic Partnership, entered into force on 1 February 2019, Article 8.73

[71] USMCA, Article 19.16.2

[72] Defined in USMCA Article 19.1 simply as 'a defined sequence of steps, taken to solve a problem or obtain a result'.

'would be subject to the same exceptions (including policy space carveouts) as New Zealand's services and investment commitments.'[73] That doubtless sounded reassuring, but the negative lists of non-conforming measures for services and investment do not technically transpose to this provision, and if they did may be subject to a standstill and ratchet. Whether the officials do not understand the technicalities, they actually believe what they say, or they knowingly provide false assurance, makes no difference; these statements mislead. The briefing noted that the government could preserve additional policy space by legislating before the CPTPP comes into force, where there is a link to the domestic regime or where the NCM was subject to a standstill or ratchet, but officials did not consider 'that any of this limited subset of commitments is likely to meaningfully affect the above commitments'. I have no idea what that means, and the next two paragraphs were redacted.

The MFAT documents did address two issues on source code. The first related to the common practice of putting source code into escrow, a practice that is governed by contract and protected in the final provision[74]. The second was an exclusion for access to source code on 'critical infrastructure'. The final text has a carveout for 'software used for critical infrastructure'. However, critical infrastructure was deliberately not defined. Any dispute would refer to the travaux, but that is only available to the parties. It is clear that the computer-based control systems for services like transportation, electricity and telecommunications would be covered. At one stage MFAT officials suggested banking was accepted as critical infrastructure,[75] but there are no additional examples.

The US Department of Homeland Security defines 16 'critical infrastructure' sectors whose 'incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof'.[76] These sectors are chemical, communications, commercial facilities, critical manufacturing, dams, defence industrial base, emergency services, energy, financial, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials and waste, transportation, and water and wastewater systems. However, the focus on *infrastructure* may be problematic. For example, the US definition does not, on its face, extend to voting software. While government procurement is excluded from the chapter, that definition applies only to processes of procurement; it is unclear whether it would protect contractual requirements. Voting software procured by non-government agencies would not be protected.

Subsequently, officials advised the new Minister in finalising the SNZCEP upgrade, that 'the provision is subject to sufficient safeguards, such as not applying to instances where government is itself procuring software. The policy constraint it imposes is not a concern in relation to future regulation in New Zealand.'[77] The next paragraph is redacted.

[73] Trade Negotiations Division of MFAT, December 2017, p.2 (find in OIA response)
[74] TPPA Article 14.17.3(a)
[75] Email MBIE to TND, Re: E-Commerce [redacted] proposals, 22 October 2013 MFAT (MFAT OIA)
[76] US Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience, 12 February 2013
[77] SNZCEP Upgrade Closing Mandate (undated), para 51, (MFAT OIA)

Cross-border information flows and privacy

Data transfers: It recognised the Law Commission's review of privacy 'might recommend the kind of barriers the US doesn't like', even though they were still modest and targeted.[78]

The privacy provision in the e-commerce chapter of TPPA is Article 14.8 Personal Information protection. It requires Parties to have a national legal framework for protection of personal information of users of e-commerce, but there is no minimum standard.[79] Parties 'should' take into account principles and guidelines of relevant international bodies. A footnote to that provision says this obligation might be met through voluntary undertakings by commercial firms operating from offshore, including digital platform like Facebook.[80] If data is being held offshore there is no guarantee of what privacy rules might apply.

Official Information Act documents provided by the Privacy Commission reveal important insights into how different agencies view this outcome,[81] especially when read alongside the MFAT release. A Commission official clearly articulated to his counterpart in MFAT the paradigmatic conflict between the 'human rights motivation predominantly in the Council of Europe and UN and to a lesser extent in OECD and EU, with economic and trade considerations predominating in OECD, EU and APEC'.[82] In the context of TPPA negotiations, the former necessarily gave way to the latter: a common position whereby a country that meets baseline requirements should not put barriers in the way of data flows would, in reality, be constrained by the trade paradigm. The official was clear from the start that 'detailed, clear or enforceable data protection rules were not on the TPP agenda'.[83] Nevertheless, his early position assumed there should be an equivalence between the treatment of privacy and data flows: if there is no strong primary obligation for a domestic privacy framework in a country, then the discouragement of cross-border barriers should be 'expressed in a very mild way'.[84]

The obligation/exception structure of such provisions would not allow for that. As importantly, nor would the power asymmetry of e-commerce negotiations in which the US was the sole demandeur, until Japan joined in mid-2013. New Zealand and others with concerns over privacy were negotiating from the US text, and proposing defensive positions, knowing there would need to be trade-offs to finalise the overall deal. The potential landing zone for 'common ground' on privacy was somewhere between the original US demand to remove all 'barriers to cross border data flows' with no

[78] Blair Stewart (Privacy Commission) to Paula Wilson (MFAT), 19 April 2011 (Privacy Commissioner OIA)
[79] TPPA Article 14.8.
[80] TPPA Article 14.8 fn 6.
[81] Privacy Commissioner to Jane Kelsey, Response to Request under the Official Information Act 1982, 31 January 2019OIA (Privacy Commissioner OIA)
[82] Memorandum from Paula Wilson (MFAT) to Blair Stewart (Privacy Commission), 'E-commerce: Privacy Issues – TPP', 31 May 2011, 2 (Privacy Commissioner OIA)
[83] Ibid, 9 (Privacy Commissioner OIA)
[84] Ibid, 11, (Privacy Commissioner OIA) also OIA16

corresponding privacy framework, and Australia and New Zealand seeking safeguards that followed the standard form of exceptions – subjective language of 'legitimate' public policy objectives, no arbitrary or unjustifiable discrimination or disguised barriers to trade, and a necessity test, to be pleaded as a defence. The US played hardball throughout the negotiations. It was considered to be huge progress when the US took a 'more accommodating' stance as negotiations on the chapter were almost complete, and acknowledged that safeguards generated trust in e-commerce.[85]

Another reminder of the importance of perspective was a query on the application of the rules to information transfers 'carried out in connection with a covered person's business'. From a privacy perspective this was seen as 'extraordinarily vague and wide', giving special rights to businesses above other interests: 'What is so significant in the public interest to allow for transfers connected with a business? … A person's business can range from the unremarkable and socially useful right through to the practices that many societies would find quite abhorrent.'[86] The trade officials rationalised the reference to 'conduct of business' (the final wording[87]) as keeping the phrase within the scope of the agreement.[88]

The documents also illustrate the hierarchical interplay of ministries, and the relative impotence of subordinate ministries to influence the potential fallout. As the Ministry responsible, MFAT decided who would be consulted, when, shown what documents, and what was done with the advice. After several months of ad hoc discussions with MFAT in 2010, the privacy official being consulted advised the Commissioner he had :

> … raised explicitly the question of providing a formal position from the Privacy Commissioner on the document. I did this because the consultation to date had been fairly informal but, on the basis of the drafting I had now seen, I was somewhat worried that the TPP negotiations could turn out to be a very bad deal for privacy interests. In particular it seems to me that [the US] may try to require participant economies to forego the right to block cross-border data flows for reasons of privacy, but without any corresponding guarantee that there would be any privacy protections in place in the receiving economy. This seemed to me to be a perverse position to take in terms of a trade agreement trying to establish trust to promote e-commerce.[89]

That memorandum, and two similar documents, were not in the bundle released to me by MFAT under the Official Information Act.

The Privacy Commission official astutely observed that words are not what they at first seem: closer inspection of proposed wording 'revealed that it is not simply an endorsement of privacy protection

[85] Blair Stewart to Marie Shroff, 13 August 2013 (Privacy Commissioner OIA)
[86] Paula Wilson (MFAT) to Blair Stewart (Privacy Commission) 31 May 2011, 2 (Privacy Commissioner OIA); similarly Blair Stewart (Privacy Commission) to Michelle Slade (MFAT), 5 December 2012, heavily redacted, (Privacy Commissioner OIA)
[87] TPPA, Article 14.11.2
[88] Blair Stewart to Marie Shroff, 13 August 2013 (Privacy Commissioner OIA)
[89] Blair Stewart to Marie Shroff, 1 June 2011 (Privacy Commissioner OIA)

as much as a limitation on privacy protection'.[90] Likewise, the commitment for each Party to have a 'legal framework' for privacy would still allow a range of appreciation, including industry self-regulation schemes backed by contract law[91] - as, indeed, the final TPPA provision explicitly allows.[92] Further, the proposal that each party merely protects data 'in a manner it considers appropriate and necessary' was 'problematic', 'vague', and 'potentially very weak', because it anticipated countries deciding for themselves what standards are appropriate and expect others to respect that decision. Not knowing the standard of protection being offered was 'a blind trust, rather than rational trust'. Including such terms would lead external stakeholders to look very cynically and suspiciously on the TPP agreement.[93] While that wording was not retained, that remains the effect of the article.

Non-trade officials are dependent on the information and legal analysis provided to them, for example on the framing of the 'safeguard' around the standard chapeau in the exceptions and a necessity test. Equally, terms like 'legitimate public policy objectives' and 'proportionality' (aka a necessity test) that appear in other international documents seem reassuring[94]; yet they have quite different meanings when viewed from the perspective of a trade panel and through the lens of a human right to privacy. A more positive example cited earlier appears to show a reservation that 'arbitrators are too quick to find' arbitrary or unjustifiable discrimination.[95] In another internal communication, the official said his concerns tended to lie in another area, on which he lacked expertise.[96] What that topic was is totally redacted. It might have been ISDS, or financial services and/or data flows, or something else, but it is impossible to know.

Elsewhere, the official noted the suggestion that another part of TPP dealt with privacy or personal information, and his response might be quite different depending on how that other party proceeds.[97] It seems that provision had not been provided. That might refer to the sub-paragraph on privacy in the general exception, transposed from GATS Article XIV into the e-commerce chapter,[98] and which would be relied on if the safeguards in Article 14.8 were deemed not to apply. I can see no explanation of the exception or its severe limitations. For the exception to provide a defence, the impugned privacy measure must not only be implementing legislation that is itself compliant with the entire TPPA, including the e-commerce chapter, but it is also subject to a necessity test, meaning the approach adopted must impose the least burden on the affected commercial interests of the options that are reasonably available to the government, and is subject to the standard chapeau that it not constitute unreasonable or unjustifiable discrimination or a disguised restriction on trade to the benefit of local firms.

[90] Blair Stewart (Privacy Commission) to Paula Wilson (MFAT), 22 June 2011, 2 (Privacy Commissioner OIA)
[91] Blair Stewart (Privacy Commission) to Paula Wilson (MFAT), 31 May 2011, 3 (Privacy Commissioner OIA)
[92] TPPA Article 14.8.2 fn 6
[93] Blair Stewart (Privacy Commission) to Paula Wilson (MFAT), 31 May 2011, 3 (Privacy Commissioner OIA)
[94] Blair Stewart (Privacy Commission) to Michelle Slade (MFAT), 5 December 2012, 3 (Privacy Commissioner OIA)
[95] Noted in Blair Stewart to Marie Shroff, 13 August 2013, (Privacy Commissioner OIA)
[96] Blair Stewart to John Edwards (Privacy Commissioner) 13 January 2016 (Privacy Commissioner OIA)
[97] Blair Stewart (Privacy Commission) to Paula Wilson (MFAT), 22 June 2011, 4 (Privacy Commissioner OIA)
[98] TPPA Article 29.1.3 importing GATS Article XIV(c).

The Privacy Commission has its own constituency and stakeholders with whom it needs to maintain a long-term relationship, and statutory independence from government policy. It was acutely aware that TPPA rules could become publicly controversial and urged MFAT to recognise the potential fallout. The private view of the Commission's expert was quite sceptical of the privacy protections. But it publicly aligned itself with the government's position. It wrote only two blogs on the TPPA and privacy, right at the end of the negotiations, providing bland information from the ministerial statement and the text.[99] The section on privacy in the National Interest Analysis raised no flags.[100] A carefully crafted statement on the CPTPP ran the government line that significant changes had been made in the revised agreement – which was irrelevant to the privacy mandate – although there were no changes in the privacy area.[101]

Other internal communications reveal a different assessment. The Commission official anticipated mistrust from stakeholders, citing a critique by Australia's former deputy privacy commissioner Nigel Waters of the APEC rules that New Zealand and others were using as reference points.[102] By the end of negotiations, the Commissioner's briefing to the Minister of Justice said 'we have been encouraged by the gradual shift over many rounds of negotiations to an end point that is looking more supportable than earlier proposals'; however, the paragraph on public concerns was largely redacted.[103] An internal email in January 2016 on a critical article on the TPP on privacy[104] was more direct:

> I don't have any concluded view on TPP but I think many of the concerns in the article are fairly reasonably based. It's not a proper answer to Graham [Greenleaf]'s concerns to say the agreement is much better (less bad?) for privacy than what [the US] really wanted in the early negotiations but it might set things in perspective. The final agreement is soft on the positive privacy side of the ledger but not entirely silent.[105]

While the Privacy Commissioner's OIA response was much more helpful than MFAT's, there are still some important lacunae. Notably, the final TPPA included a side-letter between Australia and the US extending any new US commitments on treatment of personal information in its future FTAs to Australia, and an 'endeavour' do so for any more extensive privacy protections.[106] The text of a draft letter from the Privacy Commissioner to Ministers on that matter in January 2016 was withheld in

[99] Blair Stewart, 'TPP and Electronic Commerce', 6 October 2015, https://www.privacy.org.nz/blog/tpp-and-electronic-commerce/; Blair Stewart, 'TPP Text on Protecting Personal Information', 10 Nov 2015 https://www.privacy.org.nz/blog/tpp-text-on-personal-information/

[100] MFAT, Comprehensive and Progressive Agreement for Trans-Pacific Partnership. National Interest Analysis, February 2018, 50-51

[101] Blair Stewart, What's happening with the Trans-Pacific Partnership?, Privacy Commissioner, 15 December 2017

[102] Blair Stewart to Marie Shroff, 13 August 2013 (Privacy Commissioner OIA)

[103] Marie Schroff, Privacy Commissioner, to Hon Judith Collins, Minister of Justice, 4 September 2013, 2-3 (Privacy Commissioner OIA)

[104] Graham Greenleaf, 'The TPP Agreement: An Anti-privacy treaty for most of APEC', in *Privacy Laws & Business,* Issue 138, December 2015

[105] Blair Stewart to John Edwards, 13 January 2016, (Privacy Commissioner OIA)

[106] Hon Andrew Robb to Hon Michael Froman, 4 February 2016

full.[107] It is unclear whether it was sent to ministers, and if so which ones, and if it was whether the reactions recommended New Zealand seek to follow suit and was rebuffed, by the US or did not recommend doing so and why.

Te Tiriti and Maori data sovereignty

Perhaps the starkest illustration of trade myopia on e-commerce is the monocultural conceptualisation of data and the arrogation by MFAT of the right to decide whether there might be a Tiriti issue. It apparently never occurred to MFAT officials that Māori had any interests in this chapter that might require them to engage, so as to understand Māori views and actively protect Māori interests. For the purposes of this discussion, such action is posited as a minimum requirement under te Tiriti. Had they engaged with the knowledgeable people in the right way, they would have discovered that Māori data is a taonga protected in te Tiriti and over which they have tino rangatiratanga.

Faced with that conceptual dilemma, I am pretty certain that officials would have reframed the argument as an exception and looked for safeguards within the chapter and the Treaty of Waitangi Exception. As it stands MFAT did none of that. Its omissions, and the Crown's obligation to provide protection for data as taonga in the face of e-commerce rules, stand to be tested in Stage 2 of the Waitangi Tribunal claim on the TPPA (Wai-2522). The arguments are slated for hearing sometime in the first half of 2019.

The starting point is that data is a taonga. Data, and its uses or abuses, relate to whakapapa and identity, culture and language, spiritual and physical wellbeing. Data is at the core of mātauranga. Personal data is imbued with whakapapa and mana. 'Any data set identified as being a taonga … has an inherent mana, which needs maintenance through its use and application'.[108] Data is the vehicle through which Māori culture is depicted, transmitted, manipulated and commercialised. In all these senses, data is a taonga, protected by Te Tiriti, governed by tino rangatiratanga, and subject to corresponding obligations and responsibilities on the Crown. Māori have the right to exercise tino rangatiratanga over those taonga, as well as responsibilities as kaitiaki. The Crown has a corresponding obligation to recognise and actively protect that right. Failure to do so constitutes a denial of Māori Data Sovereignty and a breach of teTiriti.

The charter of Te Mana Raraunga, a Māori data sovereignty network of prominent kaumatua and academics, asserts that Māori data is subject to the rights articulated in the Treaty of Waitangi and the UN's Declaration on the Rights of Indigenous Peoples. Indigenous Data Sovereignty is

[107] Blair Stewart to John Edwards, 29 January 2016 (Privacy Commissioner OIA)

[108] Maui Hudson, Tiriana Anderson, Te Kuru Dewes, Pou Temara, Hemi Whaanga, Tom Roa, "He Matapihi ki te Mana Raraunga" – Conceptualising Big Data through a Māori Lens', in H. Whaanga, T. Keegan and M. Apperley, *He Whare Hangarau Māori — Language, culture & technology,* Te Whare Wānanga o Waikato at 64-73 at 69.

recognised as 'a significant issue for indigenous peoples as a means to exert control over their data resources' and:[109]

> Establishes a frame of reference that expects Indigenous involvement in the governance of data and raises questions regarding the proper locus of ownership and management of data that are about Indigenous peoples, their territories and ways of life … Indigenous Data Sovereignty reflects a desire for protecting collective interests in data which centre on access to data for governance (e.g. to realise Indigenous community aspirations), and governance of data (e.g., to control access to and use of Indigenous data).

Further, 'Māori Data Sovereignty recognises that Māori data should be subject to Māori governance and that Māori organisations should be able to access Māori data to support their development aspirations'.[110]

The need for effective and informed consent to the primary collection of data, a central concern in the Wai 262 claim on traditional knowledge, is particularly acute with digital technologies, where consent may be asserted on the grounds of passive consent or lack of information or effective choice. Secondary uses of data are even less likely to be consensual and potentially more exploitive: 'Subsequent uses, without explicit permission, through data linkage, data sharing, or data aggregation, create the potential for *kaiatanga* or (mis)appropriation'.[111]

This articulation of a Tiriti and tikanga based approach to data encapsulates the systemic problem with the narrow conceptualisation of the digital domain and its shoehorning into the rubric of 'trade', the primacy of commercial interests and objectives, and the exclusionary identity of the players and the process. Suggestions that measure to actively protect Māori interests are adequately safeguarded as a 'legitimate public policy objective' would, I am confident, be views as intrinsically offensive, as well as unconvincing. Even where the legitimacy of the objective is not contested, the measure must not constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade, and must 'not impose restrictions on transfers of information greater than are required to achieve the objective'.[112] As noted earlier, less restrictive alternatives might be said to include unenforceable voluntary arrangements.

The fall-back would be the Treaty of Waitangi Exception, included in all New Zealand's FTAs since 2000, albeit without consulting Māori. However, it can only apply to breaches of these e-commerce rules where the measure gives more favourable treatment to Māori. Given the nature of data and electronic transmissions, Māori-specific rules would be intrinsically difficult without first adopting general regulations, that do not give preferential treatment. A two-step process would likely be

[109] Ibid at 64-65.
[110] Ibid at65.
[111] Ibid at68.
[112] TPPA Article 14.11.3.

necessary, such as a requirement that data is held inside the country, which is then subject to a Tiriti-compliant regime consistent with Māori Data Sovereignty.

Reflections

Few developments in international trade law will be more significant than the highly contested pursuit of global, or even regional, rules in the name of electronic commerce or digital trade. As yet, digital trade or e-commerce chapters are poorly understood, even by those who are negotiating them. Governments are signing on to them in ignorance. As new digital technologies, applications and abuses pose additional policy and regulatory challenges, this sleeping giant will stir. If these rules are adopted, expanded and enforced they will at worst prevent, and at least have a chilling effect on, the ability of future governments to regulate the digital domain in the public interest.

This paper has dissected the giant and traced its pathology through three levels: the *meta-level* issues of development, public interest, wealth distribution, geopolitics and security that already infuse debates about the future direction of global trade rules, and are at the core of emerging challenges to the digital trade agenda; the *meso-level* at which those broader concepts, concerns and interests are converted into the subject of trade negotiations and agreements; and how this plays out at the *micro-level* through the engagement of New Zealand's trade bureaucracy with specific matters of privacy, source codes and Maori data sovereignty. That analysis leads me to conclude that we are being led down cul-de-sac from which there few options for regulatory exit. It is too late to prevent that mistake in relation to the CPTPP, at least until it is reviewed. But we should not replicate it elsewhere. We need a commitment to preserve the remainder of our space to regulate the digital domain into the unforeseeable future. The government promised a new inclusive and progressive trade strategy. This is where it shouldstart.

JacksonStone House
3-11 Hunter Street
PO Box 1925
Wellington 6140
New Zealand

[redacted]
cbeard@exportnz.org.nz
www.exportnz.org.nz

1 July 2019

Ministry of Foreign Affairs and Trade
Wellington
New Zealand
Via email: e-commerce@mfat.govt.nz

DIGITAL ECONOMY PARTNERSHIP AGREEMENT (DEPA) NEGOTIATIONS

About ExportNZ

ExportNZ is a national industry association comprising of eight regional offices and representing a diverse range of exporters throughout New Zealand. ExportNZ is a division of BusinessNZ, New Zealand's peak business advocacy body.

We are a membership organisation and across our two brands have approximately 2,000 members. We also have four regional partners: Employers Manufacturers Association (Upper North Island), Business Central (Lower North Island), Canterbury Employers Chamber of Commerce (Upper South Island) and Otago Southland Employers Association (Lower South Island).

Our value proposition for members is a mixture of policy and advocacy, education and training, networking, trade missions and inspiration through awards events and conferences.

Submission

ExportNZ welcomes the opportunity to submit on the Ministry of Foreign Affairs and Trade consultation on the Digital Economy Partnership Agreement (DEPA) negotiations.

The digital economy has enabled a wide range of businesses to engage with global markets, without the traditional barriers of needing to ensure scalability

or the same scale of in-market investment to gain proofs of concept. For the New Zealand context, this has many advantages. We have many businesses in our ExportNZ network that have used e-commerce platforms and/or digital marketing to test market responsiveness and build market profile and customer engagement before expanding into a traditional in-market presence. This has also enabled them to build relationships directly with their customer audiences and increase the probability of tangible sales discussions. E-commerce solutions and digital marketing also provides opportunities for small and medium enterprises (or in the global context, often micro enterprises) to gain a global customer base, allowing a more diverse range of businesses to spring up in NZ, exploit niches, and achieve success that may not be sustainable if the business relies solely on domestic sales.

We see a strong rules-based multilateral system as critical to promoting trade and digitally-enabled trade ensuring continued growth across all exporting sectors. This applies to micro, small and medium sized enterprises (SMEs) also, in developed and developing countries alike. However, that multilateral system must remain relevant to the commercial challenges facing businesses both large and small while fostering inclusive economic growth.

For services, this means that the multilateral rules must be expanded to encompass and promote digital trade, including cross-border data flows, prohibitions on requiring data localization, a permanent moratorium on e-commerce tariffs, non-discriminatory treatment of digital products, relevant market access commitments in areas such as financial services, ICT and logistics, and trade facilitation.

All trade in goods and services – from the placing of an order to confirmation of delivery – now involves the electronic transfer of data. Data-transfer is today's all-purpose means of business communication, spurring economic growth and innovation in all industries. We see with concern, for example, the appearance of certain forced data localisation policies and practices, that may threaten to disrupt the continued growth and success of trade and commerce worldwide.

