Other Persons: Wirjo, Andre; Vásquez Callo Müller, María del Carmen; Sangaraju, Divya et al.

Book

Assessment of capacity building needs to support WTO negotiation on trade related aspects of e-commerce

Reference: (2020). Assessment of capacity building needs to support WTO negotiation on trade related aspects of e-commerce. Singapore : Asia-Pacific Economic Cooperation Secretariat. https://www.apec.org/-/media/APEC/Publications/2020/12/Assessment-of-Capacity-Building-Needs-to-Support-WTO-Negotiation/220_PSU_E-commerce_Main-Report.pdf.

Asia-Pacific
Economic Cooperation

Advancing Free Trade
for Asia-Pacific **Prosperity**

Assessment of Capacity Building Needs to Support WTO Negotiation on Trade Related Aspects of E-commerce

APEC Policy Support Unit

December 2020

Prepared by:
Andre Wirjo, María Vásquez Callo-Müller, Divya Sangaraju, Liu Jiquan Crystal and Shawn Siah
Asia-Pacific Economic Cooperation Policy Support Unit
Asia-Pacific Economic Cooperation Secretariat
35 Heng Mui Keng Terrace
Singapore 119616
Tel: (65) 6891-9600 Fax: (65) 6891-9690
Email: psugroup@apec.org Website: www.apec.org

Dr John Ure, Stacy Baird, Cheryl Tan, Gareth Tan, and Grace Gown[1]
TRPC Pte. Ltd.

Christopher Wood[2]
Washington Core

Produced for:
Committee on Trade and Investment
Asia-Pacific Economic Cooperation

APEC# 220-SE-01.20

[1] Case Studies for Focus Area B (openness and cross-border related issues); D (cybersecurity); and E (infrastructure-related aspects, including telecommunications) in Section 5.2, 5.4, and 5.5 respectively.
[2] Case Studies for Focus Area A (electronic transaction framework) and C (consumer protection and privacy issues) with the exception of the case studies for China and Chinese Taipei in Section 5.1 and 5.3 respectively.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF BOXES

EXECUTIVE SUMMARY

Background

- E-commerce presents vast opportunities for businesses and consumers. In 2019 alone, global e-commerce sales (which include both goods and services) reached highs of USD 3.5 trillion. Moreover, e-commerce growth rate continues to outperform that of global retail sales, and this is expected to accelerate in light of COVID-19.

- Although e-commerce has been driven by greater internet penetration and mobile phone usage, there are still a number of factors that could be improved to create a supportive regulatory environment where e-commerce can thrive. For instance, the outlook for greater e-commerce adoption depends ultimately on preserving the internet's open architecture, while balancing approaches to deter potential challenges and threats (e.g., cyber threats). This poses questions on how to regulate without causing internet fragmentation, which could occur with respect to the technological underpinnings of the internet, government policies and commercial aspects.

- Noting this, APEC and other international organizations have undertaken several initiatives to facilitate cross-border e-commerce. Specifically for APEC, these include the APEC Cross-border E-Commerce Facilitation Framework, the APEC Internet and Digital Economy Roadmap and the APEC Action Agenda for the Digital Economy.

- Furthermore, recognizing the importance of e-commerce for global trade, since 1998 and with the adoption of the "Declaration on Global Electronic Commerce", the WTO has hosted several discussions on trade related aspect of e-commerce. Building upon those, WTO members who accounted for 90 percent of global trade issued a joint statement in January 2019 confirming their intention to commence negotiations on global rules pertaining to e-commerce.

- This study is conducted in response to these developments, and has been designed to contribute to the ongoing process in WTO as well as the capacity building activities that may arise from it. The methodology employed comprises of two main components, namely: 1) the database component (which aims to better situate APEC economies in the wider spectrum of laws and regulations affecting e-commerce); and 2) the case study component (which intends to showcase examples of specific policies that could facilitate or affect e-commerce).

- The database component is based on a review of publicly available submissions issued by WTO members since 2018. In these submissions, WTO members explain their negotiating approach as well as the elements they believe should be included and discussed in the exploratory work and eventual agreement on e-commerce. Based on the review, the different policy issues relevant for e-commerce can be categorized into six focus areas,

namely: A (electronic transactions framework); B (openness and cross-border related issues); C (consumer protection and privacy issues); D (cybersecurity/network security); E (infrastructure-related aspects); and F (market access).

- The case study component showcases specific policies or initiatives within these focus areas that could be used to enhance the potential of e-commerce. It complements the database component and sheds more details on the motivations as well as the practicalities of APEC economies' approaches.

Insights from database of laws and regulations

Focus Area A: Electronic Transactions Framework

- As part of efforts to foster the digital economy, several APEC economies have introduced digital and digital-related strategies. In some economies, initiatives with implications on e-commerce are embedded within wider strategies. However, there have also been cases where economies have introduced standalone strategies on e-commerce.

