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:

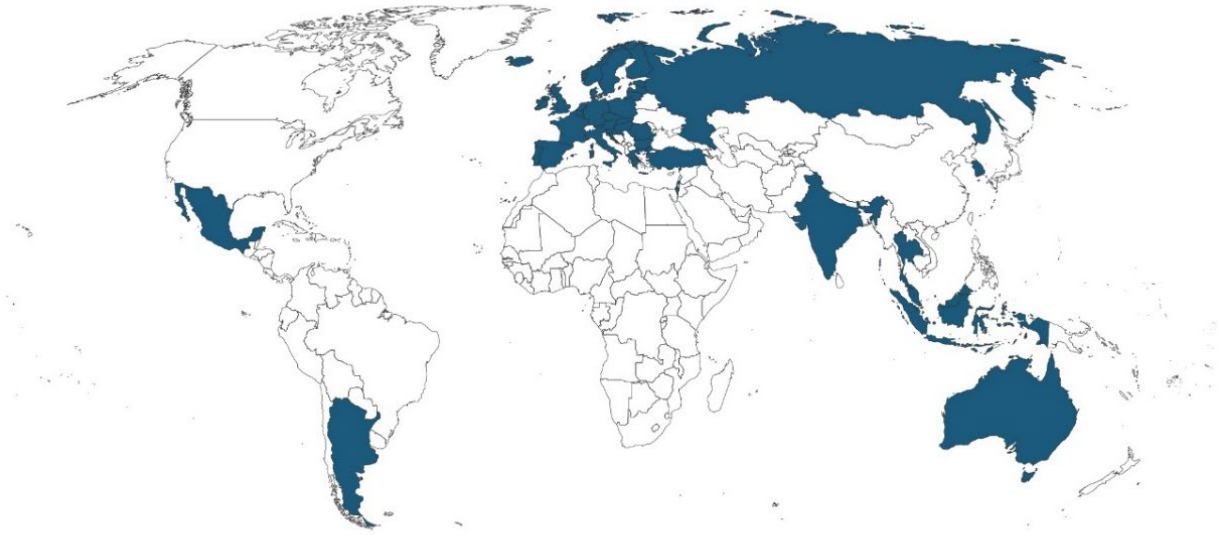
- child pornography (many countries);
- malware (e.g., Australia);[45]
- investment fraud (e.g., Australia);[46]
- online gambling (e.g., Quebec, Canada and Singapore);[47]
- pornography (e.g., India);[48]
- prostitution (e.g., India);[49]
- terrorism (e.g., the United Kingdom, Australia, France, and 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 economy for 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/.