In taking on the task of forging DEPA and crafting rules that facilitate the flow of trade in goods and services, there needs to be trust among individuals that their personal data will be securely held and handled according to local privacy rules; and there needs to be certainty for businesses that data protection regimes will be transparent, predictable, and as least trade restrictive as possible. We recognise that data-security and appropriate and effective protection of personal data are essential and must be assured through compliance with local privacy and security regulations. Any exceptions to the principles promoting cross-border data flow and avoiding forced localisation should be limited to legitimate public policy objectives and be non-discriminatory. In fact, we believe New Zealand could use DEPA as an opportunity to define a framework for data localisation rules with our negotiating partners.

We also recognise the focus on data must also be accompanied by appreciating the linkages between the digital economy and the physical movement of goods. While the digital environment opens up many new avenues for consumers, customs authorities must ensure border procedures support the movement of goods across borders as seamlessly as possible.

While there are challenges in the swiftly changing digital economy environment, we see the digital economy as holding many additional opportunities for our government's key priorities. Given the Trade For All agenda, the digital economy has the ability to support SMEs, women in trade and Maori business. There are also opportunities for NZ to support Pacific Island countries in enabling their growth through utilising e-commerce platforms rather than traditional means of trade.

It is critical that New Zealand, especially as a small nation heavily reliant on the global trade market, is instrumental in shaping a trade-friendly global framework for the digital economy, and we support NZ's involvement.

Thank you for the opportunity to submit on the consultation on the Digital Economy Partnership Agreement (DEPA) negotiations.

Yours Sincerely,

Catherine Beard
Executive Director
ExportNZ

1 July 2019

Ministry of Foreign Affairs and Trade
Via email: e-commerce@mfat.govt.nz

Dear Sir or Madam,

Digital Economy Partnership Agreement (DEPA) negotiations

Chartered Accountants Australia and New Zealand (CA ANZ) welcomes the opportunity to provide a submission to the Ministry of Foreign Affairs and Trade (MFAT) on the Digital Economy Partnership Agreement (DEPA) negotiations.

We have focused our feedback on the key areas where we consider we can add the most value. Appendix A provides our detailed submission and Appendix B provides more information about CA ANZ.

Key Points:

- We recommend the Government nominates an entity, such as the Ministry of Business, Innovation and Employment, to raise awareness of, and provide education on, the risks and support available to digital economy participants.
- The Government should consider practical support for small to medium entities (SMEs) as they adapt their business infrastructure to the changing nature of payment practices through digital technologies.
- We support progressing e-invoicing through DEPA.
- We suggest DEPA includes provisions safeguarding consumer and SME access to internet communications and minimising the risk of anti-competitive behaviour by dominant players. This could be achieved through a commitment to net neutrality.
- Privacy and data protection safeguards that appropriately balance privacy rights and encourage innovation in the use of data sets should be built in to DEPA.
- We support DEPA including provisions for an Artificial Intelligence ethical framework.

Should you have any questions about the matters discussed in this submission or wish to discuss them further, please contact Karen McWilliams via email at karen.mcwilliams@charteredaccountantsanz.com or phone [redacted].

Yours sincerely

Peter Vial FCA
Group Executive – New Zealand & Pacific
Chartered Accountants Australia and New Zealand

Karen McWilliams FCA
Business Reform Leader
Advocacy & Professional Standing
Chartered Accountants Australia and New Zealand

General comments

Chartered Accountants ANZ supports the Digital Economy Partnership Agreement (DEPA) negotiations and MFAT's openness to including the views of the public in shaping negotiations. These negotiations are timely given New Zealand's changing export mix, and will encourage further development of higher value services-based trade.

In 2018, Chartered Accountants ANZ provided a submission to the Ministry of Foreign Affairs and Trade on the Trade for all Policy. In this submission we provided key recommendations to Government including working with businesses to examine the barriers to service export growth and the importance of digital technology. We also provided in the submission general comments from our two thought leadership papers in 2017, *Quest for Prosperity – How can New Zealand keep living standards rising for all?* and *The Future of Trade- Are we ready to embrace the opportunities?* MFAT may wish to consider them in the lead up to DEPA negotiations.

Encouraging digital economyparticipation

In our view, a nominated government entity, such as the Ministry of Business, Innovation and Employment, should raise awareness and provide education on the risks of, and support available to, users (including businesses and consumers) in a digital economy. The nominated entity could play an active role in building trust by highlighting the benefits for business and consumers of buying and selling (and other related activities) in a digital environment.

We recommend that Government examines existing consumer support mechanisms to determine how these can be adapted to keep up with the changing pace of trade in the digital era.

Small to Medium business

Some of our members who either own or work within small to medium businesses have continued to note that late payments, and other adverse payment practices, are critical issues. As digital trade increases in popularity, many small to medium sized businesses may not have the resources to adapt their businesses' infrastructure to the changing nature of payment practices. We recommend that Government considers practical support, in particular to those transitioning to the use of digital technologies for the first time.

E-invoicing

E-invoicing has the potential to make billing and payments processes faster, more accurate, and more efficient through the exchange of invoice data between suppliers' and buyers' financial systems. This can assist cash flow management, a major factor in the success and failure of small businesses due to the often significant disparities in payments terms between small and large businesses.

We support progressing e-invoicing through DEPA. The Australian and New Zealand Governments recently announced that the trans-Tasman e-invoicing initiative will use the Pan European Public Procurement Online (PEPPOL) framework, which is also in use in Singapore and in other countries across Europe, Asia and North America. We recommend that the PEPPOL framework also be the basis for e-invoicing interoperability in DEPA.

Alevel playing field online

Access to fast and high quality internet communications is critical in a thriving digital economy. We recommend that the Government consider including net neutrality requirements in DEPA. Net neutrality, in essence, is the principle that internet service providers (ISPs) treat access to data equally irrespective of the content (so long as it is legal), platform, application, or method of communication. Where ISPs are able to discriminate, for example by throttling data or charging more for data for certain platforms or websites, there is a risk of anti-competitive behaviour by dominant players. Those most affected are likely to be non-market dominant SMEs and consumers.

We understand that Singapore and Chile both have some form of legal protections for net neutrality / internet access. We recommend that the New Zealand Government ensures through DEPA that New Zealand companies and consumers are protected and that unencumbered access to internet communications services in Singapore and Chile is assured on the same basis as for local companies and consumers.

Privacy safeguards and data protection

Consumers are increasingly concerned with protection of their personal data, particularly in the age of big data and social media. At the same time, big data sets and an open global information economy provide commercial opportunities. It is important that our trading partners have appropriate safeguards for personal data and that there are clear and easy to follow rules for businesses. We recommend that DEPA ensures there are appropriate privacy and data protection standards in New Zealand, Chile and Singapore.

DEPA policy goals alignment and the digital services tax proposal

We support the Government's intention to promote digital trade and to implement robust, transparent and interoperable trade rules. DEPA negotiations can directly contribute to achieving these goals. However, the Government's proposal for a unilateral digital services tax is incongruent with these policy goals; our view is that it will dis-incentivise innovation and investment in digital commerce in New Zealand, actively working against what DEPA seeks to achieve. We are submitting separately to Inland Revenue on the digital services tax proposal and our support for New Zealand continuing to seek a multilateral agreement through the OECD. We consider it important that all parts of Government are working cohesively towards the same policy goals.

Open data

We commend the Government for its commitment to open data in New Zealand; improving accessibilityto public data can promote transparency, confidence in institutions, and provide opportunities for commercial and public sector innovation. New Zealand and Chile have adopted the International Open Data Charter, which contains the principle that government data should be open by default. Singapore however has not adopted the charter. We support DEPA including commitments to open data in all three countries and suggest that officials explore the possibility of progressing open data interoperability standards.

Artificial intelligence

There is the potential for significant commercial opportunities through artificial intelligence (AI) technology but these come with risks, for example privacy impacts and the ethical implications of automated

decision-making on consumers and workers. We have previously considered some of these issues in our discussion paper *Machines can learn, but what will we teach them?*

We note that Australia is currently developing an ethical framework for AI. We support DEPA including provisions for an AI ethical framework or a process to develop agreed minimum standards for AI use and development across the three countries.

About Chartered Accountants Australia and New Zealand

Chartered Accountants Australia and New Zealand is a professional body comprised of over 120,000 diverse, talented and financially astute members who utilise their skills every day to make a difference for businesses the world over.

Members are known for their professional integrity, principled judgment, financial discipline and a forward-looking approach to business which contributes to the prosperity of our nations.

We focus on the education and lifelong learning of our members, and engage in advocacy and thought leadership in areas of public interest that impact the economy and domestic and international markets.

We are a member of the International Federation of Accountants, and are connected globally through the 800,000-strong Global Accounting Alliance and Chartered Accountants Worldwide which brings together leading Institutes in Australia, England and Wales, Ireland, New Zealand, Scotland and South Africa to support and promote over 320,000 Chartered Accountants in more than 180 countries.

We also have a strategic alliance with the Association of Chartered Certified Accountants. The alliance represents 788,000 current and next generation professional accountants across 181 countries and is one of the largest accounting alliances in the world providing the full range of accounting qualifications to students and business.

Fonterra position paper on e-commerce

Introduction

E-commerce is growing in prominence as a channel to an increasing number of markets for Fonterra's products, and e-commerce models operating globally are evolving rapidly to meet growing consumer demand and preferences. As a major dairy exporter exporting to more than 140 markets and with sales offices, customers, and consumers around the world, Fonterra has a strong interest in e-commerce disciplines being developed in key markets. Related issues around data, privacy and cybersecurity are particularly important, with disciplines developed through domestic policy and regulatory mechanisms, as well as the World Trade Organisation (WTO) and New Zealand's Free Trade Agreements (FTAs). This paper aims to provide an overview of Fonterra's current and future e-commerce interests, and recommendations for policy-makers and negotiators.

E-commerce overview

2 Fonterra is currently utilising e-commerce platforms as a channel to market in a number of different ways, including Global Dairy Trade marketplace (online store for dairy ingredients), general e-commerce trade (B2B or B2B2C) and cross border e-commerce (CBEC) which involve the sale of goods across e-commerce platforms. A brief overview of the models is outlined below:

- ***General e-commerce trade (B2B or B2B2C)*** The majority of Fonterra's e-commerce trade is carried out via e-commerce sales within national borders. This means that products are either imported directly, or manufactured locally, and then sold on an e-commerce platform, with the customer invoiced by a local entity. All these activities occur within the national borders of the country.

- Alternatively, bulk product may be sent to a free trade zone or bonded warehouse where the product is then repackaged or sent directly by fast freight (e.g. FedEx) to the consumer (B2B2C).

- The regulatory, customs and tax requirements in key markets such as China generally remain the same as for general trade. Fonterra is selling products via e-commerce platforms using these models in a number of markets including China, Australia, South East Asia, and the United States.

- ***Cross border e-commerce (CBEC)*** In addition, a small but growing percentage of Fonterra's e-commerce trade is exported via the CBEC channel, directly from Fonterra to the consumer via an e-commerce platform or distributor.

- Currently, Fonterra is only engaged in cross-border e-commerce in China, where the Chinese Government has established specific regulations to govern the trade of CBEC for goods included on a 'positive list'. The regulatory and customs requirements for export from New Zealand remain the same, but for the goods entering China there is no tariff, a reduced sales tax, modified language labelling requirements and Chinese consumers are limited to a regulated amount and value of product each year. At a general level, this approach has supported the growth of Fonterra's CBEC trade into China.

- Given the high value products that are typically traded via CBEC channels, we expect to see continued growth in this channel and the expansion of its use into new markets.

- ***Global Dairy Trade (GDT) Marketplace*** GDT Marketplace is an online dairy trading hub that provides a platform for buying and selling dairy globally, acting like a global shop front and directly connecting businesses. While it is owned by Fonterra Cooperative Group, it is operationally and physically separate from Fonterra. The regulatory, customs and tax requirements remain the same as for general trade.

E-commerce: a growing and valuable channel for Fonterra

3 As noted above, e-commerce is growing in prominence as a channel to an increasing number of markets for Fonterra, and e-commerce models operating globally continue to evolve.

4 To give a sense of the scale of cross-border trade for Fonterra, e-commerce and omnichannel (a multichannel approach to sales that seeks to provide customers with a seamless shopping experience, whether shopping online from a desktop or mobile device, by telephone, or in a brick-and-mortar store) now accounts for 55%+ of total Fonterra sales in China. China is, Fonterra's largest market and sales via these channels have grown at ~80%+ volume p.a. over the past 3-4 years.

5 The majority of Fonterra's e-commerce trade occurs via general e-commerce trade, with a small but growing percentage (approximately 5%) of Fonterra's e-commerce trade with China exported via the cross- border e-commerce (CBEC) channel directly to the consumer through a Fonterra distributor.

6 Fonterra utilises global e-commerce platforms such as GDT, Alibaba (China), Amazon (US, Australia), or Lazada (South East Asia). As such, while this trade is subject to regulations and customs requirements in both the importing/exporting country, the specific terms of the transaction – such as customer data, trading terms, pricing etc - are determined by the specific e-commerce platforms. The size and relative influence of these platforms in key markets can mean that there is little room to negotiate or shape these terms for exporters.

7 Looking ahead at how these channels may evolve, and reflecting the growing inter-connectedness of global supply chains, it is possible to envisage Fonterra utilising a centralised hub for re-exporting via e-commerce channels (e.g. where in theory product is exported from New Zealand, stored in Malaysia, and re-exported to Vietnam).

8 Given the high value products that are typically traded via cross-border channels, we expect to see continued growth in this channel, and the expansion of its use into new markets and models based on the trends observed in China. As noted above, where specific policy approaches have been developed, these appear to have been driven by specific e-commerce platforms, or individual countries, rather than through a global or multilateral approach.

Considerations around data, privacy, and cybersecurity

9 As a global company headquartered in New Zealand and exporting to more than 140 markets worldwide, Fonterra collects, stores, manages, analyses and transfers significant amounts of data within and between jurisdictions. The type of information includes, but is not limited to, data relating to customers, employees, vendors, suppliers, products, consumers, sales, and financials.

10 In addition, an authorised third party (such as a Fonterra supplier, vendor or partner) may collect data on behalf of Fonterra and is subject to local laws and regulation in the jurisdiction in which they operate.

1 July

11 The ways in which Fonterra is utilising and managing these types of data across our supply chain and wider business is not static and is constantly evolving. Currently, existing uses for data within Fonterra can range from customer-related data contained in our Salesforce customer management system, to the use of blockchain technology and Quick Response (QR) codes across our supply chain to enhance traceability and transparency and ensure food safety and quality.

12 Fonterra's ability to move data freely within and across borders, while ensuring the safety and security of sensitive information (such as IP, customer, or economic and market sensitive data) is critical.

13 The diversity of regulatory approaches to issues around cross-border data flows, interoperability and standards, or approaches to personal data protection and privacy globally does not reflect the global nature of commerce and creates operating challenges, adds complexity and uncertainty, and significantly increases compliance costs for a company like Fonterra which is operating at scale across multiple jurisdictions.

14 While some of these approaches are aimed at meeting a legitimate public policy goal, the design of the policy or regulation may unintentionally restrict trade more than necessary to meet the objective. In other instances, the purpose of such restrictions may be outright protectionist, designed to favour domestic competitors or create localjobs.

15 Fonterra therefore supports disciplines and regulatory approaches that enhance transparency, the free flow of data across borders, privacy and cybersecurity in order to facilitate commerce, enhance trust and social licence to operate.

16 We recommend that such approaches must be consistent and transparent, developed using good regulatory practice, and in close consultation with the private sector to ensure they do not unnecessarily restrict trade and commercial activity.

17 Consistent with this approach, we provide the following recommendations for policy-makers and trade negotiators.

Recommendations

18 Fonterra recommends that when considering domestic policy development and in the WTO/Digital Economy Partnership Agreement (DEPA) e-commerce negotiations and e-commerce chapters in other FTA negotiations currently underway, the New Zealand Government build on e-commerce provisions in existing FTAs (such as the Comprehensive and Progressive Trans-Pacific Partnership Agreement, CPTPP) to facilitate e-commerce and the free flow of data across borders, whilst at the same time ensuring consumer safety and rights.

19 This could include the following:

1) Consider New Zealand domestic policy settings (customs, biosecurity, food safety, tax etc) to enable businesses to capture the value generated through cross-border e-commerce channels, whilst maintaining our regulatory standards and reputation as a reliable trading partner and producer of high-quality, safe and suitableproducts.

This includes ensuring that New Zealand's domestic tax regime is supportive of e-commerce transactions (for both imports and exports) and in line with OECD Frameworks in order to deliver on the G20's stated aim of avoiding uncoordinated and unilateral actions.

2) Identify and develop international best practice and alignment for customs clearance, tax and regulatory requirements for e-commerce trade in goods, (particularly where these differ from general trade requirements) through relevant international organisations (e.g. WTO, WCO, OECD, APEC) and encourage greater transparency, harmonisation and/or systems recognition, particularly in relation to the following issues:

    a. Simplification of labelling requirements, including language requirements
    b. Simplification of product and factory registrations
    c. Product eligibility requirements (e.g. health certificates, halal, composition, certificate of origin requirements) as well as label registrations.
    d. Tax requirements, particularly where these differ from generaltrade
    e. Tariff treatment, particularly where these differ from generaltrade
    f. Volume limitations, particularly where these differ from generaltrade

    Best practice recommendations should also be considered for inclusion of relevant ongoing workstreams (e.g. the WCO Working Group on e-commerce, the Agreement on Trade Facilitation and the Revised Kyoto Convention (currently under review)).

3) The application of trusted trader principles/approaches for general trade (ie. New Zealand Customs Secure Export Scheme) to be considered for e-commerce. Inspection rates for trusted/approved exporters should be very low, compared to a package from a new provider or infrequent supplier. These principles should be aligned with those used for commercial shipments and focus on 'high risk' cargo/export countries.

4) Encouraging countries to adopt a consistent and high *de minimis* threshold for e-commerce trade. In addition, when the value of products imported via cross-border e-commerce for personal consumption is less than the *de minimis* level, such products should also be exempt from market access and regulatory requirements that commercial quantities are subject to. This approach would be facilitative and supportive of growing high value CBEC exports in a wider range of markets.

5) Enhanced and standardised electronic certification and paperless trading systems and provisions to allow the sharing of information to streamline clearance processes, reduce costs and improve efficiencies.

6) A prohibition on data localisation requirements and other restrictions on cross border data flows, including on the basis of cybersecurity or national security concerns. Any exceptions to this should be required to be on the basis that they are designed to meet a legitimate public policy outcome and be as least trade restrictive aspossible.

7) While recognising the rights of countries to regulate, domestic laws relating to the mandatory provision of data should only be permissible in countries with equivalent privacy protections and with a stated intent for use only for legitimate and specific purposes e.g. criminal enforcement.

8) Policy approaches to personal privacy or cybersecurity requirements that are no more burdensome than necessary to meet the stated objective.

9) Greater coherence around regulatory and legislative approaches to privacy, data and cybersecurity to reduce complexity and costs for businesses operating across multiple jurisdictions.

1 July

10) Ensuring New Zealand's 'adequate country status' enjoyed under the previous EU data protection directive is maintained in the EU's General Data Protection Regulation (GDPR).

11) The application of competition policy to e-commerce platforms in order to enhance transparency, support consumer choice, and competition.

12) A permanent moratorium on tariffs on electronic transmissions.

13) Provisions that provide regular opportunities for e-commerce provisions to be reviewed and enhanced with appropriate private sector input, recognising the potential growth and rapid evolution in supply chain and e-commerce technology.

Trade Strategy and Global Stakeholder Affairs
Fonterra Co-operative Group
1 July 2019

ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

July 2, 2019
Trade Negotiations Division
New Zealand Ministry of Foreign Affairs and Trade
195 Lambton Quay
Wellington, 6160, New Zealand

Dear Ms. Alison Hamilton,

The Information Technology and Innovation Foundation (ITIF) appreciates the opportunity to make a submission to the New Zealand Ministry of Foreign Affairs and Trade's inquiry into the recently launched negotiations with Chile and Singapore for a Digital Economy Partnership Agreement.

ITIF is a non-partisan, non-profit think tank based in Washington D.C. which focuses on the intersection of technological innovation and public policy. Ranked the world's top science and technology policy think tank in the latest edition of the University of Pennsylvania's Global Go To Think Tank index, ITIF provides research and advice to policymakers around the world on a range of pertinent issues, including digital trade, intellectual property, advanced manufacturing and automation, the Internet of Things, and data-driven innovation.

Sincerely,

Nigel Cory
Associate Director, Trade Policy, The Information Technology and Innovation Foundation

CONTENTS

OVERVIEW

The central premise of New Zealand's effort to negotiate Digital Economy Partnership Agreements (DEPA) should be a recognition that data and data-driven innovation, and by extension, digital trade, are a force for good.[1] Across society, data innovation—the use of data to create value—is creating more productive and innovative economies, transparent and responsive governments, and better social outcomes (improved health care, safer and smarter cities, etc.).[2] But to maximize the innovative and productivity benefits of data, countries need to put in place the rules for an open, rules-based global digital trading system. Some issues will require prescriptive rules to support digital trade and to prohibit existing and potential barriers to digital trade. Others will require a focus on common principles and references to existing and emerging international best practices in order to create interoperable systems for data governance that support data flows and digital trade. New Zealand needs to keep pushing for new rules as the potential benefits of an open, innovative, and rules-based global digital economy are at risk as a diverse range of countries—especially China, India, Indonesia, and Russia—enact ever more extensive barriers to data flows and digital trade.[3]

As a relatively small, trade-dependent economy, New Zealand needs to deepen and extend its regional and global ambitions in digital trade if it wants to create the space for its firms to thrive in the global digital economy. New Zealand policymakers and firms need to recognize that there are multiple entry points into the global digital economy, many of which have been utilized by Estonia, Singapore, Sweden, and others to transform themselves into global technology leaders.[4] With the right domestic and international trade policies, the size of these economies does not have to be a limitation. Technology allows firms to access international markets with small "asset footprints," leading to the emergence of so-called micro-multinationals and the born-global firms that quickly attain global reach with minimal cross-border investment.[5] But New Zealand needs to enact the rules that protect the ability of domestic firms to leverage digital technologies to engage in digital trade.

New Zealand (along with Chile and Singapore) needs to use digital trade policy to build the economies of scale that are critical to the success of data-driven firms. One reason China and the United States have had considerable success in the digital economy is that their large internal markets allow local firms to achieve economies of scale. Recognizing this, the European Union (EU) is now striving to internally harmonize its own laws and regulations, even while inadvertently erecting new barriers. New Zealand is in competition with these countries and regions that are making data-driven innovation and digital development and adoption a centerpiece of their policies. To achieve similar scale and integration, New Zealand and likeminded partners must pursue an even more ambitious digital trade framework.

Failure to seize the initiative with an ambitious DEPA will hold back New Zealand's digital competitiveness. New Zealand's firms already face considerable barriers trying to engage in digital trade with China, India, and many other countries. These difficulties will only grow if new rules do not curb such barriers. Obviously, the global digital economy already owes policymakers from New Zealand and its partners in the Trans-Pacific Strategic Economic Partnership (known as the P4) a debt of gratitude for putting in motion the initiative which eventually culminated with the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), an ultimately positive development for digital trade protections. However, more needs to be done to achieve a larger, more seamless digital market for New Zealand firms. An ambitious DEPA

would also send a clear signal to other trade partners as to where the gold standard lies in terms of new and better rules for a truly open, competitive, innovative, and rules-based global digital economy.

Part of the challenge for New Zealand and its efforts for DEPA lies in looking ahead to address the challenges and opportunities as the next wave of information communication technology (ICT)-based innovations emerge. Advanced nations and regions are in the beginning stages of a major technology wave signifying a transformation to a more sophisticated, powerful, and wide-ranging digital system. This system will be much more connected (a massive number of "things" will be connected through more advanced networks), automated (devices and systems will enable more work to be done by "machines"), and smart (algorithms will play important roles in making sense of and acting upon information). As a shorthand, we call this system connected, automated, and smart (CAS).[6] Digital trade policy needs to account for these issues in the most effective and expedient way possible.