- There has been increased recognition of electronic authentication (i.e., electronic contracts and signatures) in the APEC region. Applicable laws generally specify the requirements that must be met for an e-signature to be recognized as valid and they could vary between economies. The terms 'e-signature' and 'digital signature' are often used interchangeably, but within the laws, a distinction between simple and enhanced e-signatures/digital signatures has consistently been made.

- While many APEC economies have electronic payment (e-payment) laws and regulations, there is often no single law that regulates it. Furthermore, the interpretation of e-payments are varied across the region. To further encourage the development and adoption of newer technologies in the payment sector, some APEC economies have introduced FinTech regulatory sandboxes.

- Several APEC economies have mandated or encouraged the adoption of e-invoicing through laws and regulations, considering that they are relatively more efficient as compared to the traditional, paper-based invoicing method.

- Trade facilitation is another cog in the wheel of the e-commerce value chain given that while e-commerce transactions may be completed online, commerce involving physical goods would still have to be physically transported. In response, APEC economies have facilitated it by introducing paperless trading, blockchain technology, Authorized Economic Operator programs and single window systems.

Focus Area B: Openness and Cross-Border Issues

- Regulations on cross-border data flows establish conditions under which data exports of personal data can occur and/or are allowed. Across APEC economies, these conditions can be broadly classified as: 1) transfers based on consent, 2) transfers based on the existence of similar levels of protection and consent, and 3) transfers based on the accountability of the business operator that is transferring the data. Some economies are also part of international/regional frameworks that regulate or facilitate cross-border data transfers, including the APEC Cross-Border Privacy Rules (CBPR) System, while a few have been accorded adequacy decisions by the European Commission.

- Competition laws are being tested given new forms of collusion (e.g., via algorithms) and the wider use of data. Although most APEC economies have competition laws in place, most of them do not have specific policies for competition issues associated with online platforms. Yet, in some cases, there are initiatives to adapt competition laws specifically to the digital environment.

- APEC economies have taken different approaches toward network management practices (i.e., practices undertaken by internet services providers regarding the prioritization of certain traffic). Considering that there is an ongoing debate on the advantages and disadvantages of network management practices and network neutrality, some economies have adopted network neutrality principles/rules while others have not.

- APEC economies have varying regulations pertaining to internet intermediary liability. Most economies have a conditional liability regime (often relying on safe harbors which exempt from liability if the intermediary adopts certain policies, for instance removing content upon request). The definition of what an intermediary is also varies considerably across APEC economies.

- To better protect against unlawful or offensive content, various APEC economies have issued laws and regulations to better regulate them. These include content that threaten domestic security, misinformation and child pornography.

- Most APEC economies have either an economy-wide policy, plan or law promoting an open government data environment, or an available open data portal. This has been influenced by the membership of some economies to open data or open government international frameworks.

Focus Area C: Consumer Protection and Privacy Issues

- All APEC economies have consumer protection laws and regulations. While enacted consumer protection laws broadly cover e-commerce transactions, only a few have made

specific references to it or have legislations devoted to it. Coverage differs among APEC economies with respect to misleading, deceptive and/or fraudulent practices.

- Many APEC economies have enacted laws to deal with unsolicited commercial electronic messages or SPAM. Variations can be observed in terms of how consent is defined (i.e., express, implicit or assumed), what constitutes as SPAM, and whether the law extends beyond the economy.

- Most APEC economies have introduced laws on data privacy and protection. However, they differ in terms of what is defined as personal information. Some regulations offer extra level of protection for more sensitive data. Many APEC economies have data protection authorities, but the number and scope of responsibility vary by economy. Other aspects covered by the laws and regulations include those relating to data breach notification and appointment of data protection officers.

Focus Area D: Cybersecurity/Network Security

- Different APEC economies have cybercrime legal frameworks embedded in their criminal laws, which often penalize crimes committed using a computer, computer network or other form of ICT. Additionally, some economies have laws and regulations that are specific to cybercrime and therefore, can complement the criminal acts.

- Apart from cybercrime legislation, a number of economies have cybersecurity laws, which deal with a larger set of issues such as the protection of Critical National Information Infrastructure. Some existing cybersecurity laws also contain requirements for monitoring, preventing and handling cyber risks and threats.

- A large majority of APEC economies have developed strategies to protect themselves against cyber threats. In contrast to cybercrime and cybersecurity laws which are specific to identifying, penalizing and setting legal procedures to combat illicit acts, the content of cybersecurity strategies is overarching and can include setting goals for a determined period of time, basic principles, as well as identification of key stakeholders and their respective responsibilities.

Focus Area E: Infrastructure related aspects

- Telecommunications infrastructure plays the role of an enabler for e-commerce. The rules governing telecommunication services in the context of WTO are established in the General Agreement of Trade in Services (GATS), the GATS Annex on Telecommunications, and the WTO Telecommunications Reference Paper.

- Most APEC economies have adopted full market entry liberalization for their GATS commitments on telecommunication services. Additionally, many have made more

commitments via free trade agreements. Most economies have also adopted the Telecommunications Reference Paper with little variation in their GATS schedules.

Focus Area F: Market Access

- Access to devices such as mobile phones and computers as well as their underlying parts and components is key for e-commerce. Recognizing its importance, most APEC members have joined the WTO Information Technology Agreement, a tariff elimination agreement designed to facilitate such access.