Obviously, an ambitious, proactive digital trade policy is only one part of the strategy New Zealand needs to implement to support its domestic digital economy. As it faces this next wave, New Zealand will need to consider three principal types of digital economy policies: foundational, field clearing, and proactive. Foundational policy activities are focused on addressing potential harms from ICT or ICT companies. Field-clearing policies are focused on clearing barriers and limiting future barriers to digital innovation. Proactive policies seek not only to open markets and enable digital entrants to compete, but to actively support digital transformation throughout New Zealand. Proactive policies represent an area of differentiation between economies. They include policies to expand and improve the resources firms rely on for success, including ICT research and development, data, broadband networks, and digital skills. Often implemented through public-private partnerships, proactive policies also support digital innovation and adoption in key technology areas that New Zealand wants to consider within DEPA, such as artificial intelligence (AI) and digital IDs. Other potential issues include high-performance computing, robotics, and key application areas such as health IT, smart grids, and smart cities.

New Zealand should use DEPA to set a new gold standard for digital trade. New Zealand should maintain its pragmatic approach to working with an initially small group of members to set an initially high bar in terms of new rules, before opening it up for others to join, but to vet potential partners based on their willingness to work towards the same level of ambition. This is far preferable to the two alternative approaches that define Internet policy—universalism and Balkanism.[7] These opposing approaches are why there has been little substantive progress in creating a framework for resolving the many conflicts over Internet policy as countries try to enforce their views on the rest of the world. Universalism fails because it attempts to apply a particular nation's worldview, such as promoting democracy and freedom of expression (as in the case of the United States), or a certain view of privacy (as in the case of the EU). Meanwhile, Balkanism stems from an unyielding desire to maintain political control (as in the case of nations such as China and Russia).[8] The DEPA and World Trade Organization (WTO) negotiations on e-commerce provide a better alternative in that they represent a realistic effort to achieve an ambitious agreement between a sub-group of countries that together recognize the value of an open, rules-based, and innovative global digital economy.

The following submission details the policy principles and rules that ITIF recommends for New Zealand's upcoming talks with Chile and Singapore. These recommendations exclude some of the obvious digital trade policies that New Zealand has already enacted, such as the prohibition of duties on digital products, on the grounds that they do not warrant further debate in a nation with an already-advanced digital trade policy.

SUMMARY OF POLICY RECOMMENDATIONS

1. DEPA should enact stronger rules to protect cross-border data flows by strengthening provisions that prohibit barriers to data flows by limiting the potential for countries to misuse broad, self-defined general exceptions to enact forced local data storage (known as data localization). New Zealand should push for language that explicitly states that data localization is not a legitimate policy to protect the privacy or security of data under most scenarios.

2. New Zealand should use DEPA negotiations to enact a framework for "global protections through local accountability" in relation to data flows, data-related legal responsibilities (such as for privacy, data protection, and regulatory access to data), and cooperation with counterparts on shared concerns raised by cross-border data flows (such as joint privacy investigations). Rather than tell firms where they can store or process data (i.e. data localization), policymakers should emphasize that they will hold firms accountable for managing data they collect, regardless of where they store or process it.

    a. New Zealand should use DEPA negotiations to announce that it plans to join the Asia Pacific Economic Community's (APEC) Cross-Border Privacy Rules (CBPR) system. Afterwards, it should reference APEC CBPR as an example of interoperability in DEPA text.

    b. New Zealand should use DEPA negotiations to prohibit measures that prevent the transfer of financial, tax, accounting, and payments data, and data associated with publicly listed companies. New Zealand should advocate for provisions that makes clear that what matters is not the location of data storage, but that relevant regulatory authorities have timely access to data (upon request). In line with this, New Zealand should remove its Inland Revenue Service's forced local data storage requirement for business records.

3. In tandem with DEPA negotiations, New Zealand should seek new or updated mechanisms with Chile and Singapore for managing cross-border requests for access to data for law enforcement purposes. Existing legal processes and treaties (such as mutual legal assistance treaties) are woefully out of date, needlessly complex, and often delayed due to poorly resourced local agencies. Policymakers enacting data localization often cite law enforcement concerns. The cooperation section of a digital trade chapter in DEPA could reference this cooperation to highlight the fact that the parties are addressing (in a positive way) the legitimate concerns law enforcement agencies might have while still allowing data to flow freely as part of digital trade.

4. New Zealand should use DEPA to enact rules that explicitly allow trade partners to stop data flows of illegal content, especially relating to copyright infringement (for digital trade) and violent material (given New Zealand's interest in this issue). New Zealand should enact a clear, detailed, and balanced legal framework that allows rightsholders at home to use website blocking as a tool to block access to offshore websites that facilitate access to large amounts of copyright-infringing material (as seen

already in Australia, Singapore, the United Kingdom, and many of New Zealand's trading partner countries).

5. New Zealand should protect encryption's role in securing data flows and digital trade by enacting rules that prohibit governments from requiring firms to build "back doors" into their encryption or to otherwise modify the design of their systems to facilitate access to law enforcement. By putting such commitments in DEPA, New Zealand would be joining other countries, such as Germany and the Netherlands, in clearly and publicly disavowing such measures.

6. New Zealand should ensure DEPA's new digital trade rules protect the Internet-based services that are key agents of digital trade as they provide the communication, media, and other services that are increasingly popular with consumers around the world. A growing number of countries are using behind-the-border regulations (in the form of legacy regulatory frameworks) to discriminate against these foreign providers as traditional telecommunication and cable service providers struggle to compete. New Zealand's goal should be to create a regulatory framework that is transparent and evidence-based to ensure that policymakers looking to "level the playing field" (often a euphemism for protectionist policy) between industries and firms are focused more on equivalent protection, not equivalent regulation.

7. New Zealand should use DEPA negotiations to protect the intellectual property tied up in the source code behind algorithms whereby countries use "algorithmic transparency" requirements as a mercantilist measure to unfairly acquire the source code.

8. New Zealand should pursue the principles and policies for an ambitious open data framework in each country. Such an initiative creates value for everyone, as it increases both the quantity and quality of data that firms can use to provide new, data-driven goods and services. New Zealand should push for a specific section on open data, which should recognize that opening up public information for re-use has considerable and widespread benefits to government, industry, and the public. Such a section should reference international agreements and partnerships that signal a country is committed to enacting policy best practices, such as the G8 Open Data Charter and the Open Government Declaration.

9. New Zealand should use DEPA to setup a framework for members to allow electronic labeling for the ICT products that drive the digital economy. DEPA should include a mechanism for domestic agencies to cooperate and exchange information about their electronic labeling requirements, with the goal of facilitating compatibility and prohibiting country-specific technical standards (which act as a barrier to trade).

10. New Zealand should work with Singapore and Chile in DEPA to share information and best practices on "open data" frameworks, such as in the banking sector. This could include hortatory language in a digital trade chapter about the role that open application programming interfaces (APIs) can play in facilitating access to data in certain sectors and about how such access promotes innovation, competition, and trade. The parties should also work together on enacting compatible API standards. These mechanisms are a key tool to help facilitate access to data in certain public and private sectors that hold valuable and sensitive data but lack the ability to securely and efficiently

share it with one another. However, as this is an emerging issue, there's the potential for countries to enact country-specific technical standards that prevent foreign firms from easily accessing domestic data.

11. New Zealand should use DEPA negotiations to ensure countries have interoperable legal frameworks for electronic signatures and invoices that do not include country-specific technical standards (such as for encryption) that can act as a barrier to digital trade. New Zealand should ensure that electronic signatures and invoicing issues are explicitly mentioned as topics for regulatory cooperation between trading partners to ensure there is a mechanism for respective agencies to work together. Ultimately, New Zealand and its DEPA partners should aim to mutually recognize each other's digital certificates and electronic signatures.

DEPA SHOULD LEAD TO STRONGER RULES TO PROTECT CROSS BORDER DATA FLOWS

New Zealand's digital trade policy should be built on the central feature of the global digital economy—the free flow of data. Data will naturally flow across borders unless governments enact artificial barriers that prevent it from doing so. Businesses use data to create value and many can only maximize that value when data can flow freely across borders. Rules and frameworks that protect the free flow of data—all types, such as health, tax, financial, and other personal data—are critical to this as there is uncertainty about whether current WTO trade rules apply to data. Countries have exploited this uncertainty to enact barriers to data flows as part of efforts to protect and support local companies at the expense of foreign firms and their goods and services. The CPTPP's e-commerce chapter took many steps in the right direction to protect cross-border data flows, but more needs to be done to strengthen these protections. In many cases, the ideas outlined below do not address specific barriers to digital trade in Singapore or Chile, but reference policies considered or enacted in other countries that would help push back against growing global digital protectionism in setting a new global norm if more countries sign onto DEPA.

While seemingly semantic, a key difference between the CPTPP and the United States-Mexico-Canada (USMCA) free trade agreements is that the latter strengthens provisions that prohibit barriers to data flows by limiting the potential for countries to misuse general exceptions to enact forced data localization (a policy that ITIF shows does not, in most instances, increase commercial privacy or data security).[9] For example, the USMCA's provision on computing facilities is the same as the CPTPP's in that it is simple and definitive, stating that "No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory."[10] However, the USMCA provision does not include sub-sections about exceptions to this provision, namely that a country would be able to enact barriers to data flows if it was needed to achieve a "legitimate public policy" objective, which could include privacy and public interest and morals issues.

This is a looming challenge for global digital trade as some countries consider data localization a legitimate public policy tool (without explaining why it is necessary and why alternative policies are not used) and therefore look to use these types of overly broad exceptions to enact the very policies they are designed to prohibit. For instance, Vietnam directly references similarly broad exceptions for national security and the public interest in WTO agreements in justifying data localization requirements under the nation's new

cybersecurity policy.[11] In a similar way, the EU is advocating an approach to data flows and privacy that creates a similar self-judging loophole by including digital trade provisions that allow a party to enact whatever measures it "deems appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data."[12] Essentially, as long as a country states that data localization is for data privacy, the policy is valid within the EU trade policy framework, thus legitimizing the very policies the EU vision apparently opposes.[13] The scenario whereby countries defend data localization on their broad, self-judging (and spurious) definitions of privacy and cybersecurity (never mind the vague term of the public interest) would render useless any rules that supposedly protect data flows.

Similar to USMCA, New Zealand should therefore push to narrow the potential misuse of exceptions by explicitly stating that data localization is not a legitimate policy for achieving privacy or cybersecurity.

NEW ZEALAND SHOULD USE DEPA TO CREATE A FRAMEWORK BASED ON "GLOBAL PROTECTIONS THROUGH LOCAL ACCOUNTABILITY"

Accountability and interoperability should lie at the heart of New Zealand's approach to managing data flows and data-related responsibilities in DEPA, especially as it relates to privacy provisions, regulatory concerns over access to data, and data protection. The following section explains why New Zealand should use DEPA negotiations to enact a framework for "global protections through local accountability" involving data flows, data-related legal responsibilities (such as for privacy, data protection, and regulatory access to data), and cooperation with counterparts on shared concerns raised by cross-border data flows (such as joint privacy investigations). In line with this, New Zealand should use DEPA negotiations to announce that it plans to join the APEC Cross-Border Privacy Rules (CBPR), perhaps alongside Chile, which also isn't a member. New Zealand is already a member of APEC's Cross-border Privacy Enforcement Arrangement (Singapore is as well, but Chile is not). It should also explicitly mention APEC CBPR in DEPA provisions as an example of interoperability (similar to USMCA) and push for USMCA-like provisions that focus on regulatory access to data (rather than location) in order to address related concerns over financial oversight.

When policymakers deal with data governance and cross-border data flows, the basic expectation should be that when it comes to handling data, companies doing business in a country should be responsible and held accountable under that nation's laws and regulations, for both their own actions and the actions of their agents and business partners, regardless of whether they're located inside or outside the country where a firm collects or manages data. Therefore, the focus for policymakers in making data-related laws and regulations is ensuring they hold firms accountable regardless of where the firms store, process, or transfer data. This accountability principle is based on two key points: A firm with "legal nexus" in a country's jurisdiction has to abide by its data-related laws (even if the company transfers data abroad), and each country's domestic data governance needs to be global in scope and interoperable in practice given the globally distributed nature of the Internet.

First, policymakers should focus on ensuring that their legal frameworks and trade agreements make clear that firms with a legal nexus in their jurisdiction are responsible for managing data in a certain way, wherever the data is transferred and stored. This expectation could be made clear in law by declaring that companies doing

business in a country are legally responsible for any failures to manage data (such as personal data) from that country, regardless of whether those failures are the fault of a domestic or foreign firm or an affiliate or business partner in that country or abroad. In other words, a country's data-protection rules would travel with the data. Companies doing business in a given country would have a strong incentive to assist their business partners outside that country in adhering to its privacy protections, because citizens and the government could seek remedies from that company for any privacy violations, such as a data breach, irrespective of whether that company or its partners were at fault.

Focusing on this key legal nexus concept would cover the behavior of many firms that attract regulatory scrutiny. Just as a global bank or manufacturer with branches or plants in a given nation is subject to that nation's privacy and security laws and regulations, foreign technology (or any other) firms cannot escape from complying with a nation's laws by transferring data overseas. But what about companies without legal nexus in a particular country (i.e., the firm has no physical presence, business activity, or marketing directed toward a specific foreign country)? For example, the citizens of nation A might visit the website of a small company located in nation B, which has different privacy and security laws. This company did not have a legal nexus in country A, so it cannot be expected to abide by the laws there. In this case, the only way nation A's laws can be enforced—whether or not they require data localization—is if they simply cut off their citizens' access to all foreign websites. This is not the case for most businesses involved in foreign digital activity, as they have legal nexus, but it highlights the fallacy of countries trying to enact policies that affect the entire Internet and cannot be contained within borders.

This accountability-based approach is shared by most nations, after all, including for data privacy. Both New Zealand's Privacy Act and its Health Information Privacy Code protect personal information and health information even when it is transferred outside of New Zealand.[14] Likewise in the United States. Even though it does not have an "adequacy" standard such as in the EU, most companies in the United States must disclose certain data-privacy practices and adhere to those requirements. Even when processing data outside the country, companies remain responsible for the data. U.S. companies mitigate these risks by stipulating requirements in relevant data-handling and processing contracts they implement with other companies. For example, foreign companies operating in the United States must comply with the privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA), which regulates U.S. citizens' privacy rights for health data—even if they move data outside the United States. And, if a foreign company's affiliates overseas violate HIPAA, then U.S. regulators can bring legal action against the foreign company's operations in the United States. Such an approach demonstrates how firms already comply with data-related laws and regulations, as well as being a key part of existing data-transfer mechanisms used by countries and firms alike (such as model contracts, binding corporate rules, the EU-US Privacy Shield, and the APEC CBPR.[15]

New Zealand needs to use DEPA negotiations to build out an accountability-based framework rather than one in which countries force firms to exclusively store data locally (a concept known as "data localization") in the mistaken belief that this is the only way to enforce data-handling requirements on foreign organizations. While any country can demand extraterritorial application of its laws, it may not always be able to enforce them (as this can be quite complex). Multiple criteria are used by courts to determine when a country has the authority to impose its laws on actors outside of its borders.[16]

However, as long as a firm has a legal nexus within a country's jurisdiction, it must abide by the laws of that country, regardless of where it stores data. Just as international financial firms operating in a foreign country fall under the purview of that country's local regulatory agencies, regardless of where they transfer money to, so too do firms that collect and use data as part of their business within that region. For example, many businesses have foreign workers (e.g., sales teams) or foreign assets (e.g., real estate, products, or bank accounts) that give foreign countries viable mechanisms for enforcement of failures to abide by civil or criminal laws. Policymakers have leverage over firms doing business virtually because they can block access to domestic markets through tactics like prohibition of local advertising.

Second, this accountability principle is based on the fact that modern technology, especially the Internet and cloud data storage, means that each country's domestic regulatory regime for data (such as for privacy) needs to be globally interoperable given that each country faces the same challenge in applying its laws to firms that may transfer data between jurisdictions. Interoperable privacy frameworks are the international extension of this accountability-based approach such that data is still able to flow between different privacy regimes, and countries'' data protection rules flow with it. The goal for interoperability also reflects the fact that there will be no one globally harmonized privacy regime. It is no surprise that interoperability—not harmonization or even adequacy—is a key objective of several of the leading data-protection initiatives, such as those from the Organization for Economic Cooperation and Development (OECD) and APEC.

No doubt, domestic regulators need support and resources to fully operationalize such a framework in order to give them greater confidence in their ability to enforce local laws in the Internet era. In part, this can be done through additional international mechanisms that support the development and application of shared principles and cooperation between regulatory authorities. For example, there is obviously room for improvement in facilitating greater cooperation between different countries' privacy regulators. For example, New Zealand could use its membership in the Global Privacy Enforcement Network to better work with other members on shared privacy issues.[17] Another example is its membership of the APEC Cross-border Privacy Enforcement Arrangement (CPEA), which creates a regional framework for information sharing and cooperation on enforcement among privacy regulators.[18] At the level below this, New Zealand's privacy regulators should set up bilateral arrangements (e.g., memorandums of understanding) with counterparts. Countries can then use these bilateral mechanisms to both share information and best practices and to cooperate on joint investigations (as the U.S. Federal Trade Commission has done with over a dozen countries).[19]

The 2015 data breach at Ashley Madison (an adult dating website) provides a valuable example for how New Zealand's privacy regulators can operationalize these interoperability mechanisms. Ashley Madison is headquartered in Canada, but its websites have a global reach, with users in 50 countries, including Australia. Although the firm that owns Ashley Madison does not have a physical presence in Australia, it conducts marketing in Australia, targets its services to Australian residents, and collects information from citizens in Australia. It therefore falls under Australian law. Canada's privacy regulator (the Office of the Privacy Commissioner of Canada) initiated a joint investigation with its Australian counterpart (the Office of the Australian Information Commissioner) based on each nation's respective participation in the APEC CPEA—

which allowed for cooperation and the exchange of information on certain aspects of the investigation, despite each side conducting their own investigation according to their respective data privacy laws. The final analysis was that Ashley Madison held significant amounts of personal data (much of it sensitive) and should have had security measures in place, such as an explicit risk-management process to identify information security risks. Ashley Madison agreed to a compliance and enforcement undertaking with both the Australian and Canadian privacy regulators to implement the regulators' recommendations.[20]

Beyond interoperability, the two alternative approaches to data governance—data localization and the EU's General Data Protection Regulation (GDPR)—are problematic in their own ways. The EU's GDPR regime is problematic because it pushes for harmonization and tries to make foreign countries responsible for enforcing European data privacy standards instead of using domestic regulations to hold companies responsible for breaches of European data privacy laws. GDPR imposes a general prohibition on transfers of EU personal data to only a small group of foreign countries it has determined (as part of an opaque and ad hoc process) provide an "adequate" level of protection equal to data protection at home. A critical flaw in the EU's approach is the mistaken logic that this country-by-country assessment approach is effective in promoting better data privacy and protection by companies that manage personal data.[21]

Furthermore, the EU's top-down approach is ultimately untenable, as differences in social, cultural, and political values, norms, and institutions are behind countries not regulating privacy the same way. For example, given the country's approach to data protection and privacy, it is inconceivable China would ever be deemed "adequate" from a European perspective. Yet, the fact that Europe has not applied to China the same standards it applies to the United States with regard to EU personal data highlights the arbitrary nature of its approach.[22] Ultimately, an interoperable framework for global protections through local accountability represents a more realistic and tenable approach to global data privacy—as, so far, outside of European and British territories, only six countries have received a national adequacy finding from the EU: Argentina, Uruguay, Israel, Japan, Switzerland, and New Zealand.

Meanwhile, data localization is becoming more common as a growing number of countries are forcing firms to store data locally in the mistaken belief that data is more private and secure when it is stored within a country's borders (which is not true) and that it needs to be stored locally to ensure regulatory oversight for data-related issues (also not true, as detailed in see the subsequent section).[23] As to the former, controlling where organizations store data does not impact how they collect and use it (privacy)—or how they store and transmit it (security). Policies that lead to local data storage can actually undermine personal data protection, as without an independent judiciary and set of legal protections, governments can bring more pressure and tools to bear in forcing local providers to disclose data (for both social and political purposes). Even if a data privacy framework only requires a copy of data to be stored locally, rather than prohibiting transfers of all data, it nevertheless lays the groundwork for such an outcome. Furthermore, wherever data privacy intersects with cybersecurity, forced local data storage can make personal data more susceptible to inadvertent disclosures (i.e., data breaches) if the local data center is not committed to enacting best-in-class cybersecurity measures. Such inadvertent disclosures are the result of security failures. When it comes to data storage and protection, it is important the company involved (which either runs its own networks or uses a third-party

cloud provider) be dedicated to implementing the most advanced methods to prevent such disclosures. The location of these systems has no bearing on the security of data.

New Zealand should use DEPA to announce that it plans to join APEC's CBPR, given it is a clear example of an interoperable data governance systems that focuses on "global protections through local accountability." In this way, it would be similar to USMCA (Article 19.3.6), which explicitly recognizes APEC's CBPR as one of these valid mechanisms to facilitate cross-border information transfers while protecting personal information. Given Chile also isn't a member (but Singapore is), New Zealand could do this concurrently with Chile. In the text of a digital trade chapter, New Zealand and its trade partners could make clear the relevant point that a country can enforce its rules on any foreign or domestic organization with legal nexus. Moreover, a country can enforce its rules on these organizations based on how they handle the data they collect, even if that data handling occurs abroad or with a third party. Given that rigorous local enforcement is needed to protect data globally, New Zealand could indicate in DEPA that it wishes to expand its enforcement capabilities by entering into cooperative agreements that allow foreign regulators to investigate jointly, share findings, and impose penalties on violators, thereby strengthening the hands of regulators globally.

New Zealand, Singapore, and Chile should enact a data-governance framework based on local accountability and interoperability in order to provide a clearer, and better, alternative to the two other main, contrasting approaches: efforts by countries (mainly European) to make other countries adopt their (universalist) approach to data privacy in order to make them responsible for enforcement (instead of holding firms responsible) and countries forcing firms to only store data locally.

Tax, Financial, and Securities Regulators Should Focus on Firms Providing Access to Data (Not Where Data is Stored)

New Zealand should use DEPA negotiations to enact rules that make clear that it and its trading partners will not create barriers to the transfer of financial, tax, accounting, and payments data, and data associated with publicly listed companies. Furthermore, New Zealand should advocate for provisions that clarify that what matters is not the location of data storage, but that relevant regulatory authorities have timely access to data (upon request). Companies that fail to provide data for legitimate regulatory purposes should face legal and financial penalties. As a clear signal of its commitment to the free flow of data and interoperable data governance frameworks, New Zealand should revise its own approach, given that the Inland Revenue Service issued a "Revenue Alert" that outlines that companies are required to store business records in data centers located in New Zealand in order to comply with the Inland Revenue Acts.[24]

New Zealand, Chile, and Singapore should pursue a clear and detailed framework that highlights that what matters is that companies are able to provide access to data upon request, regardless of where it is stored, as a growing number of countries, including China, India, Indonesia, Russia, and Turkey, are misusing regulatory concerns to enact data localization requirements as part of financial oversight frameworks.[25] At one stage, even the United States pursued trade policy provisions that created the potential for localization, but it has since revised its approach.[26] While many countries (such as India and Russia) use regulatory concerns as cover for protectionist intentions, there are other cases where underlying regulatory concerns over access to data are legitimate, albeit mistaken, and used to justify data localization policies.

Similar to USMCA, New Zealand should use DEPA negotiations to set out a legal framework for financial data, as it is among the most commonly targeted data categories (besides personal data). Policymakers are enacting data localization requirements in the mistaken belief that they are the best and only way for data to remain accessible to government agencies for regulatory oversight. Policymakers are wrong to believe firms can avoid oversight (and requests for data) by simply transferring data out of a given country. This is especially true for financial firms and firms listed on a local stock exchange, as they already have a clear legal nexus in a jurisdiction and have likely had to seek regulatory approval from local financial authorities to operate in a given jurisdiction. Indicative of many issues involving data, there are likely to be cases wherein jurisdictions come into conflict over access to data due to local laws and regulations (such as privacy). But similar concerns over other financial oversight issues have not prevented a more integrated global financial system. Nor should they, in the case of data governance. In contrast they have led to the International Monetary Fund, the Financial Stability Board, and others working together on such shared concerns, including on data, as they recognize the mutual benefits of cooperation.

New Zealand should apply an accountability-based approach in ensuring that firms provide timely access to data in response to requests for data from tax and financial regulatory authorities (in the case of financial and payment services firms) and stock exchange administrators (for publicly listed companies). Modern cloud computing, which allows transfers of data with the mere click of a button, enables firms to provide timely access as part of regulatory oversight, while still allowing them to move financial data freely in order to provide secure, innovative, global services. Given the clear legal nexus of these firms, regulators should be confident they can ensure firms comply with data requests, regardless of where those firms store data. The focus for a nation's data governance frameworks should be on regulatory access to firms' data being timely, direct, and complete, regardless of where this data is stored. Obviously, if firms are unable to provide authorities with timely access to data, they should face legal penalties. But again, the focus should be on holding firms accountable regardless of where they store data. In this way, just as consumer safety and other laws apply to tangible goods that flow in and out of a country as part of international trade, regulatory, cybersecurity, and other rules should apply to both data and the financial firms that move and store data in other nations.

The respective approaches of the United States and the European Commission (EC) provide examples regarding regulatory oversight and access to data. As part of efforts to build a Digital Single Market, the EC is working to remove barriers to the transfer of company, tax, bookkeeping, and financial data, and asking that member states focus on mandating access.[27] For example, in 2015, Denmark changed its local data storage requirement for accounting data such that companies could store their data anywhere, as long as Danish authorities were given easy access to it on request.[28] This is where the focus should be: putting in place the legal framework to ensure companies can provide data to regulatory authorities in a timely manner.

Reforms to the U.S.'s domestic data governance regime also serve as a reference point for New Zealand's domestic arrangements (given its own rules about local data storage for tax data) and in regard to its plans for DEPA negotiations. During the global financial crisis, U.S. regulators faced issues gaining access to data in key banks' (such as Lehman Brothers') IT systems.[29] This made it difficult during bankruptcy proceedings for

the regulators to access the data needed to unwind positions and ascertain what money was owed to whom.[30] However, subsequent legal reforms in the United States (e.g., the Dodd-Frank Act, enacted in 2010) have addressed these concerns by focusing on how companies disclose to regulators the way they manage their IT and data as part of regular prudential compliance activities. In the event of a crisis, regulators know companies will be able to provide the data they want.[31] These new mechanisms ensure that regulators know how U.S. firms manage and secure their IT systems and how they store, access, and manage data on an ongoing basis (as part of periodic compliance activities).[32]

U.S. trade policy compliments this domestic data governance framework with detailed, access-focused provisions that make data localization truly a last resort. Initially, the United States created a loophole in the Trans-Pacific Partnership trade agreement for data localization by excluding financial data from the agreement's prohibitions on data transfer restrictions and not specifying (in detail) the exact interests and emergency scenarios in which this would be acceptable.[33] Recognizing this risk, the United States revised its approach in the USMCA to show how legitimate issues raised by cross-border data flows can be addressed while allowing the free flow of data as the default and predominant policy approach. It is important to note that the USMCA still treats financial services data differently (which, in an ideal world, it would not), as neither the provisions that prohibit data localization nor data flow provisions apply to financial services. USMCA parties agreed to recognize "that immediate, direct, complete, and ongoing access by a Party's financial regulatory authorities to information of covered persons, including information underlying the transactions and operations of such persons, is critical to financial regulation and supervision, and recognize the need to eliminate any potential limitations on that access."[34]

A key lesson from USMCA that New Zealand should consider emulating is that each member agreed to provide firms with a reasonable opportunity to make changes to their IT systems (i.e., shift data storage from one jurisdiction to another) if they find they are unable to provide regulators with immediate and ongoing access to data. Highlighting (again) the central focus on access to data, the USMCA details that whenever a financial regulator requires a firm to change where it stores data, that new location does not necessarily have to be to the firm's computing facilities in its home country, and may instead be a third-country jurisdiction in which both the firm and its domestic regulators are confident they would have access. In designing these and other provisions, the United States Trade Representative's Office designed narrow and detailed language that facilitates government access to data for regulatory purposes, while ensuring countries remain committed to avoiding policies that require data localization or other barriers to data flows.[35]

PARALLEL EFFORT TO DEPA: NEW ZEALAND SHOULD SEEK NEW OR UPDATED MECHANISMS TO MANAGE CROSS-BORDER ACCESS TO DATA FOR LAW ENFORCEMENT PURPOSES

Many countries enact barriers to cross-border data flows due to law enforcement concerns over access to data needed for investigatory purposes. While not strictly within the context of trade agreements, New Zealand should use the DEPA process to draw respective legal and law enforcement authorities together to put in place new or updated mechanisms to better manage cross-border access to data for law enforcement purposes. This cooperation and engagement could then be referenced in a general provision in a cooperation section of a digital trade chapter to highlight the fact that the parties are addressing (in a positive way) the legitimate concerns law enforcement agencies might have while still allowing data to flow freely as part of digital trade.

An updated/new framework to access data, law enforcement authorities could be certain that they can access data stored in other jurisdictions in a timely manner should the legitimate need arise. This would assuage authorities' concerns and enable the free flow of data. The problem is existing legal processes and treaties (such as mutual legal assistance treaties) are woefully out of date, needlessly complex, and often delayed due to poorly resourced local agencies. In New Zealand, mutual legal assistance is largely governed by the Mutual Assistance in Criminal Matters Act of 1992, which allows for requests to be made to New Zealand by an already-authorized list of other countries (such as Australia, the United Kingdom, and the United States), while laying out criteria for any other country to make a request.[36]

The broad problem is that countries have mismatched legal assistance treaties, conflicting laws, and differing norms. Indeed, there is currently no comprehensive framework for how to successfully navigate cross-border jurisdictional disputes, especially those involving the digital economy. As the threat of cybercrime rises, there is an increasing need for clarity on these questions, particularly regarding government access to data outside of its borders. The challenge facing New Zealand and other likeminded countries that value international cooperation and the broader benefits of data flows is working together to establish new and improved international legal standards and mechanisms for facilitating legitimate law enforcement requests for cross-border access to data.[37] The alternative some countries are pursuing under the guise of law enforcement interests—data localization—threatens to undermine the global digital economy, especially if such an approach becomes the norm, as it would raise the specter of many—or perhaps even all—countries being stymied in their pursuit of cross-border criminal investigations (as each country would horde data locally). It would be better for countries to recognize the mutual benefit in implementing new and better mechanisms to help each other, given the increasing frequency in which local authorities encounter investigations that involve data held in another jurisdiction.

The United States' experience with its relatively new legislation—the Clarifying Lawful Overseas Use of Data Act (CLOUD) Act—provides an example of the types of law enforcement cases that can arise in today's global digital economy, and how policymakers should respond in creating new mechanisms to facilitate cross-border law enforcement requests for data. The CLOUD Act stemmed from a case in late 2013 when U.S. federal law enforcement officials obtained a warrant as part of an anti-narcotics investigation to seize the contents of an email account belonging to a Microsoft customer whose data the company stored in Dublin, Ireland.[38] Microsoft refused to comply with the order, arguing that the U.S. government could not force a private party to do what U.S. law enforcement has no authority to do itself: use a warrant to conduct a search-and-seizure operation on foreign soil. This case exposed the cracks in the foundation of the current framework used by law enforcement agencies to access digital information and determine jurisdiction on the Internet.

In response, U.S. policymakers enacted the CLOUD Act to reform the current system and address the problems raised in the Microsoft case, while protecting consumer privacy, enhancing the capabilities of law enforcement, and preserving international comity. The legislation authorizes the U.S. government to form reciprocal data-sharing agreements (called "executive agreements") with other countries, giving them an incentive to remove barriers to sharing data with U.S. law enforcement. It also creates a statutory right for companies to challenge data requests from law enforcement that conflict with other nations' laws.[39]

Importantly, as it relates to digital trade, the CLOUD Act requires the U.S Department of Justice (DOJ) to provide a written certification that a country (with whom it enters an executive agreement) "demonstrates a commitment to promote and protect the global free flow of information and the open, distributed, and interconnected nature of the Internet."[40] Even though the ability to make such a certification is one of many factors DOJ must consider when entering into an agreement with another country, a requirement to localize data suggests DOJ would consider this as a contravention of the CLOUD Act's criteria.

One option for New Zealand would be to improve existing mutual legal assistance treaty (MLAT) processes and tools used to manage cross-border law enforcement requests for data. In this way, countries can implement the individual building blocks that support the longer-term goal of a new multilateral agreement. To encourage more countries to adopt new or updated MLATs with each other, leading countries should also standardize and strengthen these agreements. New Zealand should work with major economic organizations and forums to establish and adopt model MLAT language, or a "MLAT 2.0." This treaty should create a common process so that governments do not necessarily need to negotiate agreements with each individual country, but instead, allows them to use fairly standardized agreements across many nations. The goals of an MLAT 2.0 would be fourfold.

First, MLAT 2.0 should create a common framework for when and how countries may use domestic authorizations to access data outside their borders. This may include arrangements such as reciprocal recognition of domestic search warrants (when countries meet certain legal standards) in order to expedite the process. Similarly, the agreement may include comity analyses or notice requirements as a condition of this reciprocal recognition.

Second, MLAT 2.0 should commit countries to modernizing their methods for responding to foreign data requests, such as through the processes outlined in the previous recommendation.

Third, countries should commit to complying with their counterparts' lawful requests for data in a timely fashion, unless those requests would violate mutually agreed upon provisions, such as for national security reasons.

Fourth, countries should report the number of requests they receive, the number of requests they fulfill, response times, and progress in their modernization efforts. The goal of reporting is to hold participating nations publicly accountable for their timeliness in adopting and modernizing MLAT processes, as well as to identify inefficiencies in the process. Once adopted, New Zealand and others could push their trading partners to agree to MLAT 2.0s alongside trade negotiations (given the trade implications of data localization), thereby encouraging more countries to adopt improved MLATs with one another. New Zealand could lead by example in pushing for such an outcome in tandem with DEPA negotiations with Singapore and Chile. Similar to other countries, New Zealand could use MLAT 2.0 agreements with Chile and Singapore as part of a broader upgrade to the global framework for the exchange of law enforcement data. This would complement U.S. efforts to negotiate CLOUD Act executive agreements with the United Kingdom and others, while the EU is updating its "e-evidence" rules for its member states, while also starting negotiations on a new mechanism to exchange law enforcement data with the United States.[41]

Ideally (given the global nature of the Internet), the goal for New Zealand, Chile, Singapore, the United States, the EU, and others would be for countries to come together to negotiate a new multilateral agreement—a Geneva Convention on the Status of Data—to establish international rules for transparency, settle questions of jurisdiction, engender cooperation for better coordination of international law enforcement requests, and limit unnecessary government access to data on citizens of other countries.[42] This would also help countries follow similar rules and procedures for cross-border law enforcement requests and actions.[43] Finally, it would address the issues of localization and barriers to data flows, with parties agreeing not to enact data localization (as this would undermine the central point of the agreement).

Such a multilateral initiative would be based on national sovereignty, as different nations have different sets of values, priorities, and legal systems. And because Internet companies offer services over global networks, it is often the case that two or more countries have interests in the same data. This initiative should not force a particular nation's policies, such as promoting the strict standard of probable cause to gather evidence (as in the case of the United States) or allowing government access to evidence at the detriment of personal freedoms (as in the case of nations such as China and Russia), on the rest of the world. Therefore, each business should be subject to the laws of each country in which they have a legal presence. This principle would ensure no company can escape complying with a nation's laws by merely transferring data overseas. It is simply a matter of coming up with a framework to create interoperability between different countries' approaches.

As countries sign up to the Geneva Convention on the Status of Data and this network of new MLATs emerges, responsible member countries will be better placed to identify those countries that act to circumvent good faith efforts and international legal processes for providing law enforcement agencies with lawful access to data as "data havens." Under these respective agreements, nations will (ideally) also have the authority to block data flows to, or ban companies from basing servers in, these scofflaw data havens, as they have demonstrated they cannot be trusted to work with their counterparts on shared interests in the global digital economy such as cross-border law enforcement investigations.

DEPA SHOULD ALLOW COUNTRIES TO (RESPONSIBLY) STOP DATA FLOWS OF ILLEGAL CONTENT

New Zealand should use DEPA to enact rules that explicitly allow trade partners to stop data flows of illegal content, especially as it relates to copyright infringement (for digital trade) and violent material (given New Zealand's interest in this issue). In line with this, New Zealand should enact a clear, detailed, and balanced legal framework that allows rightsholders at home to use website blocking as a tool to block access to offshore websites that facilitate access to large amounts of copyright-infringing material (as used in Singapore and many other key trading partners). Some people interpret the concept of free flow of data across borders to mean that all data should be allowed to traverse borders without barriers. But within the concepts of digital free trade and the free flow of data, it is important to recognize that not all data flows should be treated the same, as some data flows are rightly illegal. Thus, there is nothing contradictory about strongly supporting the global free flow of data while also supporting the blockage of the flow of illegal data, any more than it is to strongly support the free trade of goods, while supporting the blocking of trade in endangered species or human trafficking. While this section largely focuses on the use of website blocking for copyright enforcement

purposes, many of the same principles apply to the use of website blocking for preventing access to violent material.

While policymakers can obviously implement domestic laws to manage illegal online activity within their own country, due to the globally distributed nature of the Internet, such activity often remains accessible from foreign providers. From a pragmatic perspective, this is why a growing number of countries (including Australia, Singapore, India, and the United Kingdom) ask their Internet service providers (ISPs) to block access to websites engaged in illegal activities — such as those facilitating cybercrime, child pornography, or terrorism — because it is one of the few means available to authorities responding to illegal services and materials hosted abroad. Blocking websites engaged in intentional and systematic copyright infringement should not be considered any differently. Obviously, it is important that any such framework be transparent and include legal checks and balances to ensure it is used appropriately, but its growing use around the world shows that this is eminently achievable and that website blocking can be an effective part of a country's policy tool box to promote and protect creativity and innovation in the global digital economy.[44]

Many countries use website blocking to apply both new and existing legislation to a range of legitimate public policy goals that involve the Internet.

Examples of the types of websites countries block include:

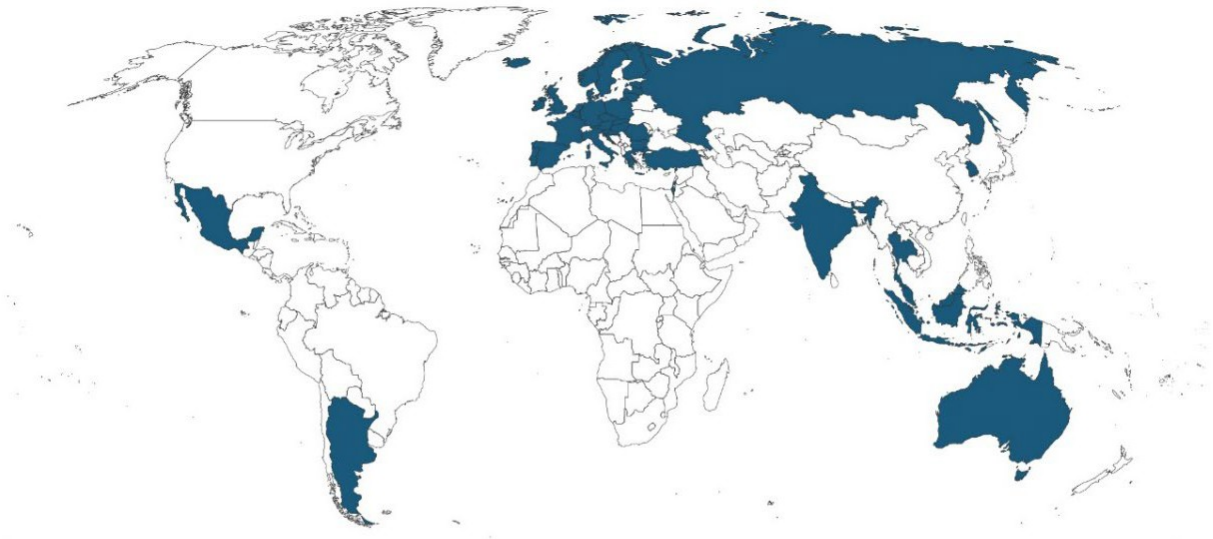
- child pornography (many countries);
- malware (e.g., Australia);[45]
- investment fraud (e.g., Australia);[46]
- online gambling (e.g., Quebec, Canada and Singapore);[47]
- pornography (e.g., India);[48]
- prostitution (e.g., India);[49]
- terrorism (e.g., the United Kingdom, Australia, France, and India);[50] and
- copyright-infringing content (at least 42 nations).[51]

As an example, website blocking is used extensively to block child pornography websites. The 190 members of the International Criminal Police Organization (INTERPOL) voted unanimously to promote the use of all technical tools, including website blocking, to fight child pornography. INTERPOL maintains a list of domains containing websites that disseminate the most severe child abuse material worldwide as part of a "worst of" list.[52] It also provides domains, not URLs, for blocking. As INTERPOL explains, blocking does not by itself remove the offending content, but it does dramatically reduce the amount that is accessible and available to most users. As with many other issues, website blocking is used in conjunction with other measures.

Policymakers in New Zealand should recognize that website blocking is a constructive intellectual property (IP) policy tool for copyright enforcement and to enact changes that allow website blocking. Such formal

recognition would reflect the fact that website blocking for copyright infringement has finally been normalized as an anti-piracy tool around the world. For online copyright infringement, there are at least 42 countries that have either adopted and implemented, or are legally obligated to adopt, measures ensuring ISPs block access to copyright-infringing websites, as demonstrated in Figure 1.[53] The first website blocked for copyright infringement was AllofMP3 in Denmark in 2006. In the decade thereafter, fewer than 1,000 websites were blocked. However, over the past three years, countries have blocked more than 3,000 new piracy websites.[54] The actual figure is likely much higher, as some countries, such as the United Kingdom, do not release specific details on which websites are being blocked so as not to alert website operators. In February 2019, a Motion Picture Association of America presentation outlined that countries block a total of 3,966 websites and 8,150 domain names. Europe is home to the most countries that allow website blocking. Portugal and Italy have each blocked 944 and 855 websites respectively.[55] Furthermore, some countries, such as India, Singapore, and the United Kingdom, now allow "dynamic" blocking orders that extend to proxy websites that piracy operators create after their primary sites are blocked, and are to be enacted during live sporting events.[56] Some of the lessons to take away from the growing use of website blocking is that for it to be effective and workable, it needs to be predictable, transparent, accountable, low-cost, and quick to implement. If countries enact a framework along these lines, it can be a reasonable and useful tool to reduce piracy and encourage consumption of legal content.

Figure 1: Countries that allow website blocking for copyright infringing content[57]



Argentina, Australia, Austria, Belgium, Bulgaria, Croatia, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, India, Indonesia, Ireland, Israel, Italy, Korea, Latvia, Liechtenstein, Lithuania, Luxembourg, Malaysia, Malta, Mexico, Netherlands, Norway, Poland, Portugal, Romania, Russia, Singapore, Slovakia, Slovenia, Spain, Sweden, Thailand, and the United Kingdom.

Website blocking is a logical weapon to use given all the targets and tools countries have in their toolbox to fight digital piracy. Domestically, the first of these is straightforward and already well underway: enacting

policies that support an increase in the number of legal service providers in order to make it easier and cheaper for users to get legal media content online instead of using piracy sites. Alongside this, countries can enact legal remedies to combat certain activities. For example, for domestically hosted content in the United States, copyright holders rely on remedies in the Digital Millennium Copyright Act, which has a "notice and takedown" process for rights holders to get website operators to remove infringing material. Domestic stakeholders, such as brand owners, advertising intermediaries, and rightsholders, can also work together to voluntarily address aspects of the digital piracy ecosystem, such as by ensuring ads from reputable brands are not placed on piracy websites (thus cutting off a source of their income).[58]

Fighting digital piracy gets much harder at the international level. The first option is for law enforcement agencies to specifically target website owners who operate digital piracy sites.[59] However, in most cases, law enforcement cannot get cooperation from their counterparts in other countries to remove infringing material. This problem reveals that many countries are home to digital piracy sites, as they have governments that will not or cannot shut them down, either because there are weak or nonexistent intellectual property protections or for political reasons. Despite the fact that virtually every nation that acts as a haven for pirate sites is a member of WTO and World Intellectual Property Organization (WIPO) and has signed on to multilateral agreements protecting intellectual property—such as the Trade-related Aspects of Intellectual Property Rights (TRIPS) agreement—many nations refuse to effectively address digital piracy in their own jurisdictions (as is the case for Brazil, Pakistan, Russia, and Ukraine).[60] This weakens trust in these agreements. Thus, absent changes to these institutions, or a change in the attitude of governments of scofflaw nations, governments will need to work with Internet intermediaries as the main solution.

Website blocking for piracy, child pornography, or other illegal material is never going to be the silver bullet in stopping the distribution or access to certain illicit material, but it can definitely play a role. While there may be ways for users and piracy site operators to circumvent these methods (such as the use of virtual private networks), it is important to remember that the aim of website blocking is not to eliminate online piracy altogether, but to change consumers' behavior by raising the cost—in terms of time, risk, and willingness to find alternative sites and circumvention tools—of accessing illegal content and making legal sources and their creators more appealing.

For example, an April 2016 Carnegie Mellon University study shows that website blocking in the United Kingdom has been effective in fighting digital piracy. The study used consumer data to analyze the impact of a court order for ISPs to block 53 websites in the United Kingdom in November 2014. It showed that website blocking, when done on a large-enough scale, can shift consumers from accessing copyright-infringing material to consuming legal content online.[61] The study proves an intuitive understanding about online copyright enforcement: If enough piracy sites are blocked, then people will shift to legal sources, especially given the growing number of such services.

Proposals to use website blocking often face a range of ideological opposition, especially that blocking are antithetical to efforts to preserve a "free and open" Internet. While this is a rightly and broadly supported goal, at least in most democratic nations, it does not mean every website should be freely accessible.[62] Just as supporting bans on the importation of ivory or cross-border human trafficking does not make one a

protectionist, supporting website blocking for sites dedicated to piracy does not make one an opponent of a free and open Internet. Clearly, society should want as little as possible to be blocked or taken off the Internet, and that such processes should have appropriate legal checks and balances. But this does not mean policymakers should oppose attempts to block online materials that are clearly illegal.

Critics also assert that website blocking will establish a negative precedent if used by democratic countries and will weaken the moral authority of democratic nations to criticize totalitarian governments for limiting Internet access unrelated to intellectual property. Critics claim these governments would point to democratic nations' use of website blocking to justify their own Internet censorship. But there is no comparison between a country that uses detailed and transparent legal means, supported by an independent legal system, to administer and enforce intellectual property online and a country simply censoring political speech online. Likewise, the U.S. government has not abandoned laws requiring child pornography to be blocked because it thinks doing so would give carte blanche approval to dictatorships that want to block dissenting websites. Online intellectual property enforcement is far from alone in being a public policy that could be misused in order to pursue unrelated or illegitimate objectives. In each case, what matters is the actual intent and the integrity of the process involved in administrating these policies.