- A few APEC economies have put in place regulations such as those requiring the use of specific encryption standards, the licensing of encryption products and/or their exports. Several economies also require the regulation of electronic and/or IT products other than those related to encryption (e.g., licensing, pre-installed with specific software). Some of these regulations could have an inadvertent impact on market access.

- For the most part, APEC economies do not tie market access to the provision of proprietary information of products (e.g., source codes, algorithms). In fact, some require parties to eliminate such conditions through trade agreements. Although this may be so, there are economies that still condition market access with the provision of proprietary information.

- While digitally-enabled trade includes goods and services which in essence are traded electronically, the e-commerce value chain is also supported by another range of services that make the value chain to function properly and efficiently. These include transport/logistics, computer related and professional services. Most or all APEC economies have made commitments in their GATS schedules regarding these services, with additional commitments being made through trade agreements as well. However, there continues to be variation in the extent of liberalization at the MFN level between economies.

Insights from case studies

Focus Area	Economies covered	Main topics
***A:* Electronic transaction frameworks**	Australia[2]	E-payment (New Payment Platform)
	China[1]	E-Commerce Law
	Chinese Taipei[1]	Electronic Signatures Law
	Thailand[2]	E-payment (PromptPay)
***B:* Openness and cross-border related issues**	Australia[3]	Data Portability (Consumer Data Right) Open Banking
	The Philippines[3]	IPR enforcement ISP liability
	Singapore[3]	Cross-border data flows
***C:* Consumer protection and privacy issues**	China[1]	Regulation for Protecting Children's Personal Information Internet Courts
	Japan[2]	Online Dispute Resolution (Cross-border)
	Mexico[2]	Online Dispute Resolution (Concilianet)
***D:* Cybersecurity/ network security**	Chile[3]	Cybersecurity strategy
	Japan[3]	Cybersecurity laws and capacity building
	The United States[3]	Stakeholder involvement in cybersecurity policy IoT security
***E:* Infrastructure-related aspects, including telecommunications**	Korea[3]	Universal broadband access
	Mexico[3]	Promotion of competition in telecommunications Expansion of broadband access
	Chinese Taipei[3]	International telecommunications Connectivity Universal broadband access

Note: 1 – contributed by the economy and PSU; 2 – contributed by Washington Core; 3 – contributed by TRPC.
Source: Compilations by PSU.

Focus Area A: Electronic Transactions Framework

Case studies under this section cover four economies and consider three aspects: e-payments, electronic signatures and e-commerce laws. Specifically:

- *Australia*, one of the most mature e-payments markets in APEC, launched a New Payments Platform in 2014 seeking to modernize e-payment systems. Australia's case

highlights the value of educational outreach to raise awareness and encourage adoption of e-payments.

- *Thailand's* PromptPay hopes to improve efficiency and enable more people to participate in electronic transactions. This case study shows the importance of international engagements and adoption of international standards in promoting platform interoperability.

- *China*'s E-Commerce Law provides insights on how the economy sets out to establish a framework for electronic transactions regarding legal rights and obligations of online businesses vis-à-vis their offline counterparts and the recognition of e-contracts.

- *Chinese Taipei*'s Electronic Signatures Law underscores the value of providing legal recognition to electronic records and signatures, as well as key insights derived from the development process of the law, including the importance of involving multiple stakeholders and balancing their interests.

Focus Area B: Openness and Cross-Border Issues

Case studies under this section cover three economies and consider five aspects: data portability, cross border data flows, IPR enforcement, ISP liability, and open banking. Specifically:

- *Australia's* Consumer Data Right (CDR) exemplifies the value of data portability as a means to increase data sharing, promote interoperability, customer mobility and ultimately boost competition in the e-commerce market. The CDR case study highlights the value of early industry feedback and leveraging international best practices in order to help reduce compliance costs for implementing organizations. The case study also sheds light into the implementation of the CDR in Australia's open banking.

- *Singapore* has adopted different measures to enable cross-border data flows. These include the adoption of and use of DPTM, CBPR and ISO 27001 certifications. The case study exemplifies the value of privacy certification in signaling data protection adequacy.

- *The Philippines*' Intellectual Property Office of the Philippines (IPOPHL) has leaned towards existing international practices when setting new rules to combat online IPRs infringement and it is seeking to boost enforcement by proposing, among others, that e-commerce vendors be identified through their business registration numbers. This case study highlights the importance of cross-agency collaboration and public-private cooperation.

Focus Area C: Consumer Protection and Privacy Issues

Case studies under this section cover three economies and consider two aspects: online dispute resolution (ODR) and data protection. Specifically:

- *China*'s Regulation for Protecting Children's Personal Information aims to provide more detailed regulations to better protect children's personal data and include some key elements such as requiring companies and platforms to receive consent from parent/guardian prior to collecting children's information; additional legal liabilities beyond those which are pecuniary in nature; and encouraging self-regulation by the industry.