DEPA SHOULD PROTECT ENCRYPTION'S ROLE IN SECURING DATA FLOWS AND DIGITAL TRADE

New Zealand has already taken a step in the right direction by agreeing to rules that protect ICT products that use cryptography as part of the CPTPP (Annex 8-B), which prohibits parties from enacting a range of discriminatory and restrictive measures as a condition of market entry or sale of commercially-focused ICT goods.[63] However, New Zealand should build on this by enacting rules that prohibit governments from mandating firms from building mandatory "back doors" into their encryption or providing unspecified technical assistance to law enforcement authorities.

For data to flow "with trust," New Zealand needs to take into consideration encryption, the key technology that people and businesses rely on to ensure the confidentiality of data.[64] Encryption is a process that secures information from unauthorized access or use, mainly by changing information which can be read (plaintext) to make it so it cannot be read (cipher text).[65] Over the last few decades, researchers and firms have steadily gotten significantly better at using encryption to secure the privacy and integrity of data—which has been integrated into goods and services in order to improve security for consumers and businesses. In particular, the development of public-key cryptography, which allows users to communicate securely over an untrusted network such as the Internet, has underpinned most modern ICT products and services. As such, encryption has become a fundamental component of improving cybersecurity, as law enforcement, civil society, security experts, and even the former president of the United States all agree on its benefits.[66] As ITIF argued in "Unlocking Encryption: Information Security and the Rule of Law," the problem is that as the methods citizens and businesses use to secure their information have evolved, some governments, citing law enforcement and national security concerns, have pushed back and proposed or enacted laws that undermine encryption and the beneficial role it plays in today's economy.[67]

Encryption is increasingly important to the global digital economy, as it protects the confidentiality and security of data. Whether consumers realize it or not, encryption is as ubiquitous as the many ICT devices

they use in their daily lives. Even without a user's interaction, devices may use encryption when communicating to other devices to ensure commands received from one device are authenticated before being executed.[68] As such, encryption allows consumers and firms to securely engage in a variety of online activities, such as through access to services (e.g., logons, passwords, e-commerce applications) and privacy of communications (e.g., email, instant messaging, virtual private networks). Businesses use encryption to ensure their research is kept confidential from competitors and hackers, and to ensure transactions with their suppliers and customers are authentic. Essentially, strong encryption helps firms and consumers securely communicate with systems and individuals around the world, thereby facilitating the transactions that allow the global digital economy to grow.[69]

Furthermore, firms use encryption to ensure, and prove, compliance with laws and regulations that require they use "technical measures" to protect data, such as for privacy, financial, data security, and other issues. Such encryption-related provisions focus on firms using technological tools to ensure they protect certain categories of data, while still preserving their ability to transfer, share, and use data. For example: HIPAA uses encryption to protect personal health information; encryption of cardholder data is an acceptable method of rendering data unreadable in order to meet the Payment Card Industry Data Security Standard, which is a set of security controls (an industry-required standard) businesses are required to implement to protect credit card data; and the EU's GDPR emphasizes data governance and accountability when firms manage personal data, requiring them to assess the risk of data loss and data breach and commit them to consider technical "state of the art" measures to mitigate those risks, including encryption.[70]

Proposed and enacted government policies that undermine encryption have taken on a few forms:

- requirements that firms license or register encryption with government agencies,
- requirements that firms only use a government-mandated encryption standard,
- local encryption key storage,
- prohibitions on client-side encryption,
- firms disclosing source code, and
- legal and administrative requirements that firms provide vague, arbitrary, and nontransparent decryption or technical support to government agencies, including installing "back doors" into their products.

New Zealand should look to the USMCA as a model as it expands upon CPTPP (to a degree) in providing clearer details as to the narrow exceptions for the rules by elaborating upon exactly what agencies and processes it does not cover.[71] However, New Zealand should go beyond USMCA to prohibit parties from forcing firms to build backdoors or to otherwise modify the design of their systems to facilitate access to law enforcement as this undermines the strength and role of encryption in today's digital economy. By putting such commitments in a DEPA, New Zealand would be joining other countries, such as Germany and the Netherlands, in clearly and publicly disavowing such measures.[72]

Most recently, Australia, China, and the United Kingdom have enacted laws mandating that tech firms cooperate with governments to install back doors into ICT products and services.[73] Beyond Germany and the Netherlands, the United States considered such laws, but decided against them. Previous government efforts to limit encryption have had various levels of success in restricting wider use of secure technology, such as the much-maligned Clipper Chip proposal in the 1990s.[74] Other attempts have been clandestine, generating distrust among the general public, foreign governments, and industry stakeholders, such as the National Security Agency's surreptitious efforts to introduce backdoors into U.S. products and hide security vulnerabilities it has discovered in commercial systems in order for the government to exploit those weaknesses.[75]

Governments should not restrict or weaken encryption. Any government attempt to undermine encryption reduces the overall security of law-abiding citizens and businesses, makes it more difficult for companies from countries with weakened encryption to compete in global markets, and limits advancements in information security. For example, mandating companies build so-called back doors into their products or to facilitate government access undermines the integrity of firms' encryption products. A weakness or opening provided for one stakeholder inevitably weakens the overall level of protection, as it provides an opening for others, such as hackers. Furthermore, such requirements raise a range of concerns for firms, such as defining technical requirements based only on a particular government's subjective view of what is reasonable and practical, without due regard for how encryption is developed, how it works, or how it is deployed globally.[76]

Moreover, attempts to restrict or weaken encryption would be ineffective at keeping this technology out of the hands of criminals and terrorists, who would be able to access encryption technology on their own.[77] Furthermore, such requirements do not even guarantee success. In the case of data at rest (in electronic storage), even if a law enforcement agency gets a court order to access a person's data stored by a third-party provider (e.g., a cloud storage company), it would not be able to make sense of the data if it is encrypted and that agency does not have the key. If firms that provide services do not have the key to their customers' encrypted data, then they will be unable to comply with requests by intelligence agencies to search through this data. For data in motion (information moving between two or more endpoints), law enforcement may try to gain access through court-ordered wiretaps to monitor specific communications. Again, law enforcement may be able to gain access to messages passed through a messaging service, but if the communications are encrypted end-to-end so only the endpoints (i.e. users) have keys, law enforcement officials will be unable to decipher it.

While many governments have enacted (or considered) such policies for law enforcement and national security reasons, others have used these concerns as a disguise for mercantilism. Encryption products are often at the cutting edge of technological innovation, so some countries view regulatory requirements as a way to help local firms catch up by providing copies or access to source code and related material. Similarly, some countries see regulatory restrictions as a way to discriminate against foreign firms and their products. For example, a requirement for local encryption key storage would result in a firm or its customer having to set up a local server to facilitate the authentication and encryption process.

DEPA SHOULD PROTECT INTERNET-BASED SERVICES/APPS THAT PROVIDE COMMUNICATION, MEDIA, AND OTHER SERVICES

New Zealand should ensure DEPA's new digital trade rules protect key agents of digital trade—those Internet-based platforms that provide communication, media, and other services that are increasingly popular with consumers around the world but are targeted in a growing number of countries using behind-the-border regulations to discriminate against foreign providers. These services are often referred to as "value-added services" within trade agreements.

Technological innovations have changed consumer behavior in media and telecommunications markets. This is especially the case in developing countries that have deployed mobile-phone services before (or instead of) traditional phone services, thereby leapfrogging costly fixed-line infrastructure. It also contributes to the development of a vibrant app and digital economy, as people are using smart phones in new ways. Firms and individuals can use new platforms and digital services as intermediary services and as final consumer goods, such as services for communications (e.g., Skype, Viber). For messaging, "over-the-top" (OTT) service providers (such as WhatsApp, WeChat, Skype, and Facebook) provide instant-messaging services as an alternative to text-messaging services provided by traditional mobile telephone and telecommunication companies. In broadcasting, so-called OTT service providers (such as Netflix, Hulu, and HBO Go) deliver audio, video, and other media over the Internet instead of being packaged with cable TV subscriptions.

Many countries categorize and regulate these services as OTT services because they utilize broadband Internet networks that can manage voice, data, and multimedia traffic to provide services, often (though not always) without the direct involvement of the ISPs, which are often traditional telecommunications and cable TV operators. While there is no universal consensus on how best to differentiate and classify the various kinds of platforms and services—whether as OTTs, but often mixed in with concepts such as the platform economy, sharing economy, peer-to-peer economy, and others—it is clear that their role (whether direct and indirect) as agents of digital trade is important and that rules and regulations that impede their ability to play this role deserve attention.

The problem is that tech firms providing these new, innovative services face a growing range of barriers as countries use legacy regulatory frameworks for traditional telecommunications and broadcasters to enact discriminatory and restrictive regulations. While motivations vary, and often involve legitimate public policy concerns (such as taxation), a common refrain is that restrictions are needed to "level the playing field" with traditional telecommunications and broadcasting companies. In many cases, these measures serve to protect incumbent and traditional telecommunications and broadcasting providers, impede trade in online services, and make it substantially more difficult for U.S. platforms and Internet-based services to access and compete in local markets.

However, just because an OTT service like Netflix or YouTube provides video does not mean it is equivalent to an over-the-air TV broadcaster, or that Skype or other voice-over Internet protocol (VoIP) services are like circuit-switched telephony. The fundamental point to understand about these newer Internet protocol (IP)-based services is that they are more like email than television or telephony. In other words, these new services

simply transport digital bits, just like email, web surfing, and other applications. In some cases, the bits are displayed as text on a screen, in other cases as sound coming out of a computer's speakers, and in still other cases as video on a computer or smartphone screen. As such, they are not the same functionally as services that use dedicated, single-purpose technology to deliver specific services (e.g., telephony). Moreover, the relationship between OTT platforms and traditional telecom firms is not win-lose, but one of interdependence. For telecommunications firms, the declining demand for traditional voice and text messaging services from OTT services is counterbalanced by increasing demand not only for data but for connectivity itself, which is partly driven by OTTs. OTTs need a reliable high-speed network, and telecommunication firms need Internet-based applications to stimulate demand for data traffic.

Countries are enacting discriminatory measures that target foreign OTT service providers as there is considerable uncertainty about whether current international trade rules apply (or not). For example, a basic question is whether OTT services are covered by existing trade services classifications. Are OTT voice and messaging services a form of mobile telephone services or a form of data and message transmission services? The answer is the latter. What about the online distribution of audiovisual content?[78] Is it a form of traditional television distribution or an Internet service? Once again, it is the latter. Along similar lines, do commitments countries took on at the WTO with regard to telecom services cover OTTs?[79] Countries are able to exploit the lack of agreement on technical issues to enact measures that cut off or restrict market access. Thus, New Zealand should use DEPA negotiations to bring clarity and certainty to trade rules involving OTT services in digital trade.

Vietnam and Indonesia are two clear examples of countries using legacy frameworks alongside other new policy concerns, such as how to address the dissemination of false information and to ensure tax arrangements work in today's digital economy, as a cover for digital trade protectionism.[80] For instance, Vietnam enacted new regulations that require OTT firms to locate servers in Vietnam. The regulation also restricts how foreign OTT services operate in Vietnam by forcing them to form a joint venture with Vietnamese telecommunications companies. Meanwhile, it promulgates differentiated regulations for free- and fee-based OTT services, as the latter need to get a license from the government, while the former do not.[81] Media reports also state that Vietnam's prime minister ordered the Ministry of Information and Communications to restrict free OTT apps, such as Viber and Zalo (a local app), due to the impact these apps were having on traditional mobile carriers. As a Zalo representative rightly pointed out, free email services took over from postal services, but no one banned these services, yet the government seems intent on trying to do this with OTT services. Similarly, Indonesia used restrictive policies to force foreign media firms to setup joint ventures with local firms as a condition of market entry. In April 2017, the Indonesian state-owned telecommunication company Telkom signed a strategic partnership with Netflix, after earlier blocking Netflix. Netflix CEO Reed Hastings told CNBC that Telkom is the only ISP in Asia that bans the company's service.[82]

New Zealand should push for new rules in a digital trade chapter that prohibit countries using legacy regulatory frameworks and poor and opaque regulatory processes to discriminate against foreign Internet-based service providers. In many ways, these digital trade provisions would complement the types of provisions that are typically included in 'good regulatory practices' chapters in trade agreements. USMCA provides a useful reference point as it took a step in the right direction by including provisions on value-added services in the

telecommunications chapter that address regulatory process issues for telecommunication services, and potentially, audiovisual and other sectors.

New Zealand should include these provisions within a digital trade chapter of a DEPA given the key role OTT services play in facilitating digital trade. Reflecting this, the opening sentence for this section on value-added services should explicitly recognize the importance of these services to innovation, competition, consumer welfare, and digital trade. The DEPA should include a clear and detailed definition of these value-added services in the digital trade chapter's list of definitions. The CPTPP did not define value-added services, nor include any specific provisions related to them. Within the context of telecommunication services, USMCA defines value-added services as those "telecommunications services employing computer processing applications that: (a) act on the format, content, code, protocol or similar aspects of a customer's transmitted information; (b) provide a customer with additional, different or restructured information; or (c) involve customer interaction with stored information."

Similar to USMCA, New Zealand should seek to create a framework that accounts for the key services targeted, while also acknowledging the fact that countries have different regulatory frameworks for these. For example, whether a country has one or multiple regulators for telecommunication, broadcasting, and related services will determine the nature of the framework it needs. New Zealand should aim to replicate the central point of USMCA's value-added services provisions (article 18.14), which specify that countries should not have their telecommunication regulators use legacy regulatory frameworks or new restrictions to unduly and unnecessarily burden new (largely Internet-based) value-added communication services in order to "level the playing field" (often code for protectionism) with traditional telecommunication providers (and potentially those in other service areas for which the regulator is responsible).

New Zealand should look to build upon USMCA provisions to improve transparency and the need for clear evidence in relevant rulemaking so as to prevent countries from being able to use vague regulatory processes and criteria to enact protectionist measures. New Zealand should advocate for explicit language that would require countries to justify any regulations by considering whether they truly contribute to achieving a legitimate public policy objective. It should also require countries to consider the technical and economic feasibility of any proposed requirements (as some measures that may be possible with traditional providers may not work for Internet-based providers). The section for these two key provisions could detail further steps that ensure relevant regulations reflect good regulatory practices and detail some form of cost-benefit analysis, such as requiring countries to publish a regulatory impact statement that outlines the need for the measure, evidence that the proposed policy is technically feasible, and proof that the proposed policy actually addresses the underlying public policy issue and is not unnecessarily trade-restrictive. In addition to this, New Zealand should replicate USMCA provisions that require that any licensing, permit, registration, or notification procedures that relate to value-added services are transparent and non-discriminatory. Similarly, it should enact USMCA (article 18.14(b))-like provisions that prohibit methods by which countries can use non-tariff measures to unfairly discriminate against foreign firms, such as by stipulating service coverage, mandating or justifying cost structures, or forcing firms to use particular telecommunication networks or technical standards.

New Zealand's goal should be to create a framework that ensures that policymakers looking to "level the playing field" between industries and firms are focused more on equivalent protection, not equivalent regulation. In other words, the goal should not be to subject new digitally-based business models to the same regulations as incumbents, which often limits innovation and digital trade. Instead, the aim should be to ensure that regulation of new business models provides the same overall level of protection, even if the regulatory requirements themselves differ. The USMCA provisions are indicative of the many possible non-tariff tools that countries can use to discriminate against foreign tech firms given they provide a similar, but different, service to incumbent traditional telecommunication/broadcasting firms, many of which are struggling to compete with new providers. In using similar rules, New Zealand would be promoting transparency and the use of evidence-based policy making among its trading partners so that they cannot use behind-the-border rules to close off this promising area of digital trade. While Canada and Mexico do not have OTT regulations that would be affected by USMCA, the rules (if enacted) will have a major impact if repeated in future U.S. trade agreements. The same scenario exists for New Zealand: Singapore and Chile do not have any offending regulations (that ITIF is aware of), but it remains important for the three parties to send a signal that they recognize that these types of digital trade barriers exist and that these rules are not acceptable within their framework for an ambitious, open, and rules-based global digital trading system.

SOURCE CODE AND ALGORITHM PROTECTION: USE DEPA TO FILL THE GAP

Today's economy is a data economy as organizations use data and analytics to drive productivity and innovation. But this is transitioning into an algorithmic economy, in which many more organizations invest in artificial intelligence (AI) to automate processes, develop new products and services, improve quality, and increase efficiency.[83] Using data, AI has the potential to impact virtually every sector of the economy, given its ability to make and test assumptions (sometimes without human intervention) and learn autonomously. AI's impact on economic productivity holds the potential to be much broader, as various aspects of it can be understood as being "general purpose technologies" (such as microprocessors) that have historically been influential drivers of long-term technological progress as they affect most functions in an economy.[84] New Zealand needs to ensure that its digital trade policy explicitly protects the source code at the heart of AI, which is susceptible to theft. AI is going to be increasingly central to competitiveness in the global digital economy, thereby making it an increasingly attractive target for countries which don't want to develop or pay for it as part of a fair exchange, but instead seek to steal it.

New Zealand has already agreed to (much needed) new rules to protect source code in the CPTPP. However, there is one critical, clear omission in the source code provision (article 14.17), as it does not explicitly cover algorithms (as the similar provision does in USMCA).[85] The source code—the lines of computer code at the heart of software—associated with AI is susceptible to theft and replication, and therefore relies on intellectual property protections. A firm from New Zealand might invest many millions of dollars as part of the high-fixed costs for research and development to bring the first copy to market, but given low marginal costs required to produce subsequent copies, if the source code they develop is subsequently stolen, they risk losing the basis of their competitive position going forward. Therefore, this is an important gap to address as it reduces the risk of parties imposing mandates for algorithmic transparency on AI systems developed in other countries, which raises considerable intellectual property risks.[86] It's easy to imagine how some countries could misuse algorithmic transparency requirements to force foreign firms to reveal intellectual property that would aid

domestic firms. While this USMCA provision would still allow parties to enact algorithmic transparency mandates for all firms, both foreign and domestic, this provision prohibits them from using algorithmic transparency as a protectionist measure.

DEPA SHOULD ENACT A FRAMEWORK FOR OPEN DATA AND DIGITAL TRADE

"Open data" refers to data that is made freely available without restrictions.[87] Many governments have begun to embrace open data as a way to encourage transparency and accountability, increase public participation, and promote economic growth. By allowing open data, government agencies can foster data-driven innovation not only within government, but also among private-sector organizations, civil society, academia, and individuals who can make use of these data sets. The impact of releasing open data can be substantial. A 2013 McKinsey Global Institute report estimated that open data could add over $3 trillion annually in total value to the global economy.[88] The benefits of releasing open data can be grouped into three main categories: economic growth; improving government services; and reducing fraud, waste, and abuse in government programs.[89] It therefore represents another potential area of opportunity for digital trade if a firm is able to freely access and use comparable data from another country in providing digital goods and services.

However, there's the potential for governments to undermine the "openness" of open data regimes by enacting measures (either directly or indirectly) that restrict foreign firms access and use of the many data categories that could fall within "public" data frameworks, such as education, tax, mapping, financial, and health data. While these policies don't exist in Chile or Singapore, the examples below highlight the potential for countries to use economy-wide or sectoral data governance policies that result in an open data framework that is ultimately discriminatory on a trade basis. For example, mapping data is a broad category of data that governments often play a key role in regulating. Yet, as it becomes a key input to emerging technologies (like autonomous vehicles) and digital services (like mapping services), countries like China and South Korea have enacted restrictive and discriminatory regime for the collection, preservation, ownership, usage, and export of geospatial data, citing broad and vague concerns over national security, state secrets, and privacy.[90] Another example involves countries (such as China and Indonesia) enacting overly broad, restrictive, and discriminatory data classification regimes (which divide data into distinct categories based on sensitivity levels) that would undermine foreign access and use of many types of public data. For example, China is enacting a data governance regime that restricts the handling and storage of many public data categories by broadly defining its high-sensitive category "important data" as "data that, if divulged, may directly affect national security, economic security, social stability, or public health and safety, such as undisclosed government information or large-scale data on the population, genetic health, geography, mineral resources, etc."[91] Ultimately, these types of restrictions would give local firms preferential access to public data, which can be useful for training AI (by improving their predictive capabilities). If domestic firms are given privileged access to that data, it could (in effect) create an indirect subsidy to the domestic AI industry.[92] Such discriminatory requirements would cut off New Zealand firms from the public data that they could otherwise use to provide valuable digital goods and services into that market.

New Zealand has had an open data framework in place for several years.[93] New Zealand ranks 29th of 178 countries in the Open Data Inventory (ODIN)'s global index (of open data regimes for national statistical offices).[94] New Zealand clearly recognizes that opening up public information for re-use has considerable and widespread benefits to government, industry, and the public. Digital trade provisions can act as an extension of these domestic policy frameworks by ensuring that data-driven New Zealand firms know they are able to access and use public data from other countries (as other firms should be able to do likewise with public data from New Zealand) as part of their efforts to provide data-driven goods and services to respective governments and consumers and the private sector. For example, the Open Data Impact Map shows that there are at least 41 firms from New Zealand using open government data, with these firms coming from finance, real estate, mapping, infrastructure, engineering, and other sectors.[95] Digital trade provisions on open data would ensure these and other firms would have the opportunity to use their existing business models to provide the same or similar digital goods and services in other markets after accessing public data from that country.

While both Singapore (ODIN rank 1st) and Chile (ODIN rank 121st) both also have open data frameworks in place and do not discriminate against who uses such data, New Zealand should use provisions in DEPA to provide certainty that its firms will have access to open government data and to send a broader signal to other trading partners that it considers free and fair access to each other's public data to be part of its broader vision for an open, innovative, and rules-based global digital economy.[96] Here, New Zealand should build upon USMCA, which was the first trade agreement in the world to promote the publication of open government data. Article 19.18 of the agreement officially recognizes that "facilitating public access to and use of government information fosters economic and social development, competitiveness, and innovation." While USMCA does not require parties to publish open government data, to the extent they choose to publish this data, it directs them to adhere to best practices for open data, including ensuring it can be in open, machine-readable formats. Additionally, the deal directs parties to try to cooperate and identify ways they can expand access to and use of government data, particularly for the purposes of creating economic opportunity for small and medium-sized enterprises (SMEs).

New Zealand should adopt and build upon these provisions. Within the digital trade chapter, New Zealand should push for a specific section on open data, which should start with the general recognition that opening up public information for re-use has considerable and widespread benefits to government, industry, and the public and mention that innovation is an explicit reason to release public data. The DEPA should require parties to have an open-by-default framework for government data in place (without being prescriptive, as each country will approach the issue in their own way) and demand that trading partners should adhere to best practices for open data, including ensuring it is published in open, machine-readable formats.

New Zealand should link these provisions to the fact that enacting data standards for government data (as per global best practices) increase the value for everyone as it increases both the quantity and quality of data firms can use to provide new, data-driven goods and services. In line with this, New Zealand should explicitly reference international agreements and partnerships that signal that a country is actually committed to enacting policy best practices. A good reference point for provisions on open government data is the G8 Open

Data Charter, which, as well as supporting the release of data to promote transparency, is more explicit about the quality and format in which data should be released and, importantly, adds innovation as a reason to release data.[97] The four EU members of the G8 (now G7)—France, Germany, Italy, and the United Kingdom—have all signed up to the charter (the EU has also endorsed the G8 Open Data Charter for its own institutions). Another good initiative worth referencing is the Open Government Declaration, a global open data initiative led by the Open Government Partnership (OGP), an international organization promoting more open, effective, and accountable government.[98] New Zealand and Chile are already members of the OGP.

DEPA SHOULD SUPPORT ELECTRONIC LABELLING FOR ICT PRODUCTS

As ICT products get smaller, manufacturers face the challenge of fitting multiple small labels on their products to show a range of regulators and consumers that these products conform to regulations. This can lead to jumbled collections of barely legible labels that convey little or no information. As ITIF argues in "How E-Labels Can Support Trade and Innovation in ICT," allowing the display of regulatory and other product information via electronic means—an "e-label"—is a sensible solution that ensures labels don't inhibit product innovation while helping to minimize cost and maximize consumer convenience.[99] New Zealand should include a provision on e-labelling in the DEPA given its close connection to the devices which drive the digital economy.

Traditionally, manufacturers have had to use physical labels on ICT products to convey the compliance information required to facilitate market access to a country, such as to address concerns over safety, electromagnetic interference, energy, materials, and/or recycling. Manufacturers tend to place product labels on a single panel so as to allow this information to be more easily located, fabricated, and controlled, as well as to minimize the negative visual impact to what may otherwise be a sleek and innovative product appearance (which is critical for market appeal). Manufacturers must either etch or print these labels on the device or on a label attached to the device or associated packaging. Complicating this process is the fact that some countries dictate where labels must be physically placed. Given the number of such labels required for major ICT products, the requirement to use physical labels increases costs and potentially limits design options while ineffectively conveying information to consumers about products. A major problem with physical labels is that many ICT products are made for distribution in multiple markets, meaning that a product can have 20 or more regulatory labels.

Compliance markings serve two audiences—regulators and consumers. But even then, it is an open question as to how much attention consumers give to physical labels. E-labeling does not undermine each country's right to regulate ICT products for public health, safety, and other reasons. E-labeling is simply a way to convey information to consumers and regulators more effectively and efficiently than is possible with physical labels. Growing smart phone ownership means that many consumers have the ability to easily access information about their products electronically, whether this is on their device or via a link to a webpage on the Internet.

There are a range of benefits to e-labeling:

- Greater information and utility: Consumers and regulators are faced with the challenge of deciphering a multitude of labels crammed together onto a single panel of an ICT product, which is further complicated as ICT products get smaller. E-labels offer a more accessible and understandable mechanism for users to find the mark that is relevant to them, accompanying product statements and instructions, and any further details the manufacturer wishes to include, such as product warranties, contact details, recycling, and trade-in opportunities. Furthermore, e-labels can be more accessible, comprehensive, and readable for the simple fact that there are fewer size constraints when it comes to the electronic display of information, in contrast to the small font typically used in printed statements that accompany ICT products when sold.

- Easier enforcement: A master list of labels and compliance information on the Internet or on the device, kept up to date by manufacturers, would offer real-time compliance information far beyond a simple mark on a tiny label. For the most part, the e-label has the same information as the physical label. Regulators can easily check if a manufacturer is abiding by e-labeling requirements (including changes) by simply checking the e-label on devices with an in-built screen, or, if using a code or link for devices with no screen, by checking the designated website of the product.

- Reduced environmental impact: E-labels allow manufacturers to reduce the material they use in labels and the replacement of labels. This includes the waste involved in recalling products and replacing labels (which often requires replacing the product's entire back plate) if requirements change after the product is manufactured and distributed. Furthermore, an e-label provides an easier way for manufacturers to provide details to consumers on how to environmentally dispose of the product.

- Reduced impact on product innovation: Technological innovation means that ICT products are shrinking in size such that physical labeling requirements may become a constraint on product design as manufacturers reach a point where they need to alter the optimal design of a product just to satisfy labeling requirements. This could act as a brake on product design and innovation, which, in many product categories, would otherwise lead to products getting smaller still. Furthermore, by making product design easier, e-labeling can shorten the launch schedule for new products, as for major ICT manufacturers a change in something as simple as a physical label can take months to include as part of complex design and manufacturing processes.

- A live and interactive label: Physical labels are static and problematic in terms of updating—it takes time and money to recall products and remove and replace physical labels. In contrast, e-labels can act as interactive sites for product information that can be updated remotely to address any product user issues, manufacturer contact details, regulatory changes, and inaccuracies, such as typographical errors.

- Cost savings: As ICT products have become smaller and more aesthetically appealing, etching or applying physical labels requires more design time and expensive equipment. Manufacturers spend

significant amounts of money on the creation, control, maintenance, and production of product markings, packaging, and instruction sheets that have traditionally been used to convey required certification or conditions-of-use information. These costs increase if manufacturers need to modify labels, re-work products, and perform in-country retrofits due to changing labeling requirements. E-labeling reduces or eliminates these costs without sacrificing a user's access to relevant regulatory information.

E-labelling remains a relatively new approach to conveying compliance and other information to regulators and consumers. While several countries currently allow e-labeling, only a few companies have begun using it. However, this list includes major ICT producers and markets for ICT products, including China, Japan, and the United States. Other major economies, such as India, are considering following suit.

Besides Canada, Mexico, and the United States, other major trading partners also allow e-labels:

- Australia: In 2015, Australia enacted the Telecommunications (Labelling Notice for Customer Equipment and Customer Cabling) Instrument 2015, which allowed e-labeling for devices with an inbuilt display as part of broader changes to the testing, labeling, and record-keeping obligations for suppliers of specified telecommunications equipment.[100] Australian industry groups supported the development of e-labeling.[101] The compliance label for telecommunications products in Australia is the Regulatory Compliance Mark, which can be displayed electronically on products with built-in screens.

- Japan: In 2010, Japan enacted administrative reforms to allow e-labels for devices with an inbuilt screen. Documentation that accompanies the device must show the user how to display the e-label.[102]

- Malaysia: On June 1, 2015, the Malaysian Communications and Multimedia Commission (MCMC) enacted rules allowing e-labels for communications products with an inbuilt screen. The Malaysian approach is voluntary, not mandatory. Details of how to access the marks must be included in the accompanying documentation.[103]

- Singapore: Since 2012, Singapore has allowed e-labels as compliance labels for devices with an integral screen. The product documentation accompanying the product must explain how the label is displayed.

The potential problem is that as more countries allow e-labeling, they might make it overly complicated and prescriptive and substantially different from country to country. Divergent approaches to e-labeling would undermine its benefits in terms of simplicity and efficiency. Furthermore, if countries design approaches that are significantly different from one another (including a potential future international standard on e-labeling), e-labeling then becomes a potential technical barrier to trade in ICT goods. As we've seen with other technical issues, an outlier country could use its e-labeling approach as a barrier to keep foreign ICT products out, as manufacturers must decide whether to spend the time and money to alter the design of their product to meet the specific regulatory requirements for an individual country. Recent history shows us that fragmentation is a real threat to global trade in ICT products. ITIF demonstrated how this can happen in its "The Middle

Kingdom Galapagos Island Syndrome: The Cul-De-Sac of Chinese Technology Standards" report, which explained how China's use of indigenous technology standards discriminates against foreign firms in order to support domestic ones.[104] This is why countries need to ensure that as they consider allowing e-labeling, they work toward achieving a degree of alignment with other countries, ideally through an international standard, to ensure e-labeling requirements don't hinder the global design, production, and trade in ICT products.

Country-to-country differences in technical regulation and standards and conformity assessment procedures raise compliance costs for companies operating across multiple countries. Such costs are particularly daunting for small-and medium-size enterprises. While it is difficult to estimate the precise costs involved, the need to comply with such different approaches involves direct and indirect costs for producers and exporters. The Organization for Economic Cooperation and Development (OECD) finds that differing standards and technical regulations, combined with the cost of testing and compliance certification, could constitute between 2 and 10 percent of overall production costs.[105]

New Zealand should use DEPA to setup a framework for members to allow e-labeling (at the moment, Chile is the only one of the initial three members to not allow e-labels). As the first trade agreement to include language on electronic labeling, USMCA is a model for New Zealand. USMCA defines e-labels as "the electronic display of information, including required compliance information." In article 12.C.4 in the sectoral annexes chapter of USMCA, under Regional Cooperation Activities on Telecommunications Equipment, the parties agreed that "If a Party requires equipment subject to electromagnetic compatibility and radio frequency requirements to include a label containing compliance information about the equipment, it shall permit this information to be provided through an electronic label." [106] This should be the first step for a country moving toward a compliance labeling systems that accounts for digital innovation. Parties should also reference ongoing work towards an international standard for electronic labeling (talks on ISO/IEC CD 22603 are ongoing at the International Organization for Standardization).[107]

The second step would be for New Zealand to use DEPA to setup a mechanism for respective agencies to cooperate and exchange information about their electronic labeling requirements, with a view to facilitating compatibility.[108] Besides accounting for the fact that Chile does not currently allow e-labels, this would allow a (technologically) flexible approach, as policymakers in New Zealand, Singapore, and Chile should view the development of e-labeling policy as an iterative process. They can start by allowing e-labeling to display information for products with an inbuilt screen, such as a smart phone, before expanding the scope of products in subsequent revisions, such as to include products that don't have a screen but can connect to one. This can eventually extend to allowing e-labels to be accessed through URL or QR (Quick Response) codes for ICT products that don't have a screen. In this way, policymakers can move forward with basic e-labeling rules, even if they aren't ready for advanced ones.

DEPA SHOULD SUPPORT OPEN DATA FRAMEWORKS AND TECHNICAL STANDARDS FOR APIS

A fundamental building block of the data market is access. Not in the coercive sense, in terms of forcing private firms to hand over data, but in sectors where there are clear benefits to all parties from allowing new connections and digital goods and services. In these select cases, policymakers should look to enact a

framework that creates a clear, standardized, and open process for firms to access data. Application programming interface (API)-related frameworks are at an early stage of development and vary around the world (both between different domestic sectors and between countries). Given this, New Zealand could use DEPA to make clear their interest in the issue by identifying it as an area for cooperation and information exchanges. This could extend to developing shared high-level principles and standardized transmission mechanisms (for APIs), which are likely to become a key tool to facilitate access to data and the delivery of digital goods and services in the future. The greater the compatibility and commonality between standards that can be achieved at such an early stage, the greater the potential for New Zealand's firms to be able to develop and deliver digital products in these (and other) markets.

"Open APIs" are one of the best-practice tools to use to help facilitate access to data in certain public and private sectors, which hold valuable sensitive data, but lack mechanisms to securely and efficiently share it with one another. Rules around APIs form the basis for all the "open banking" frameworks (for the voluntary exchange of bank-held data) proposed to date.[109] An API is a set of commands, functions, protocols, and objects that programmers can use to create software or interact with an external system. It provides developers with standard commands for performing common operations so that they do not have to write the code from scratch. APIs are routinely used within organizations, but open APIs allow third-party access to information as well. API-related issues deserve attention, as they facilitate the sharing of data to promote innovation, trade, and other societal benefits. However, policy discussions on open API frameworks should not be used as a disguised attempt by misguided advocates that have argued that businesses which possess large quantities of data, such as social media companies, present inherent competition concerns.[110] As ITIF argues in "The Myth of Data Monopoly: Why Antitrust Concerns About Data Are Overblown," these concerns are misplaced for a number of reasons, one being that competitors can often obtain similar data from other sources.[111]

Beyond banking (detailed below), policymakers could consider mandated data sharing rules and open APIs to address specific cases in which a small number of firms have exclusive access to particular datasets, which they could use to exploit their market power to limit access to that data through both technical and administrative means without any legitimate business justification. In "Blocked: Why Some Companies Restrict Data Access to Reduce Competition and How Open APIs Can Help," ITIF analyzed this scenario in the United States in the real estate, banking, and air travel sectors.[112] This type of anti-competitive behavior limits innovation and hurts consumers, and when these problematic practices occur, policymakers should intervene. Open APIs should be part of the antidote to these scenarios.[113]

The financial sector is the sector where APIs are having their earliest, biggest impact as banks and non-banking fintech companies use new digital technologies and partnerships to compete for market share by providing innovative digital goods and services. The evolution from a closed model, where each financial institution retained and controlled the information it collected about its customers, to an open model, has the potential to improve competition in the sector and see the creation of new products and services based on that data.[114] Open banking provides great opportunities for all sorts of businesses, including existing banks and fintechs, to innovate, strengthen customer relationships, and gain a share of new emerging financial product and service markets. It also holds potential for other financial services, such as insurance and superannuation.

This has led to various regulatory reforms around the world, including on APIs, as it raises associated concerns about financial stability, regulatory oversight and auditing, data privacy, and data security.[115]

There is a clear global trend toward open banking frameworks in the financial sector, including in Australia, the EU, Singapore, and the United Kingdom. For example, the EU and member nations have taken important steps in the right direction on open APIs through the Payment Services Directive (PSD2).[116] In Australia, Scott Farrell's "Review into Open Banking: giving customers choice, convenience, and confidence" laid out a regulatory blueprint.[117] The United Kingdom's Open Banking Standard demonstrates how this approach could be taken further by requiring banks to make their data available in a standardized format and therefore easier for third parties to access and use to develop further innovations for consumers.[118] In the case of both PSD2 and the United Kingdom's Open Banking Standard, the overriding goal is to ensure consumers can share their personal financial data with third parties and increase market transparency about bank fees, not to force companies to turn over their own proprietary data. In contrast, there is no centralized approach to data governance in the United States (although the U.S. Treasury Department has examined the regulatory issues), which has given rise to a series of fintech innovators and a patchwork of one-off bank agreements (such as partnerships struck in the United States by Chase and Wells Fargo with Xero and Finicity).[119] However, the absence of a U.S. framework has also led to some financial institutions blocking certain firms from accessing their APIs, variations in means of accessing data (i.e. inconsistent API standards), and inconsistent policies for charging for access to use them. Meanwhile, Singapore has developed a large fintech market, built largely around APIs, for instance, for risk-decisioning in the absence of formal credit-scoring agencies (the Monetary Authority of Singapore provides regulatory oversight).[120]

Data sharing frameworks can vary significantly based on the entities obliged to make data shareable (including whether it is mandatory or voluntary), the type of customers entitled to share data, the timing of the data sharing (real time vs. deferred), how data is shared between the parties, the entities with which data can be shared, and the standardization of transmission mechanisms (APIs).[121] As it relates to New Zealand and the DEPA, the central challenge for a section on open data would be to bring together respective domestic agencies to try and develop standardized communication mechanisms via APIs. Table 1 below provides an overview of how major, open banking frameworks deal with API standards.

Table 1: How Different Mandatory Data Sharing Frameworks Manage the Standardization of the Transmission.[122]

	Opening Banking (UK)	PSD2 (EU)	GDPR (EU)	Open Banking (Australia)	Open API Framework (Hong Kong)	FinTech Law (Mexico)
Standardization of the transmission	Using mandatory standardized APIs.	Only basic standardization is necessary.	No standardization is mandatory.	APIs will be developed, but screen scraping will not be forbidden.	Various internationally recognized standards.	Standardized APIs (pending definition).

Whether common regional or global standards will emerge as countries begin to enact open banking systems is unclear, but the stakes are high. If countries pursue conflicting standards for APIs, the resulting fragmentation could inhibit the spread of open banking and other open data frameworks and the ability of

firms in one country to achieve critical economies of scale through access to data in a foreign market.[123] This scenario would be similar to what we are already seeing with regard to countries enacting data localization measures and country-specific cybersecurity standards. To the extent that these and related requirements (such as for API standards) heavily restrict the use of data across borders, efforts to integrate and rationalize cross-border financial activity through open banking regulations may be limited.[124] To promote open banking at a regional and global level then, New Zealand and its likeminded trading partners should coordinate their efforts.

New Zealand is already heading in the right direction in using APIs to improve competition and innovation in the financial sector.[125] In early 2018, Payments NZ unveiled an industry API pilot (with six partners) to test open banking and digital payments in the country. Since then, Payments NZ has been working on a shared API framework and pilot to bring common API standards and an API standards ecosystem to life.[126] It is an emerging issue that could hold potential digital trade implications given each country's respective frameworks will set the terms and standards for access to data, which can be used as an input to design and deliver new digital goods and services. It overlaps with other data-related issues covered by digital trade agreements, such as privacy, cybersecurity, and consumer protection, without the need to be overly prescriptive. However, conceptually, there's no clear reason why technical standards should vary between trading parties. In such a case, a firm in New Zealand that has developed an API as part of an innovative new financial service could use the same software (pending other regulatory approvals and considerations) to access data from a bank in a trading partner in other to provide the same service into this other market. Eliminating or minimizing technical differences makes such digital trade easier.

DEPA negotiations are an opportunity for New Zealand to work with Singapore and Chile to outline their commitment to share information and best practices as they each enact their own respective frameworks. These discussions could lead to hortatory language in a digital trade chapter about the role that open APIs can play in facilitating access to data in certain sectors, that such access promotes innovation, competition, and trade, that such frameworks should be open to firms from anywhere (as long as they abide by local data related laws and regulations), and that the parties will work towards developing compatible (technical) standards in defining API frameworks.

DEPA SHOULD SUPPORT THE ROLE OF ELECTRONIC SIGNATURES AND INVOICING IN DIGITAL TRADE

Electronic signatures and invoices represent basic building blocks for firms wishing to engage in digital trade.[127] The parties need to be able to use electronic signatures as part of a digital trade transaction. Ensuring that customers can provide approval or consent online when downloading a digital product, checking out of a digital shopping cart, or validating payrolls are all basic steps for digital trade. Meanwhile, the widespread adoption of electronic invoice-based taxation and accounting systems facilitates digital trade (and traditional trade) by facilitating easier accounting and tax reporting in multiple jurisdictions (especially if firms use accounting service providers who operate across multiple countries) and help firms engaged in trade (such as through more efficient factoring or managing accounts receivable). However, there is the potential for countries to enact unique technical standards that act as a barrier to digital trade, which New Zealand should prohibit as part of DEPA negotiations.

New Zealand should open sections on electronic signatures and electronic invoices by noting the importance of both issues to digital trade. At the heart of these efforts should be the three core principles advanced by the United Nations Commission on International Trade Law (UNCITRAL, who set out model electronic transaction and signature laws)– non-discrimination, functional equivalence, and technological neutrality.[128] New Zealand should use DEPA negotiations to push beyond basic electronic signature and authentication provisions (such as those in CPTPP, which are still very much needed) and aim to enact interoperable systems that prohibit country-specific technical requirements that barrier digital trade. Otherwise, divergent domestic rules on electronic transactions, signatures, and invoices make cross-border digital activities more complex, and more costly, for New Zealand firms doing business in multiple markets.[129]

Building out these provisions should be achievable. New Zealand, Singapore, and Chile all have non-restrictive electronic signatures and invoicing frameworks.[130] New Zealand obviously recognizes the broader significance, given its support in creating the Australia and New Zealand Electronic Invoicing Board (ANZEIB) and its intention to develop an interoperable framework for trans-Tasman e-invoicing.[131] While specific barriers related to these issues may not yet be a major problem in foreign markets, there are cases (in Mexico and Brazil, as detailed below) that highlight how they could become another technical barrier to digital trade. Given their essential role in facilitating digital trade, New Zealand should get out in front of these potential barriers and push for strong provisions to provide certainty for its firms. Such a move would set a clear, high bar for other countries that may eventually join the DEPA and would send a broader signal about New Zealand's effort to set the gold standard in relation to comprehensive digital trade rules.

New Zealand should still cover the basics in DEPA negotiations by ensuring that its trading partners have a legal framework in place for electronic and digital signatures, as without these, users must rely on paper documents. According to the United Nations Conference on Trade and Development (UNCTAD), 145 countries have enacted such laws, of which 104 are developing or transitioning economies. Almost half, 46.3 percent, of African economies have adopted e-transactions laws, compared to 72 percent of Asian, 81.8 percent of Latin American and Caribbean, and 97.6 percent of developed economies.[132] While this will not be an issue in Chile or Singapore, it remains an issue for many other countries. New Zealand should include this commitment to reinforce its role as a necessary part of the legal framework for digital trade, as according to the OECD-WTO Global Review 2017 Aid for Trade Monitoring Exercise, electronic signatures were ranked fourth among the top ten challenges facing enterprises and consumers when accessing and using Internet services.[133] Given Chile's and Singapore's membership in the CPTPP, it should not be controversial to insist that trade partners maintain a legal framework governing electronic transactions consistent with the principles of the UNCITRAL Model Law on Electronic Commerce 1996 or the United Nations Convention on the Use of Electronic Communications in International Contracts.[134] In line with this, New Zealand and its partners should again (as in CPTPP) include the explicit provision that no party shall maintain measures that differentiate between the legal treatment of digital vs. physical signatures and that parties to a transaction should be able to determine the authentication method.[135]

However, New Zealand needs to go beyond these basic provisions on electronic signatures, as there is the potential for country-specific technical requirements to act as a barrier to digital trade.[136] While many

countries have enacted UNCITRAL model laws, there is no universal approach to implementation, which gives rise to substantial differences between how economies enact their own e-signature laws.[137] Hence, New Zealand should push for parties to commit to enacting interoperable systems and to remove country-specific technical requirements for electronic and digital signatures and electronic invoicing systems. CPTPP included the more limited commitment that parties "shall endeavor to avoid any unnecessary regulatory burden on electronic transactions" and that parties "shall encourage the use of interoperable electronic authentication."[138] A more ambitious goal would be somewhat similar to other trade agreements countries have put in place to ban specific actions, such as the Australia-Japan FTA, where both parties agreed that they will not enact "measures regulating e-transactions that …(b) discriminate between different forms of technology."[139] This extends the UNCITRAL central principle of non-discrimination and technological neutrality.
New Zealand's trade negotiations need to recognize that countries fall into one of two main categories in terms of electronic signatures—prescriptive and minimalist—to better understand why they need these provisions. Problems generally arise when countries pursue a prescriptive approach, which usually requires firms to use a specific method or digital signature technology to sign documents electronically in order for those documents to be legally recognized. Indonesia, for example, recognizes only digital signatures created through a specific certificate provider.[140]

Another example is Brazil, which allows for e-signatures, with important restrictions. Under Brazilian law, a written signature may not be required for a valid contract but may be needed in case of a dispute. E-signatures may be admissible as acceptance of a contract—for instance, confirming purchase orders, invoices, and sales agreements.[141] However, while local technology standards and use are not required for an e-signature to be considered valid under Brazilian law, there are exceptions for certain, government-regulated cases, such as when parties are engaged in foreign exchange transactions, factoring, and transactions with the Brazilian government. In these cases, Brazil forces the various parties to use e-signatures that use Brazilian IT infrastructure and services in the form of a local government-authorized certification authority called ICP Brazil.[142] ICP Brazil maintains the root certification authority and requirements that must be met for both government-recognized timestamping and public key infrastructure (PKI) signature policies. When a local certificate authority, such as a tax administrator, updates their digital certificate requirements (so that they can apply what they deem to be the most appropriate security measures), all digital providers need to revise their country-level services to account for this, which can cause brief complications around compatibility. The use of this local tech standard diverges from UNCITRAL model law. Such local certification protocols are a barrier for firms that aim to use a fairly standardized, region-wide IT systems. As DocuSign (a major electronic signature and digital transaction management company) explains, due to the difficulty of distributing and maintaining these digital certificates, use of ICP Brazil-backed electronic signatures in Brazil is generally limited to a few high-value, high-volume transactions.[143] This undermines the broader adoption and use of EIs in Brazil's economy.

Instead, New Zealand should seek to embed within its trade agreements the framework and rules that support the minimalist approach, which is considered business-friendly as it is easier to use and more adaptable to new technologies. Besides New Zealand, minimalist laws have been adopted in the United States, Canada, Australia, and Singapore.[144] For example, Australia's Electronic Transactions Act (1999) established that electronic signatures can take the place of handwritten signatures for nearly all documents except certain

exclusions such as wills and powers of attorney.[145] Meanwhile, in 2014, the EU adopted new legislation designed to provide, for the first time, a consistent single market for the cross-border trade use of electronic signatures across the EU. The regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS) mandates mutual recognition of e-signatures across Europe. Similar to the situation with differential UNCITRAL adoption at the global level, UNIDAS replaced an earlier EU electronic signature directive that had been implemented in different ways by individual member states that, in practice, meant that many members would not recognize each other's electronic signature laws (and that electronic signatures were not applicable across the EU). According to the European Commission, the diverging national frameworks made it "de facto impossible to conduct cross border electronic transactions."[146] This is the scenario that New Zealand should aim to avoid in advocating for more comprehensive rules on electronic signatures and invoices.