- *China*'s Internet Courts are established to provide an avenue to resolve e-commerce disputes and provides learnings on how technology can be better integrated into the daily functioning of the judiciary so as to increase efficiency of proceedings. It also provides insights on how technology can be adopted without compromising on the courts' ability to provide impartial justice; and how the courts have continued to evolve across various metrics.

- *Mexico*'s Concilianet was established as a pilot project in 2008 to test whether consumer conflict resolution processes could be migrated online using ICT. This case study showcases how an online dispute resolution mechanism can increase access to consumer justice, while at the same time, identifies its current limitations.

- *Japan* plans to establish a yet-to-be named cross-border ODR mechanism to complement the existing options which have been deemed as insufficient to address the growing number of transaction issues. This case study illustrates the Japanese government's efforts towards realizing this objective and the progress to date.

Focus Area D: Cybersecurity/Network Security

Case studies under this section cover three economies and consider three aspects: the establishment of a cybersecurity strategy, adoption of specific cybersecurity laws and related capacity building activities, and the role of the private sector in cybersecurity. Specifically:

- *Chile*'s Cybersecurity strategy accelerated after a highly publicized breach to Banco de Chile in 2018. Since then, Chile has enlisted the expertise of the private sector to formulate and implement over-arching plans. This case study exemplifies how the private sector can contribute to the ability of an economy to address cybersecurity.

- *Japan* has taken an aggressive approach to rapidly improve the economy's cybersecurity. This includes the development of cybersecurity legal framework, spurred by the need to fill gaps in the computer crime laws or criminal code and consolidate legal authorities. Japan's case study exemplifies the importance of establishing

appropriate cybersecurity laws, cooperation frameworks and strategy leadership among stakeholders, followed by addressing capacity building and cultural issues.

- *The United States* has employed a multi-pronged approach to cybersecurity which involves the private sector closely, including through the establishment of Computer Emergency Response Teams (CERTs), the development of standards-based NIST Cybersecurity Framework for critical infrastructure and the conduct of biannual 'Cyberstorm' cybersecurity exercises. The advent of new paradigms of doing things (such as remote working) and the Internet of Things (IoT) have further changed and complicated the cybersecurity threat landscape. The United States' case studies showcase the importance of collaborating with and receiving support from the private sector and encouraging IoT safety and security by design.

Focus Area E: Infrastructure related aspects

Case studies under this section cover three economies and consider three aspects: universal broadband access, competition in the telecommunications sector and connectivity. Specifically:

- *Korea* views the provision of universal access to internet services as a way to close the digital divide. This case study showcases how Korea combines consistent long-term planning and carefully calibrated policies, including those facilitating the use of TV white space (TVWS) and cloud computing to achieve this objective.

- *Mexico* recognizes that improving broadband coverage and internet usage are essential ingredients for success in the digital economy. This case study illustrates Mexico's efforts in achieving universal access and closing the digital divide, which includes establishing independent regulators and ensuring competition, among others by and addressing interconnection charges and adopting measures to address connectivity in remote areas.

- *Chinese Taipei* noted that both strong international telecoms connectivity and domestic universal broadband access are critical elements to its economic growth. This case study highlights the reforms undertaken by Chinese Taipei, which include the establishment of an independent regulator, the abolishment of interconnection charges and the launch of the Cloud Computing Application and Development Project.

Final remarks

- While this report has found that there are variations in the state of economies' laws, regulations and initiatives across all focus areas, it has also found that there are common baselines which capacity building activities could focus on. In addition, this report provides information on subject-matter case studies showcasing innovative approaches

undertaken by different economies, which can better inform efforts to fine tune e-commerce related policies.

- Building upon this report findings across all six focus areas and the case study component, the capacity building activities that APEC can consider undertaking could generally benefit two groups of economies, namely: 1) economies that do not yet have the necessary laws, regulations and initiatives pertaining to specific elements/aspects to develop one (e.g., e-invoicing, competition policies related to online platforms, cybersecurity laws); and 2) economies that already have existing laws, regulations and initiatives so that they can fine-tune them to better facilitate e-commerce.

- Furthermore, in line with the public proposals for WTO negotiations on e-commerce reviewed under this report, possible capacity building activities across all six focus areas can include: 1) encouraging the adoption of international standards, practices, guidelines and recommendations in economies' laws and regulations; 2) improving mutual recognition and interoperability among the laws, regulations and initiatives; 3) strengthening international cooperation with regards to specific aspects of e-commerce; 4) instituting new approaches to regulations, including the use of technology to facilitate process; and 5) ensuring that laws, regulations and initiatives are practical, reasonable and can be operationalized efficiently.

KEY ABBREVIATIONS

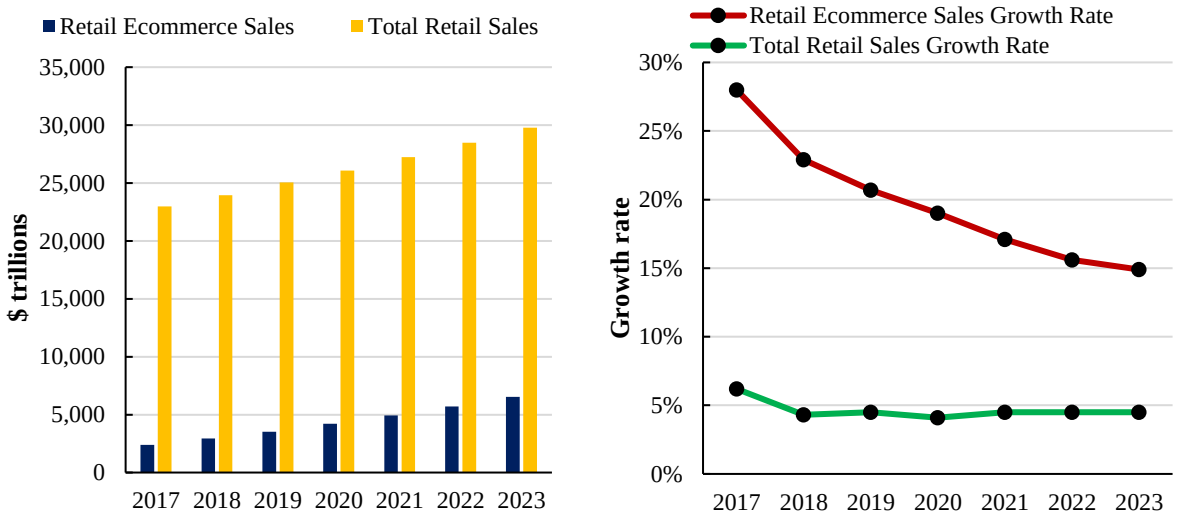
AEO	Authorized Economic Operator
ASEAN	Association of Southeast Asian Nations
CBPR	APEC Cross-Border Privacy Rules
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership
DESG	APEC Digital Economy Steering Group
EC	APEC Economic Committee
FTA	Free Trade Agreement
IP	Internet Protocol
ISP	Internet Service Provider
ITU	International Telecommunication Union
MFN	Most-Favored-Nation
MSME	Micro, Small and Medium Enterprises
OECD	Organisation for Economic Co-operation and Development
PSU	APEC Policy Support Unit
PTA	Preferential Trade Agreement
SCFAP	Supply-Chain Connectivity Framework Action Plan
STRI	OECD Services Trade Restrictiveness Index
TRIPS	Trade-Related Aspects of Intellectual Property
UNCITRAL	United Nations Commission on International Trade Law
UNCTAD	United Nations Conference on Trade and Development
UNESCAP	United Nations Economic and Social Commission for Asia and the Pacific
UPU	United Postal Union
WCO	World Customs Organization
WCT	WIPO Copyright Treaty
WIPO	World Intellectual Property Organization
WTO	World Trade Organization
WWW	World Wide Web

1 INTRODUCTION

1.1 OVERVIEW OF E-COMMERCE

In 2019, global e-commerce sales (which includes both goods and services) was estimated to reach highs of USD3.5 trillion and accounted for almost 14.1 percent of total retail sales (Figure 1.1). Although as a proportion of global retail sales, the size of e-commerce remained relatively small in comparison to other forms of sales (e.g., via supermarkets, convenience stores, bookshops and other retail shops), its growth rate continues to outperform that of global retail sales, which has hovered at approximately 5 percent. Market research firms such as eMarketer have predicted the growth of e-commerce to remain considerably higher than that of global retail sales.

Figure 1.1: Global e-commerce market sales value and growth rates



Note: "Total Retail Sales" excludes travel and event tickets, payments such as bill pay, taxes or money transfer, food services and drinking place sales, gambling and other vice good sales; "Retail electronic commerce sales" includes products or services ordered using the internet via any device, regardless of the method of payment or fulfilment; excludes travel and event tickets.
Source: eMarketer, 'Global Ecommerce 2019', 27 June 2019, https://www.emarketer.com/content/global-ecommerce-2019.

While e-commerce has been traditionally associated with the sale of goods via online channels, it is more than that on many levels. From the perspective of definition, for example, the WTO has defined it as "production, distribution, marketing, sale or delivery of goods and services by electronic means".[3] Similarly, the OECD defines it as "the sale or purchase of goods or services, conducted over computer networks by methods specifically designed for the purpose of receiving or placing of orders."[4] Hence, apart from being an end product in itself, services also play a critical role in ensuring the smooth functioning of the e-commerce value chain as they are often needed to complete the transactions and ensure product delivery among others (e.g.,

[3] WTO, 'World Trade Organization – Electronic Commerce', Last accessed May 26, 2020, https://www.wto.org/english/thewto_e/minist_e/mc11_e/briefing_notes_e/bfecom_e.htm.
[4] OECD Statistics Directorate. "Glossary of Statistical Terms - Electronic Commerce." Last updated 2013. Last accessed May 26, 2020. https://stats.oecd.org/glossary/detail.asp?ID=4721.

payment and logistics services). Indeed, despite the focus on physical goods for the purpose of its Framework of Standards, WCO recognizes the important role of services by characterizing cross-border e-commerce as involving online ordering, sale, communication and payment; as well as cross-border transactions/shipments.[5]

Box 1.1: Examples of e-commerce events around the world

E-commerce has gained widespread popularity around the world with several shopping festivals being organized around it. These festivals have helped promote the online business model and further strengthened e-commerce as a viable sales channel. Some examples of these key events within the Asia-Pacific region are highlighted below.