New Zealand should seek explicit provisions to fully articulate UNCITRAL's principle of technological neutrality. Similar to existing agreements, New Zealand and its partners should allow participants in e-transactions to determine for themselves the appropriate authentication technology, in that, governments not limit the transactions' participants to using designated authentication technologies and implementation models.[147] If there are exceptions to this general prohibition, New Zealand should get its trading partners to explicitly identify the (hopefully narrow) specific instances where parties may require authentication services for certain transactions to meet performance standards or be provided by a legally established provider, approved by an authority in accordance with the domestic law.[148]

New Zealand should ensure that electronic signatures and invoicing issues are explicitly mentioned as topics for regulatory cooperation between trading partners to ensure that there is a mechanism for the various agencies to work together. Similarly, all recent EU regional trade agreements require parties to maintain a dialogue on regulatory issues raised by e-commerce, addressing various issues, including the recognition of certificates of e-signatures and facilitation of cross-border certification services.[149] Additionally, the Korea-Peru FTA commits parties to establishing cooperation mechanisms between the national accreditation and digital certification authorities for electronic transactions.[150]

Ultimately, New Zealand and its DEPA partners should aim to mutually recognize each other's digital certificates and electronic signatures. This could follow a period of engagement and cooperation between the respective agencies involved in overseeing electronic signatures and electronic invoicing. New Zealand should look to go one further than Pacific Alliance countries (Chile, Colombia, Mexico, and Peru), which negotiated the "Additional Protocol to the Framework Agreement of the Pacific Alliance," whereby they agreed that parties may consider recognizing advanced or digital e-signature certificates issued by a certification service provider operating in the territory of another party.[151] The Additional Protocol also requires parties to establish mechanisms and approval criteria that promote the interoperability of electronic authentication between them, according to international standards. New Zealand should aim to replicate this mechanism and approval criteria.

Prohibit Local Encryption and Security Requirements for Electronic Invoicing

Modern cryptographic technology protects the authenticity and integrity of data, but country-specific technical requirements can act as a barrier to data flows and digital trade, especially how often firms (especially SMEs) rely on cloud-based data services to engage in digital trade. A recently revised policy in Mexico provides a case in how country-specific technical policies can act as a barrier to digital trade and the use of electronic invoicing. New Zealand should ask its trade partners not to enact unique, country-specific technical security requirements for electronic invoicing, which act as a de facto form of data localization.

Until recently, Mexico had a policy in place which created local data storage, protection, and encryption issues. Mexico's Tax Authority (known by its Spanish acronym—SAT) previously mandated that firms wanting to manage electronic invoices in Mexico (known by their Spanish acronym—PAC) needed to use a local Hardware Security Module (HSM).[152]

HSMs act as "trust anchors" that protect the cryptographic infrastructure by securely managing, processing, and storing cryptographic keys inside a hardened, tamper-resistant device within the data center. Electronic invoicing relies on the authorized firm and its HSM and PKIs to generate a digital signature (i.e., the process that is commonly used to digitally sign a document) and certify that digital signatures it receives are authentic, thus ensuring the integrity of the transmitted data attached to the signature. The HSM's role is to generate an asymmetric key pair—a public key and a private key. The public key is used to create a specific certificate request to be sent to a country's tax authorities. The private key is stored within the HSM's secure cryptographic device. Acting as a trusted certificate authority, the tax authority uses its private key to sign the PAC's certificate request and generates a separate certificate (which contains certain other identifying attributes and its public key) along with the initial, parent certificate to the PAC.

This allows the PAC and Mexico's tax authorities to mutually authenticate entities and to ensure that their communications are secure and trusted. Once mutual authentication has occurred, the PAC uses its private key to digitally sign their customer's financial information (which is stored in an XML-based file format in accordance with local regulations (Mexico's Miscellaneous Tax Resolution)). The PAC must use the Mexican tax authority's public key (enclosed in the digital certificate sent to the PAC for authentication) to encrypt the data. Mexico's tax authorities then use both the public and private keys to verify the PAC's digital signature. Once this process is complete, Mexico's tax authorities send the PAC a final validation message.[153]

Mandating the use of a local HSM meant that firms that provided EI services across many countries had to pay for a duplicative and expensive HSM in order to install and use SAT's digital certificate. This requirement acted as a de facto data localization requirement given that the crypto key and associated EI data, needed to be stored within Mexico in case of an SAT query or audit.[154]

Thankfully, Mexico recently decided to remove this local data storage and protection requirement and allow PACs to use cloud-based data protection and storage services. For example, cloud service providers like Microsoft Azure offer a dedicated HSM service for clients. This service has been certified by the Federal Information Processing Standard (FIPS) 140 (Security Requirements for Cryptographic Modules). This is a U.S. and Canadian government standard that defines a minimum set of security requirements for products

that implement cryptography. This standard is designed for cryptographic modules that are used to secure sensitive but unclassified information. Microsoft Azure's HSM is certified as a level 4 device (on a scale of 1-4, with 4 being the highest level).[155] This certification allows clients to meet the most stringent security and compliance requirements of clients. As part of this service, clients have full administrative and cryptographic control over Azure's dedicated HSMs. Microsoft does not have visibility into its client's cryptographic keys. This service is provided directly on a client's virtual network on Azure and can be connected to on-premises infrastructure via a virtual private network.[156]

All of this demonstrates that New Zealand should push for electronic invoice-focused provisions that ensure that data protection rules do not depend on the geography of data storage, as many leading data storage providers can provide audited, best-in-class cybersecurity protection. Instead, New Zealand should work with trade partners to explicitly identify those international, risk-based standards that firms should use to demonstrate their commitment to data protection. For example, beyond FIPS certification for HSMs, Microsoft pursues and secures a broad set of international and industry-specific compliance standards, such as the EU General Data Protection Regulation (GDPR), ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, in a manner typical of many leading cloud service providers. Globally competitive cloud storage providers simultaneously put their services through rigorous third-party audits, such as those provided by the British Standards Institute, to ensure that the services adhere to various standards.[157]

ENDNOTES

1. Nick Wallace, "Europe Should Put Data at the Service of Society," *Euractiv*, October 14, 2016, https://www.euractiv.com/section/digital/opinion/europe-should-put-data-at-the-service-of-society/; Daniel Castro and Joshua New, "The Promise of Artificial Intelligence" (Center for Data Innovation, October 2016), http://www2.datainnovation.org/2016-promise-of-ai.pdf; Alexander Kostura and Daniel Castro, "Europe Should Promote Data for Social Good" (Center for Data Innovation, October 3, 2016), http://www2.datainnovation.org/2016-data-social-good.pdf.

2. For example, see: Nick Wallace and Daniel Castro, "The State of Data Innovation in the EU" (Center for Data Innovation, October 2017), http://www2.datainnovation.org/2017-data-innovation-eu.pdf; Daniel Castro and Travis Korte, "Data Innovation 101" (Center for Data Innovation, November 2013), https://www.datainnovation.org/2013/11/data-innovation-101/.

3. Nigel Cory, "The Ten Worst Digital Protectionism and Innovation Mercantilist Policies of 2018" (The Information Technology and Innovation Foundation, January 28, 2019), https://itif.org/publications/2019/01/28/ten-worst-digital-protectionism-and-innovation-mercantilist-policies-2018; Nigel Cory, "The Ten Worst Innovation Mercantilist Policies of 2017" (The Information Technology and Innovation Foundation, January 22, 2017), https://itif.org/publications/2018/01/22/worst-innovation-mercantilist-policies-2017; Nigel Cory, "The Ten Worst Innovation Mercantilist Policies of 2016" (The Information Technology and Innovation Foundation, January 9, 2016), https://itif.org/publications/2017/01/09/worst-innovation-mercantilist-policies-2016; Nigel Cory, "Why China Should Be Disqualified From Participating in WTO Negotiations on Digital Trade Rules" (The Information Technology and Innovation Foundation, May 9, 2019), https://itif.org/publications/2019/05/09/why-china-should-be-disqualified-participating-wto-negotiations-digital.

4. Organisation for Economic Cooperation and Development (OECD), *Harnessing the digital economyfor developing countries* (Paris: OECD, December 22, 2016), https://www.oecd-ilibrary.org/development/harnessing-the-digital-economy-for-developing-countries_4adffb24-en.

5. Organisation for Economic Cooperation and Development (OECD), *The digital economy, multinational enterprises and international investment policy* (Paris: OECD, 2018), https://www.oecd.org/daf/inv/investment-policy/the-digital-economy-multinational-enterprises-and-international-investment-policy.htm.

6. Robert Atkinson, "The Task Ahead of Us: Transforming the Global Economy With Connectivity, Automation, and Intelligence" (The Information Technology and Innovation Foundation, January 7, 2019), https://itif.org/publications/2019/01/07/task-ahead-us-transforming-global-economy-connectivity-automation-and.

7. Daniel Castro and Robert Atkinson, "Beyond Internet Universalism: A Framework for Addressing Cross-Border Internet Policy" (The Information Technology and Innovation Foundation, September 2014), http://www2.itif.org/2014-crossborder-internet-policy.pdf.

8. Castro and Atkinson, "Beyond Internet Universalism: A Framework for Addressing Cross-Border Internet Policy."

9. Daniel Castro, "The False Promise of Data Nationalism" (Information Technology and Innovation Foundation, December 2013), http://www2.itif.org/2013-false-promise-data-nationalism.pdf.

10. Nigel Cory and Stephen Ezell, "Post-Hearing Submission: Investigation No. TPA-105-003, United States-Mexico-Canada Agreement: Likely Impact on the U.S. Economy and on Specific Industry Sectors" (The Information Technology and Innovation Foundation, December 17, 2018), https://itif.org/publications/2018/12/17/comments-us-international-trade-commission-regarding-united-states-mexico.

11. Nigel Cory, "Vietnam's cybersecurity law threatens free trade," *Nikkei Asian Review,* August 15, 2018, https://asia.nikkei.com/Opinion/Vietnam-s-cybersecurity-law-threatens-free-trade.

12. Nigel Cory, "EU digital trade policy proposal opens a loophole for data protectionism," *Euronews,* July 16, 2018, https://www.euronews.com/2018/07/16/eu-digital-trade-policy-proposal-opens-a-loophole-for-data-protectionism-view.

13. For example: Delegation of the European Union to India and Bhutan, *Submission on draft Personal Data Protection Bill of India 2018 by the Directorate-General for Justice & Consumers to the Ministry of Electronics and Information Technology (MeitY)* (Brussels: European Union, November 19, 2018),

    https://eeas.europa.eu/delegations/india/53963/submission-draft-personal-data-protection-bill-india-2018-directorate-general-justice_en.

14. "Privacy Act 1993," New Zealand Parliamentary Counsel office website, http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM297038.html.

15. For example, firms may implement (and demonstrate) accountability through various internal privacy and information management programs, regulated frameworks (such as the EU's Binding Corporate Rules and the EU-US Privacy Shield), industry codes of conduct, third-party certifications and seals, and international standards. Binding corporate rules state firms may transfer personal data across borders within a single company. See: "The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society" (Center for Information Policy Leadership, July 23, 2018), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf.

16. When determining whether a country has jurisdiction over an organization, factors such as physical presence, business activity, and marketing are likely to be considered.

17. International Consumer Protection and Enforcement Network website, https://www.icpen.org/; Global Privacy Enforcement Network website, https://www.privacyenforcement.net/.

18. "APEC Cross-border Privacy Enforcement Arrangement (CPEA)," Asian-Pacific Economic Cooperation, https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx.

19. Federal Trade Commission, International Competition and Consumer Protection Cooperation Agreements, https://www.ftc.gov/policy/international/international-cooperation-agreements.

20. The Office of the Privacy Commissioner of Canada (OPC), Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information

Commissioner (PIPEDA Report of Findings #2016-005), August 22, 2016, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2016/pipeda-2016-005/.

21. See: Robert Atkinson, "Don't Just Fix Safe Harbor, Fix the Data Protection Regulation," *Euractiv,* December 18, 2015, https://www.euractiv.com/section/digital/opinion/don-t-just-fix-safe-harbour-fix-the-data-protection-regulation/.

22. For example, a report for the European Parliament on data protection in China states that there is "no common ground… found between two fundamentally different systems both in their wording and in their raison d'etre." The report takes a relativist approach by saying China's culture and approach to human rights means the EU should treat China differently when it comes to trade and privacy issues, despite the fact that "China does not have a general data protection act but traces of data protection may be found in a multitude of sector-specific legal instruments." Paul de Hert and Vagelis Papakonstantinou, "The Data Protection Regime in China" (Brussels: report for the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, October 2015), http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf.

23. Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" (Information Technology and Innovation Foundation, May 1, 2017), https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.

24. "Revenue Alert RA 10/02," New Zealand Inland Revenue website, http://www.ird.govt.nz/technical-tax/revenue-alerts/revenue-alert-ra1002.html.

25. For details on cases in India and Turkey, see: Nigel Cory, "The Ten Worst Digital Protectionism and Innovation Mercantilist Policies of 2018" (Information Technology and Innovation Foundation, January 28, 2019), https://itif.org/publications/2019/01/28/ten-worst-digital-protectionism-and-innovation-mercantilist-policies-2018.

26. Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?"; Nigel Cory and Robert Atkinson, "Financial Data Does Not Need or Deserve Special Treatment in Trade Agreements" (Information Technology and Innovation Foundation, April 2016), http://www2.itif.org/2016-financial-data-trade-deals.pdf; Nigel Cory, "The TPP's Financial Data Carve Out—USTR Closes a Loophole for Digital Protectionists" (Information Technology and Innovation Foundation, July 7, 2016), https://itif.org/publications/2016/07/07/tpp%E2%80%99s-financial-data-carve-out%E2%80%94ustr-closes-loophole-digital-protectionists.

27. Julia Fioretti, "EU looks to Remove National Barriers to Data Flows," *Reuters,* September 29, 2016, http://www.reuters.com/article/us-eu-data/eu-looks-to-remove-national-barriers-to-data-flows-idUSKCN11Z19Q.

28. "Requirements for Exemption to Store Electronic Accounting Records Abroad Will Be Abolished," Horten website, accessed November 9, 2017, http://en.horten.dk/News/2015/February/Requirement-for-exemption-to-store-electronic-accounting-records-abroad-will-be-abolished.

29. The ability of the U.S. Federal Reserve and Federal Deposit Insurance Corporation (FDIC) to use and analyze Lehman's IT system and data was reportedly hindered as the bank's network became fragmented, overseas subsidiaries were sold off, some IT systems in overseas subsidiaries were turned off, some key IT staff departed, and restrictions on data flows were imposed due to insolvency filings in other countries—as was the case when

the United Kingdom's financial regulator took over Lehman Brothers' European division. Nigel Cory and Robert Atkinson, "Financial Data Does Not Need or Deserve Special Treatment in Trade Agreements" (Information Technology and Innovation Foundation, April, 2016), http://www2.itif.org/2016-financial-data-trade-deals.pdf; Rosalind Wiggins and Andrew Metrick, "The Lehman Brothers Bankruptcy: The Effect of Lehman's U.S. Broker Dealer" (Yale Program on Financial Stability Case Study 2014-3E-V1), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2588556; Administrative Office of the United States Courts, "Report Pursuant to Section 202(e) of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010" (Washington, D.C., July 2011); Lemieux, "Financial Records and Their Discontents"; "Lehman Brothers International (Europe) in Administration: Joint Administrators' Progress Report for the Period 15 September 2008 to 14 March 2009," PricewaterhouseCoopers, accessed April 4, 2016, http://www.pwc.co.uk/en_uk/uk/assets/pdf/lbie-progress-report-140409.pdf.

30. "Lehman Brothers International (Europe) in Administration: Joint Administrators' Progress Report for the Period 15 September 2008 to 14 March 2009."

31. The law outlined extensive new rules that require "systemically important financial institutions" (SIFIs) to prepare "resolution plans"—also known as "living wills"—that specify a company's strategy for "rapid and orderly resolution in the event of material financial distress or failure of the company. "Resolution Plans," Board of Governors of the Federal Reserve System, accessed April 4, 2016, https://www.federalreserve.gov/bankinforeg/resolution-plans.htm.

32. These "living wills" are required to provide a broad range of information relevant to resolution planning and implementation including, for example, detailed descriptions of organizational structures, credit exposures and cross-guarantees, and supporting data. The relevant section on IT and data states, "Management Information Systems; Software Licenses; Intellectual Property. Provide a detailed inventory and description of the key management information systems and applications, including systems and applications for risk management, accounting, and financial and regulatory reporting, used by the covered insured depository institution (CIDI) and its subsidiaries. Identify the legal owner or licensor of the systems identified above; describe the use and function of the system or application, and provide a listing of service level agreements and any software and systems licenses or associated intellectual property related thereto. Identify and discuss any disaster recovery or other backup plans. Identify common or shared facilities and systems, as well as personnel necessary to operate such facilities and systems. Describe the capabilities of the CIDI's processes and systems to collect, maintain, and report the information and other data underlying the resolution plan to management of the CIDI and, upon request, to the FDIC. Describe any deficiencies, gaps, or weaknesses in such capabilities and the actions the CIDI intends to take to promptly address such deficiencies, gaps, or weaknesses, and the time frame for implementing such actions."

33. Cory, "The TPP's Financial Data Carve Out—USTR Closes a Loophole for Digital Protectionists"; Cory and Atkinson, "Financial Data Does Not Need or Deserve Special Treatment in Trade Agreements."

34. United States Trade Representative, "USMCA: Chapter 17: Financial Services," https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/17_Financial_Services.pdf.

35. Nigel Cory and Stephen Ezell, "Comments to the U.S. International Trade Commission Regarding the United States-Mexico-Canada Agreement" (Information Technology and Innovation Foundation, December 17, 2018), https://itif.org/publications/2018/12/17/comments-us-international-trade-commission-regarding-united-states-mexico.

36. "Mutual Assistance," New Zealand Crown Law website, https://www.crownlaw.govt.nz/assistance-for-foreign-authorities/mutual-assistance/; "Making Requests," New Zealand Crown Law website, https://www.crownlaw.govt.nz/assistance-for-foreign-authorities/making-requests/.

37. Daniel Castro, "The False Promise of Data Nationalism" (Information Technology and Innovation Foundation, December 2013), http://www2.itif.org/2013-false-promise-datanationalism.pdf; Cory, "Cross-Border Data Flows: Where are the Barriers, and What Do They Cost?"

38. The user in the case enters in a "country code" at registration, which Microsoft uses to migrate that user's data to the closest data center, which is in Dublin, Ireland. At the time the warrant was issued, the U.S. government did not know where the data was stored. *Microsoft Corporation v. United States*, 15 F. Supp. 3d 466 (S.D.N.Y. 2014), Document Cloud, 3, http://www.documentcloud.org/documents/1149373-in-re-matter-of-warrant.html.

39. Information Technology and Innovation Foundation, "CLOUD Act Brings Congress Closer to Resolving Problem of Cross-Border Data Access, But Changes Needed to Avoid Jurisdictional Conflicts," news release, February 6, 2018, https://itif.org/publications/2018/02/06/cloud-act-brings-congress-closer-resolving-problem-cross-border-data-access.

40. Jonathan G. Cedarbaum, "Congress Enacts Law Clarifying Reach of Warrants for Overseas Data," *WilmerHale Blog*, March 28, 2018, https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/congress-enacts-law-clarifying-reach-of-warrants-for-overseas-data; Owen Daugherty, "Cruz warns 'Space Force' needed to prevent space pirates," *The Hill*, May 15, 2019, https://thehill.com/opinion/cybersecurity/405422-will-the-us-capitalize-on-its-opportunity-to-stop-data-localization.

41. European Commission, "Security Union: Commission receives mandate to start negotiating international rules for obtaining electronic evidence," news release, June 6, 2019, http://europa.eu/rapid/press-release_IP-19-2891_en.htm; "Regulation on Cross Border Access to E-evidence: Council Agrees Its Position *[sic]*," Council of the EU, July 12, 2018, https://www.consilium.europa.eu/en/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/; For example: Peter Swire and Justin Hemmings, "Recommendations for the Potential U.S.-U.K. Executive Agreement Under the Cloud Act," *Lawfare*, September 13, 2018, https://www.lawfareblog.com/recommendations-potential-us-uk-executive-agreement-under-cloud-act.

42. Alan McQuinn and Daniel Castro, "How Law Enforcement Should Access Data Across Borders" (Information Technology and Innovation Foundation, July 24, 2017), https://itif.org/publications/2017/07/24/itif-calls-united-states-lead-developing-new-approach-international-law.

43. For example, to address some of the issues raised here: "Data & Jurisdiction Work Plan" (The Internet & Jurisdiction Policy Network, February 28, 2018), https://www.internetjurisdiction.net/publications/paper/data-jurisdiction-work-plan.

44. There are three key methods for website blocking: Internet Protocol (IP) address blocking, Domain Name Server (DNS) blocking, and Uniform Resource Locator (URL) blocking.

45. Claire Reilly, "AFP Using Site Blocking Laws to Target Malware," *CNET*, October 22, 2014, http://www.cnet.com/au/news/afp-using-site-blocking-laws-to-target-malware/.

46. Josh Taylor, "FOI Reveals ASIC's IP-Blocking Requests," *ZDNet*, July 1, 2013, http://www.zdnet.com/article/foi-reveals-asics-ip-blocking-requests/.

47. "Approach to Regulating Content on the Internet," Media Development Authority Singapore, August 11, 2016, http://www.mda.gov.sg/RegulationsAndLicensing/ContentStandardsAndClassification/Pages/Internet.aspx.

48. "Banned: Complete List of 857 Porn Websites Blocked in India," *Deccan Chronicle*, updated January 10, 2016, http://www.deccanchronicle.com/150803/nation-current-affairs/article/porn-ban-complete-list-857-porn-websites-blocked-india.

49. "174 Escort Services Websites to Be Blocked: State to Bombay High Court," *dna India*, April 21, 2016, http://www.dnaindia.com/mumbai/report-174-escort-services-website-to-be-blocked-state-to-bombay-high-court-2204387.

50. For example, in 2015, France introduced a law that allows government agencies to order the blocking of websites that advocate acts of terrorism or contain images of child abuse. The legislation was brought in by revisions to the Loppsi Act, and an anti-terror bill passed by the French senate in 2014, but can now be used by the general directorate of the French police's cybercrime unit to force French Internet service providers to block sites within 24 hours, without a court order. In the United Kingdom, the government and ISPs have agreed to implement a system of blocks, similar to that used to keep child abuse material off the Internet, for websites espousing terrorism-related extremist views. Samuel Gibbs, "French Law Blocking Terrorist and Child Abuse Sites Comes Into Effect," *The Guardian*, February 9, 2015, https://www.theguardian.com/technology/2015/feb/09/french-law-blocking-terrorist-and-child-abuse-sites-comes-into-effect. the United Kingdom.

51. Nigel Cory, "The Normalization of Website Blocking Around the World in the Fight Against Piracy Online" (Information Technology and Innovation Foundation, June12, 2018), https://itif.org/publications/2018/06/12/normalization-website-blocking-around-world-fight-against-piracy-online.

52. "Blocking and categorizing content," INTERPOL, accessed May 20, 2019, https://www.interpol.int/en/Crimes/Crimes-against-children/Blocking-and-categorizing-content.

53. Cory, "The Normalization of Website Blocking Around the World in the Fight Against Piracy Online.".

54. Ernesto, "Nearly 4,000 Pirate Sites Are Blocked by ISPs Around The World," *Torrent Freak*, February 10, 2019, https://torrentfreak.com/nearly-4000-pirate-sites-are-blocked-by-isps-around-the-world-190210/.