Singles Day

On 11 November 2019, or 'Singles Day', within just 24 hours, sales of RMB268 billion (USD38 billion) were recorded. In fact, USD1 billion worth of goods were sold in the first 68 seconds while USD12 billion was logged in the first hour. More than 200,000 brands participated in the event, 22,000 of which were international brands from 78 economies. While it was started by Alibaba, many other e-commerce platforms (including JD.com, Shopee and Zalora) and in some cases, brick-and-mortar shops have joined in the festivities through their own sales campaigns and promotions.

Cyber Monday

To better compete with brick-and-mortar firms that benefit disproportionately from shopping festivals like 'Black Friday', online retailers began 'Cyber Monday'. On this day, e-commerce firms offer huge discounts to their consumers. Given the growth of the e-commerce market and the use of online sales channels by brick-and-mortar firms, it is estimated that revenue and sales from 'Cyber Monday' now exceed those of 'Black Friday'. In fact, Adobe Analytics estimated that consumers had spent USD5 billion more on the former than on the latter in 2019. Apart from the increased dominance of online retailers, it is interesting to note that buyers are purchasing both higher volume of products, and higher-priced products, underscoring the increased confidence that consumers have with online shopping.

Amazon Prime Day

While constrained largely to the Amazon platform, this festival raked in approximately USD7 billion in 2019, which is considerably higher than its revenue in 2015 at USD0.9 billion. The festival sold more than 175 million products, both physical goods and digital products (e.g., digital books and music) over 2 days and across 18 different economies. Specifically for the large retailers, it was indicated that they were able to increase their online

[5] World Customs Organization. 'Cross-Border E-Commerce Framework of Standards', Last accessed July 24, 2020. http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/activities-and-programmes/ecommerce/wco-framework-of-standards-on-crossborder-ecommerce_en.pdf?db=web.

sales by 68 percent during the festival. Amazon also indicated that it managed to increase membership sign-ups during the first two Prime Days in 2019, noting that it now has more than a hundred million paying members worldwide.

Sources:

- Alibaba Group, 'Alibaba Group Generated US$12 Billion of GMV in the First Hour of the 2019 11.11 Global Shopping Festival', Last updated 2019, Last accessed June 23, 2020, https://www.alibabagroup.com/en/news/article?news=p191111
- Kate Gibson, 'Singles Day 2019's Record Sales Make Black Friday Look Like a Church Bazaar', CBS News, Last updated 2019, Last accessed June 23, 2020, https://www.cbsnews.com/news/singles-day-2019-alibaba-sales-break-records-on-24-hour-shopping-holiday/
- Sergei Klebnikov, 'Alibaba's 11/11 Singles' Day By The Numbers: A Record $38 Billion Haul', Forbes, Last updated 2019, Last accessed June 23, 2020, https://www.forbes.com/sites/sergeiklebnikov/2019/11/11/alibabas-1111-singles-day-by-the-numbers-a-record-38-billion-haul/#6ccc40212772
- Lucas, Amelia. 'Cyber Monday Online Sales Hit Record $9.4 Billion, Boosted by Late-Night Spending Spree, Adobe Says', Last updated 2019, Last accessed June 23, 2020, https://www.cnbc.com/2019/12/03/cyber-monday-online-sales-hit-record-9point4-billion-adobe-says.html
- Ali, Fareeha, Lauren Freedman, and Stephanie Crets, 'Amazon Prime Day Sales Number 2019 % (Including Charts!)', Digital Commerce 360, Last updated 2019, Last accessed June 23, 2020, https://www.digitalcommerce360.com/article/amazon-prime-day-data/
- Thomas, Lauren, Amazon Says This Year's Prime Day Surpassed Black Friday and Cyber Monday Combined, CNBC, CNBC, Last updated 2019, Last accessed June 23, 2020, https://www.cnbc.com/2019/07/17/amazon-announces-prime-day-2019-results.html

The rapid growth in internet penetration and mobile usage has been among the main driving forces behind the growth of e-commerce. In the APEC region, 60 percent of the region's population was connected to the internet, while the mobile subscription rate was approximately 120 percent in 2017.[6] Additionally, new tools such as e-payments and e-wallets have expanded the payment options available to both buyers and sellers, hence further facilitating e-commerce. With continuous advancements and the adoption of technologies such as 5G,[7] a more stable internet at unprecedented speeds is expected, with e-commerce likely to continue breaking new barriers.

Box 1.2: The importance of digital solutions amid COVID-19

The COVID-19 pandemic is a health and economic crisis of unprecedented proportions. By mid-June 2020, about 7 million people have been infected and more than 400,000 lives have been lost despite aggressive containment measures. Even in the optimistic scenario where a partial economic recovery begins in the second half of 2020, the APEC region is expected to contract by 3.7 percent, leading to an output loss of USD 2.9 trillion and some of the highest unemployment rates reported in decades.

[6] APEC Policy Support Unit, 'APEC in Charts 2019' (Singapore: APEC, December 2019), Last accessed June 23, 2020, https://www.apec.org/Publications/2019/12/APEC-in-Charts-2019.

[7] According to a report by the GSM Association (https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/03/GSMA_MobileEconomy2020_Global.pdf), 5G networks will overtake 2G connections by 2023 and 3G by 2025.

With economies putting in place containment measures that are likely to persist for some time, the importance of digital solutions including e-commerce have come to the fore. Indeed, the onset of the COVID-19 pandemic has hastened the migration of consumer spending from brick-and-mortar stores to online platforms for groceries and meals among others. Many businesses too have adopted e-commerce as an alternative channel to replace sales lost through the traditional ones.

According to preliminary data compiled from various APEC economies, the volume of e-commerce transactions has increased precipitously amid the containment measures. As a case in point, year-on-year revenue growth of retailers in the United States was up 68 percent as of mid-April 2020, on the back of record-breaking 49 percent revenue growth recorded in January 2020. In Singapore, 37 percent of consumers surveyed indicated a general increase in their e-commerce engagement, and nearly 76 percent have indicated that they will be turning to e-commerce for purchases previously made in physical stores, even after the COVID-19 pandemic is eventually brought under control.

The benefits of digital solutions also go beyond helping with daily household needs. Online communications platforms such as Zoom and Tencent Meeting have become an essential component in remote working arrangements as well as for schools providing distance learning. Big data and tracking apps are used to monitor crowd level and undertake contact-tracing activities, hence allowing for timely data updates. Online consultations with medical practitioners are helping to ease the burden on healthcare systems. Online banking and financial technology applications are helping to address the liquidity crisis among MSMEs, especially when lockdown requirements have made it challenging to physically visit financial institutions.

While digitalization has been an ongoing process, it has certainly been accelerated by the pandemic. This calls for economies to re-double their efforts pertaining to the digital economy, including at the ongoing WTO negotiations on e-commerce.

Sources:

- Hernando, RC and EA San Andres, 'APEC, APEC in the Epicentre of COVID-19', Last accessed June 23, 2020, https://www.apec.org/Publications/2020/04/APEC-in-the-Epicentre-of-COVID-19
- Hernando, RC, 'APEC, APEC Regional Trends Analysis, July 2020 Update: Deeper Contraction Calls for Decisive Action', Last accessed August 10, 2020, https://www.apec.org/Publications/2020/07/APEC-Regional-Trends-Analysis-July-2020-Update
- Forbes Enterprise & Cloud, 'How COVID-19 is Transforming E-Commerce', Last accessed June 23, 2020, https://www.forbes.com/sites/louiscolumbus/2020/04/28/how-covid-19-is-transforming-e-commerce/#3bf813ed3544
- Nielsen, 'COVID-19: New norm emerging in Singaporean consumers' behaviour', Last accessed June 23, 2020, https://www.nielsen.com/us/en/insights/article/2020/key-consumer-behavior-thresholds-identified-as-the-coronavirus-outbreak-evolves/

E-commerce can involve various combinations of sellers and buyers (Table 1.1:). Business-to-business (B2B) and business-to-consumer (B2C) are the two major models, accounting for the

largest market share of e-commerce.[8] Other models include consumer-to-consumer (C2C), consumer-to-business (C2B) and business-to-government (B2G). Besides these models, e-commerce can be further categorized into either domestic or cross-border transactions. As the names imply, domestic e-commerce is when both seller and buyer are located within the same economy, while cross-border refers to when seller and buyer are located in different economies.

Table 1.1: Major e-commerce models

Model	Description	Examples
Business to Business (B2B)	The sale of goods and services between two businesses	Wholesale, bulk commodities, business services e.g., Alibaba.com, Amazon Web Services, Microsoft Teams
Business to Consumer (B2C)	Businesses selling directly to consumers	Retail e.g., Amazon, Lazada, Taobao, Mercadolibre, iTunes, Kindle, Skype, Whatsapp, Spotify, Netflix
Consumer to Consumer (C2C)	Consumers selling directly to other consumers	Second-hand, auction websites, "sharing economy" e.g., eBay, Taobao, Carousell, Airbnb
Consumer to Business (C2B)	Consumers selling directly to businesses	Freelance, local artisan e.g., UpWork, Freelancer, Shutterstock, Fiverr
Business to Government (B2G)	Public procurement from businesses	E-procurement portal e.g., GeBIZ
Government to Consumer (G2C)	Governments offer products and services to consumers	E-government websites where the public can apply for online ID, pay taxes, and purchase e-food stamps

Source: APEC Policy Support Unit (PSU) compilations; APEC Business Advisory Council and University of Southern California, 'Driving Economic Growth Through Cross-Border E-Commerce in APEC: Empowering MSMEs and Eliminating Barriers', Last updated June 23, 2020, https://ncapec.org/docs/ABAC Documents/USC Marshall ABAC 2015 MSMEs.pdf.