55. Ibid.

56. "Singapore Allows Dynamic Site Blocking in Landmark Court Ruling – Any Web Address Linking to Blocked Piracy Sites Can Now be Blocked as Well," Motion Picture Association, July 19, 2018, https://www.mpa-i.org/in_the_news/singapore-allows-dynamic-site-blocking-in-landmark-court-ruling-any-web-address-linking-to-blocked-piracy-sites-can-now-be-blocked-as-well/; Nigel Cory, "Using Dynamic Legal Injunctions and AI to Fight Piracy in Real-Time in the United Kingdom" (Information Technology and Innovation Foundation, December 3, 2018), https://itif.org/publications/2018/12/03/using-dynamic-legal-injunctions-and-ai-fight-piracy-real-time-united-kingdom.

57. Cory, "The Normalization of Website Blocking Around the World in the Fight Against Piracy Online."

58. "Anti-Piracy Program FAQ," tag: Trustworthy Accountability Group, accessed July 4, 2016, https://tagtoday.net/piracyfaq/.

59. Such as Kim Dotcom (the owner of the major piracy site Megaupload.com, who was arrested in New Zealand in 2012) or the operator behind Kickass Torrents (who was arrested in Poland in June 2016), "Release for Victim Notification: United States vs. Kim Dotcom, et al," The United States Attorney's Office, Eastern District of Virginia, accessed July 18, 2016, https://www.justice.gov/usao-edva/release-victim-notification; "Owner of Most-Visited Illegal File-Sharing Website Charged with Criminal Copyright Infringement," The United States Attorney's Office, Eastern District of Virginia, July 20, 2016, https://www.justice.gov/usao-ndil/pr/owner-most-visited-illegal-file-sharing-website-charged-criminal-copyright-infringement.

60. For examples, see: "2017 Out-of-Cycle Review of Notorious Markets," Office of the United States Trade Representative, January 11, 2018), https://ustr.gov/sites/default/files/files/Press/Reports/2017%20Notorious%20Markets%20List%201.11.18.pdf.

61. Nigel Cory, "How Website Blocking Is Curbing Digital Piracy Without 'Breaking the Internet'" (Information Technology and Innovation Foundation, August 2018), http://www2.itif.org/2016-website-blocking.pdf.

62. Robert Atkinson, "The Internet Is Not (Fully) Open, Nor Should It Be," *Innovation Files*, August 13, 2015, http://www.innovationfiles.org/the-internet-is-not-fully-open-nor-should-it-be/.

63. "CPTPP: Chapter 8: Technical Barriers to Trade," New Zealand Ministry of Foreign Affairs and Trade, https://www.mfat.govt.nz/assets/Trans-Pacific-Partnership/Text/8.-Technical-Barriers-to-Trade-Chapter.pdf.

64. Daniel Castro and Alan McQuinn, "Unlocking Encryption: Information Security and the Rule of Law" (Information Technology and Innovation Foundation, March 14, 2016), https://itif.org/publications/2016/03/14/unlocking-encryption-information-security-and-rule-law.

65. Encryption is the act of scrambling the data, and decryption is the act of restoring the data to its original form. To encrypt or decrypt, a key is needed. Cryptography can be described as a discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and prevent its unauthorized use. A cipher (or cypher) is an algorithm that transforms meaningful data into seemingly random data, and back again, when needed. For further information on cybersecurity and trade, see: Sweden's National Board of Trade, *The Cyber Effect: The Implications of IT Security Regulation on International Trade* (Stockholm, June 2018), https://www.kommers.se/Documents/dokumentarkiv/publikationer/2018/The-Cyber-Effect.pdf.

66. Trevor Tim, "The FBI Used to Recommend Encryption. Now They Want to Ban It," *The Guardian*, March 28, 2015, https://www.theguardian.com/commentisfree/2015/mar/28/the-fbi-used-to-recommend-encryption-now-they-want-to-ban-it; Liz Gannes, "Obama: 'There's No Scenario in Which We Don't Want Really Strong Encryption'," Recode, accessed January 4, 2016, http://recode.net/2015/02/13/obama-theres-no-scenarioin-which-we-dont-want-really-strong-encryption/.

67. Castro and McQuinn, "Unlocking Encryption: Information Security and the Rule of Law." .

68. U.S. Department of Energy, "Secure Data Transfer Guidance for Industrial Control and SCADA Systems," PNNL20776, September 2011, at http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-20776.pdf.

69. Chris Jaikaran, "Encryption: Frequently Asked Questions," Congressional Research Service, September 28, 2016, https://fas.org/sgp/crs/misc/R44642.pdf.

70. "Summary of the HIPAA Security Rule," *HHS.gov*, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

71. "USMCA: Chapter 12: Sectoral Annexes," United States Trade Representative's website, https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/12_Sectoral_Annexes.pdf.

72. Kim Zetter, "Encryption Is Worldwide: Yet Another Reason Why a US Ban Makes No Sense," *Wired*, February 11, 2018, https://www.wired.com/2016/02/encryption-is-worldwide-yet-another-reason-why-a-us-ban-makes-no-sense/; and "Dutch Government Says No to 'Encryption Backdoors'," *BBC News*, January 7, 2016, https://www.bbc.com/news/technology-35251429.

73. Lisa Lambert and Jeff Mason, "Obama Backs Away From Law to Access Encrypted Information," *Reuters*, October 10, 2015, https://www.reuters.com/article/us-usa-cybersecurity-legislation/obama-backs-away-from-law-to-access-encrypted-information-idUSKCN0S40VN20151010.

74. These attempts include banning the export of certain types of encryption, undermining encryption standards, building backdoor software and hardware, asking the private sector to develop key escrow or intercept capabilities, and developing capabilities to use brute force to decrypt encrypted data. See Jay Stowsky, "Secrets or Shields to Share? New Dilemmas for Dual Use Technology Development and the Quest for Military and Commercial Advantage in the Digital Age," Berkeley Roundtable on the International Economy, February 21, 2003, http://escholarship.org/uc/item/89r4j908; Larry Greenemeier, "NSA Efforts to Evade Encryption Technology Damaged U.S. Cryptography Standard," *Scientific American*, September 18, 2013, http://www.scientificamerican.com/article/nsa-nist-encryption-scandal/; Evan Perez and Shimon Prokupecz, "First on CNN: Newly Discovered Hack Has U.S. Fearing Foreign Infiltration," *CNN*, December 19, 2015, http://www.cnn.com/2015/12/18/politics/juniper-networks-usgovernment-security-hack/; "Discovering IT Problems, Developing Solutions, Sharing Expertise," U.S. National Security Agency, October 30, 2015, https://www.nsa.gov/public_info/news_information/2015/ncsam/discovering_solving_sharing_it_solutions.shtml; Steven Levy, "Battle of the Clipper Chip," *The New York Times*, June 12, 1994, http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html.

75. Larry Greenemeier, "NSA Efforts to Evade Encryption Technology Damaged U.S. Cryptography Standard;" Joseph Menn, "NSA Says How Often, Not When, It Discloses Software Flaws," *Reuters*, March 30, 2015, http://www.reuters.com/article/us-cybersecurity-nsa-flaws-insightidUSKCN0SV2XQ20151107#QZF5OuhmEg2KCeA5.97.

76. Aaron Tan, "Apple Challenges Australia's Proposed Decryption Law," *Computer Weekly*, October 15, 2016, https://www.computerweekly.com/news/252450584/Apple-challenges-Australias-proposed-decryption-law.

77. Castro and McQuinn, "Unlocking Encryption: Information Security and the Rule of Law"; Peter Mitchell, "Canadian who sold uncrackable phones to Australian gangs jailed," *Sydney Morning Herald,* May 29, 2019, https://www.smh.com.au/world/north-america/canadian-who-sold-uncrackable-phones-to-australian-gangs-jailed-20190529-p51scy.html.

78. United Nations Department of Economic Affairs and Social Affairs Statistics Division, "New issues requiring guidance in the Central Product Classification" (New York: United Nations, May 2015), https://unstats.un.org/unsd/class/intercop/expertgroup/2015/AC289-20.PDF.

79. Shin-yi Peng, "GATS and the Over-the-Top Services: A Legal Outlook," Journal of World Trade 50, no. 1 (2016): 21-46, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2822564.

80. Nigel Cory, "Testimony Before the United States International Trade Commission on Global Digital Trade" (The Information Technology and Innovation Foundation, March 29, 2018), https://itif.org/publications/2018/03/29/testimony-united-states-international-trade-commission-global-digital-trade.

81. Van Ly, "Ministry Protects OTT Services," The Saigon Times Daily, October 25, 2016, https://www.vietnambreakingnews.com/2016/10/ministry-protects-ott-services/.

82. Anisa Menur A. Maulani, "Indonesian state-owned telco Telkom to cancel Netflix ban, following new partnership," e27, April 12, 2017, https://e27.co/indonesian-state-owned-telco-telkom-cancels-netflix-ban-20170412/.

83. Joshua New, "Why the United States Needs a National Artificial Intelligence Strategy and What It Should Look Like" (The Information Technology and Innovation Foundation, December 4, 2018), https://itif.org/publications/2018/12/04/why-united-states-needs-national-artificial-intelligence-strategy-and-what.

84. Iain Cockburn, Rebecca Henderson, and Scott Stern, The Impact of Artificial Intelligence on Innovation (Cambridge: The National Bureau of Economic Research, December 16, 2017), https://www.nber.org/chapters/c14006.pdf; Christopher Hooton and Davin Kaing. "Exploring Machine Learning's Contributions to Economic Productivity and Innovation." The International Journal of Technology, Knowledge, and Society 14 (3): 1-25. 2018. doi:10.18848/1832-3669/CGP/v14i03/1-25.

85. "CPTPP: Chapter 14: Ecommerce," New Zealand Ministry of Foreign Affairs and Trade, https://www.mfat.govt.nz/assets/Trans-Pacific-Partnership/Text/14.-Electronic-Commerce-Chapter.pdf.

86. Joshua New, "Here's What the USMCA Does for Data Innovation," *Center for Data Innovation blog*, October 5, 2018, https://www.datainnovation.org/2018/10/heres-what-the-usmca-does-for-data-innovation/.

87. Open Data Handbook, "What is Open Data?", Open Knowledge Foundation, 2012, http://opendatahandbook.org/en/what-is-open-data/.

88. James Manyika et al., "Open Data: Unlocking Innovation and Performance with Liquid Information," McKinsey Global Institute, October 2013, http://www.mckinsey.com/insights/business_technology/open_data_unlocking_innovation_and_performance_with_liquid_information.

89. Daniel Castro and Travis Korte, "Open Data in the G8: A Review of Progress on the Open Data Charter" (Center for Data Innovation, March, 2015), http://www2.datainnovation.org/2015-open-data-g8.pdf.

90. Mark Schaub, "China: Mapping the Future - Current Challenges and Forecast trends in respect of Mapping for Autonomous Vehicles," King and Wood and Mallesons website, https://www.kwm.com/en/cn/knowledge/insights/china-mapping-the-future-20180119.

91. Yan Luo, Zhijing Yu, and Nicholas Shepherd, "China Releases Draft Measures for Data Security Management," *Inside Privacy blog post,* May 28, 2019, https://www.insideprivacy.com/uncategorized/china-releases-draft-measures-for-the-administration-of-data-security/.

92. Avi Goldfarb and Daniel Trefler, "AI and International Trade," NBER Working Paper No. 24254, Issued in January 2018, https://www.nber.org/papers/w24254.

93. "Open data," Digital.govt.nz website, https://www.digital.govt.nz/standards-and-guidance/data-2/open-data/; "Declaration on Open and Transparent Government," Digital.govt.nz website, https://www.ict.govt.nz/programmes-and-initiatives/open-and-transparent-government/.

94. "Open Data Inventory (ODIN)," Open Data Watch website, https://odin.opendatawatch.com/.

95. "Open Data Impact Map," Open Data Watch website, https://opendataimpactmap.org/map.

96. "Open Data Inventory (ODIN)," Open Data Watch website, https://odin.opendatawatch.com/.

97. Daniel Castro and Travis Korte, "Open Data in the G8" (Center for Data Innovation, March 2015), https://www.datainnovation.org/2015/03/open-data-in-the-g8/.

98. "Open Government Declaration," Open Government Partnership website, https://www.opengovpartnership.org/process/joining-ogp/open-government-declaration/.

99. Nigel Cory, "How E-Labels Can Support Trade and Innovation in ICT" (The Information Technology and Innovation Foundation, September 25, 2017), https://itif.org/publications/2017/09/25/how-e-labels-can-support-trade-and-innovation-ict.

100. "Telecommunications (Labelling Notice for Customer Equipment and Customer Cabling) Instrument 2015," (Australia's Federal Register of Legislation website, accessed August 29), 2017, https://www.legislation.gov.au/Series/F2015L00190.

101. "Digital Label Guidelines," (public submission, Australian Information Industry Association (AIIA), May, 2013), https://www.aiia.com.au/documents/policy-submissions/policies-and-submissions/2013/digital_label_guidelines_aiia_comments_05_2013.pdf; and Australian Communications and Media Authority, *Proposed Changes to Labelling Arrangements-Implementation of a Consolidated Regulatory Compliance Mark and Electronic Labelling: Discussion Paper* (Canberra: Australian Communications and Media Authority, October, 2009), http://www.australianmusic.asn.au/wp-content/uploads/2014/04/ACMA.Proposal.Nov09.pdf.

102. "Overview of Certification System for Terminal Equipment in Japan," (presentation, Japan's Ministry of Internal Affairs and Communications, February, 2013), http://www.tele.soumu.go.jp/resource/j/equ/mra/pdf/24/e-06.pdf.

103. "Guideline on Certification Mark for Self-Labelling of Certified Communication Products in Malaysia," (guide, SIRIM QAS International, January, 2015), https://members.wto.org/crnattachments/2015/TBT/MYS/15_1370_00_e.pdf.

104. Stephen Ezell and Robert Atkinson, "The Middle Kingdom Galapagos Island Syndrome: The Cul-De-Sac of Chinese Technology Standards" (Information Technology and Innovation Foundation, December 2014),

https://itif.org/publications/2014/12/15/middle-kingdom-galapagos-island-syndrome-cul-de-sac-chinese-technology.

105. University of Colorado at Boulder, Institute of Behavioral Science, Research Program on Political and Economic Change, "The Costs of Complying with Foreign Product Standards for Firms in Developing Countries: An Econometric Study," (Working Paper PEC2004-0004, May 19, 2004, 7), http://www.colorado.edu/ibs/pubs/pec/pec2004-0004.pdf.

106. "USMCA: Chapter 12: Sectoral Annexes," United States Trade Representative website, https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/12_Sectoral_Annexes.pdf.

. "ISO/IEC CD 22603-1 Information Technology -- Digital representation of product information -- Part 1: General requirements," International Organization for Standardization website, https://www.iso.org/standard/73561.html.

108. "USMCA: Chapter 12: Sectoral Annexes," United States Trade Representative website

109. Institute of International Finance (IIF), *Reciprocity in Customer Data Sharing Frameworks,* (Washington, DC: IIF, July, 2018), https://www.iif.com/portals/0/Files/private/32370132_reciprocity_in_customer_data_sharing_frameworks_20170730.pdf.

110. Maurice E. Stucke and Allen P. Grunes, Big Data and Competition Policy (New York: Oxford University Press, 2016).

111. Joe Kennedy, "The Myth of Data Monopoly: Why Antitrust Concerns About Data Are Overblown," Information Technology and Innovation Foundation, March 2017, http://www2.itif.org/2017-data-competition.pdf.

112. Daniel Castro and Michael Steinberg, "Blocked: Why Some Companies Restrict Data Access to Reduce Competition and How Open APIs Can Help" (The Information Technology and Innovation Foundation, November 6, 2017), https://itif.org/publications/2017/11/06/blocked-why-some-companies-restrict-data-access-reduce-competition-and-how.

113. Castro and Steinberg, "Blocked: Why Some Companies Restrict Data Access to Reduce Competition and How Open APIs Can Help."

114. Paul Wiebusch, "Open banking: A seismic shift" (Deloitte report, 2019), https://www2.deloitte.com/content/dam/Deloitte/au/Documents/financial-services/deloitte-au-fs-open-banking-seismic-shift-180118.pdf.

115. Paul Wiebusch, "Open banking," *Deloitte article,* 2019, https://www2.deloitte.com/au/en/pages/financial-services/articles/open-banking.html#.

116. Robert Atkinson and Stephen Ezell, "Promoting European Growth, Productivity, and Competitiveness by Taking Advantage of the Next Digital Technology Wave" (The Information Technology and Innovation Foundation, March 26, 2019), http://www2.itif.org/2019-europe-digital-age.pdf?_ga=2.203147345.1307815879.1560778182-884439753.1559746026.

117. Scott Farrell, "Review into Open Banking: giving customers choice, convenience, and confidence," Australia's Department of the Treasury, https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-_For-web-1.pdf.

118. "Open Banking," Open Banking United Kingdom, https://www.openbanking.org.uk/.

119. U.S. Department of the Treasury, "Treasury Releases Report on Nonbank Financials, Fintech, and Innovation," Press Release, July 31, 2018, https://home.treasury.gov/news/press-releases/sm447; Laura Brodsky and Liz Oakes, "Data sharing and open banking," *McKinsey and Company blog,* September 2017, https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking.

120. Ibid.

121. Institute of International Finance (IIF), *Reciprocity in Customer Data Sharing Frameworks,* (Washington, DC: IIF, July, 2018), https://www.iif.com/portals/0/Files/private/32370132_reciprocity_in_customer_data_sharing_frameworks_20170730.pdf.

122. In regards to PSD2, according to the EC FinTech Action Plan, it will help to develop more coordinated approaches on standards for FinTech by Q4 2018 and will support joint efforts by market players to develop, by mid-2019, standardized application programming interfaces that are compliant with the PSD2 and GDPR: Ibid.

123. Sean Creehan and Cindy Li, "Asia's Open Banking Push," *Federal Reserve Bank of San Franciso Pacific Exchange Blog,* December 5, 2018, https://www.frbsf.org/banking/asia-program/pacific-exchange-blog/asias-open-banking-push/.

124. Ibid.

125. "API workstream," Payments NZ, https://www.paymentsnz.co.nz/our-work/payments-direction/api-workstream/.

126. Antony Peyton, "New Zealand heads to open banking," *Fintech Futures,* March 4, 2019, https://www.bankingtech.com/2019/03/new-zealand-heads-to-open-banking/; "An open mind on open banking," Reserve Bank of New Zealand, May, 2018, https://www.rbnz.govt.nz/financial-stability/financial-stability-report/fsr-may-2018/an-open-mind-on-open-banking.

127. The following sections are drawn in part from a forthcoming report Nigel Cory has prepared for the APEC Policy Support Unit called: "Fostering an Enabling Policy and Regulatory Environment in APEC for Data-Utilizing Businesses."

128. World Economic Forum (WEF), *Making Deals in Cyberspace: What's the Problem?* (Geneva: WEF, October, 2017), http://www3.weforum.org/docs/WEF_White_Paper_Making_Deals_in_Cyberspace.pdf.

129. Ibid.

130. "e-Invoicing - enabled by the NZBN," New Zealand's Ministry of Business, Innovation, and Employment, https://www.nzbn.govt.nz/using-the-nzbn/e-invoicing/; "e-Invoicing in Chile," edicom website, https://www.edicomgroup.com/en_US/solutions/einvoicing/LATAM_einvoicing/chilean_einvoicing.html.

131. Prime Minister of Australia, "Joint Statement by Prime Ministers the Rt Hon Jacinda Ardern and the Hon Scott Morrison MP," Media Release, February 22, 2019, https://www.pm.gov.au/media/joint-statement-

prime-ministers-rt-hon-jacinda-ardern-and-hon-scott-morrison-mp; Matt Goss, "Preparing for e-invoicing requirements," *bizedge,* December 7, 2018, https://bizedge.co.nz/story/preparing-for-e-invoicing-requirements.

132. United Nations Conference on Trade and Development (UNCTAD). "Cyberlaws and regulations for enhancing e-commerce: Case studies and lessons learned." Geneva: UNCTAD secretariat, January 14, 2015, https://unctad.org/meetings/en/SessionalDocuments/ciiem5d2_en.pdf.

133. Organisation for Economic Co-operation and Development (OECD) and World Trade Organization (WTO), Aid for Trade at a Glance 2017: Promoting Trade, Inclusiveness and Connectivity for Sustainable Development, 2017.

134. Article 14.5: Domestic Electronic Transactions Framework.

135. Article 14.6.1 and 2: Electronic Authentication and Electronic Signatures.

136. Making Deals in Cyberspace: What's the Problem? Geneva: World Economic Forum, October, 2017, http://www3.weforum.org/docs/WEF_White_Paper_Making_Deals_in_Cyberspace.pdf.

137. UNCITRAL has made several attempts to increase the uniformity of these legal rules by introducing model legislation, many governments choose to enact elements it likes and discard the others. https://www.weforum.org/whitepapers/making-deals-in-cyberspace-what-s-the-problem.

138. Article 14.6: Electronic Authentication and Electronic Signatures.

139. Agreement between Australia and Japan for an Economic Partnership, art. 13.5.2.

140. "Using e-signatures for international trade," American Express website, https://www.americanexpress.com/us/foreign-exchange/articles/e-signatures-for-international-trade/.

141. "eSignature Legality in Brazil," DocuSign, 2017, accessed January 31, 2019, https:// www.docusign.com/how-it-works/legality/global/brazil.

142. "ICP-Brazil," Wikipedia page, accessed January 31, 2019, https://pt.wikipedia.org/wiki/ICP-BRASIL.

143. "eSignature Legality in Brazil," DocuSign website, accessed January 31, 2019, https://www.docusign.com/how-it-works/legality/global/brazil.

144. "A global overview of electronic signatures," Adobe, https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/adobe-global-overview-of-electronic-signatures.pdf.

145. Mike Faden, "Using E-signatures for International Trade," American Express, https://www.americanexpress.com/us/foreign-exchange/articles/e-signatures-for-international-trade/.

146. Digital Agenda: new Regulation to enable cross-border electronic signatures and to get more value out of electronic identification in Digital Single Market," European Commission; http://europa.eu/rapid/press-release_IP-12-558_en.htm.

147. 2 Singapore-Australia Free Trade Agreement, art. 14.5 See, for example, Korea-Australia Free Trade Agreement, art. 15.5. Some agreements include this mandate expressed in a negative manner, see Free Trade and Economic Partnership Agreement between Japan and Switzerland, art. 78 ("Neither party shall adopt or maintain legislation…prohibit[ing] parties…from mutually determining the appropriate electronic signature methods.").

148. 5 United States-Korea Free Trade Agreement, art. 15.4; Free Trade and Economic Partnership Agreement between Japan and Switzerland, art. 78.

149. See, for example, Deep and Comprehensive Free Trade Area (DCFTA) of the EU-Ukraine Association Agreement, art. 140; EU-South Korea Free Trade Agreement, art. 7.49.

150. Free Trade Agreement between the Republic of Korea and Peru, art. 14.8

151. Additional Protocol to the Framework Agreement of the Pacific Alliance, art. 13.10.

152. These firms are known as "Authorized Provider Certification" (known by its Spanish acronym PAC).

153. The Application of HSM Technology in Electronic Invoicing. Bulverde: FutureX, accessed January 31, 2019, https://www.futurex.com/images/uploads/Case_Study-Electronic_Invoicing-Mis_e-Folios.pdf.

154. The Application of HSM Technology in Electronic Invoicing. Bulverde: FutureX, accessed January 31, 2019, https://www.futurex.com/images/uploads/Case_Study-Electronic_Invoicing-Mis_e-Folios.pdf.

155. "FIPS 140 Validation," Microsoft Windows IT Pro Center website, April 2, 2018, https://docs.microsoft.com/en-us/windows/security/threat-protection/fips-140-validation#ID0EWFAC.

156. Tiwari, Devendra, "Announcing Azure Dedicated HSM availability," Micrsoft Azure website, November 28, 2018, https://azure.microsoft.com/en-us/blog/announcing-azure-dedicated-hardware-security-module-availability/.

157. "Confidence in the trusted cloud," Microsoft Azure website, accessed January 31, 2019, https://azure.microsoft.com/en-us/overview/trusted-cloud/.