CHALLENGES IN LEVERAGING E-COMMERCE

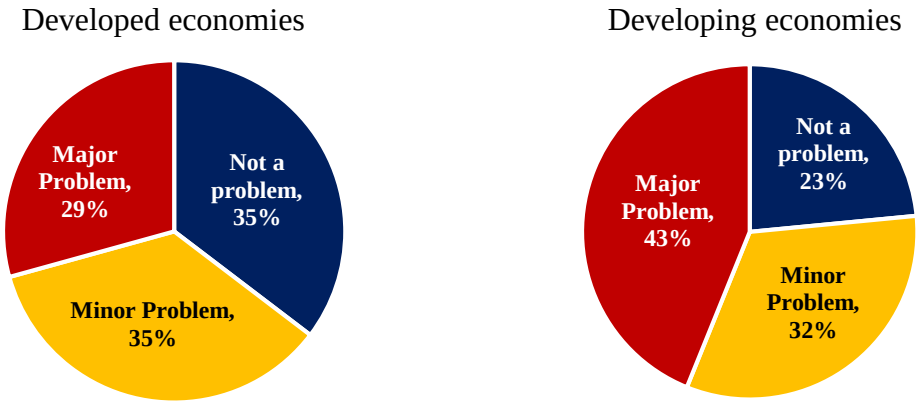
Although e-commerce presents huge opportunities to both businesses and consumers, its potential is not a given and leveraging e-commerce is not a straightforward endeavor. As with other sales/transaction channels, a supportive regulatory environment is one of the basic requirements for e-commerce to thrive. Available indicators showed that while improvements have been made to the regulatory environment pertaining to e-commerce, there is still much to be done. For instance, the United Nations Conference on Trade and Development (UNCTAD)

[8] United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP) and Asian Development Bank (ADB), 'Embracing the E-commerce Revolution in Asia and the Pacific', Last updated 2018, Last accessed June 23, 2020, https://www.unescap.org/sites/default/files/embracing-e-commerce-revolution.pdf.

B2C E-commerce index[9] - which evaluates an economy's preparedness to support online shopping - indicates that although the global score had improved from 47 to 57 between 2015 and 2019, it is arguably still low considering that the maximum score is 100. Specifically for the APEC region, while the score is relatively higher compared to the global average in 2019 (75 versus 57), there is significant variation in score among member economies (ranging from 47.5 to 95.1).

Complementing the UNCTAD index is a 2015 survey conducted by the APEC Business Advisory Council (ABAC) for all member economies. More than half of all respondents from developed and developing economies found payment issues to be a problem that affected cross-border e-commerce (Figure 1.2).

Figure 1.2: APEC MSME survey on payment issues affecting cross-border e-commerce

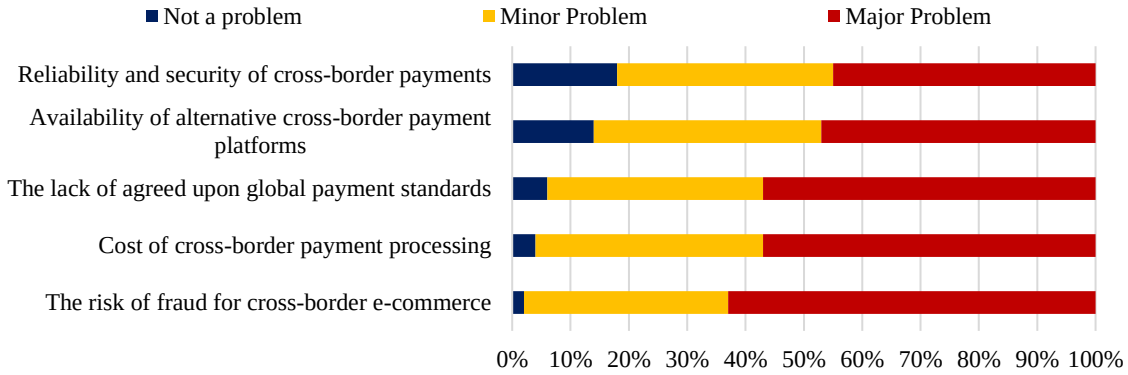


Source: APEC PSU calculations; APEC Business Advisory Council and University of Southern California, 'Driving Economic Growth Through Cross-Border E-Commerce in APEC: Empowering MSMEs and Eliminating Barriers', 2015, https://ncapec.org/docs/ABAC Documents/USC Marshall ABAC 2015 MSMEs.pdf.

Among the impediments posed by payments include the risk of fraud for cross-border e-commerce, cost of processing cross-border payment and lack of agreed global payment standards (Figure 1.3).

[9] The UNCTAD E-commerce index measures an economy's preparedness to support online shopping. The index consists of four indicators: (1) account ownership at a financial institution of with a mobile money service provider; (2) individuals using the internet; (3) postal reliability index; and (4) secure internet servers.

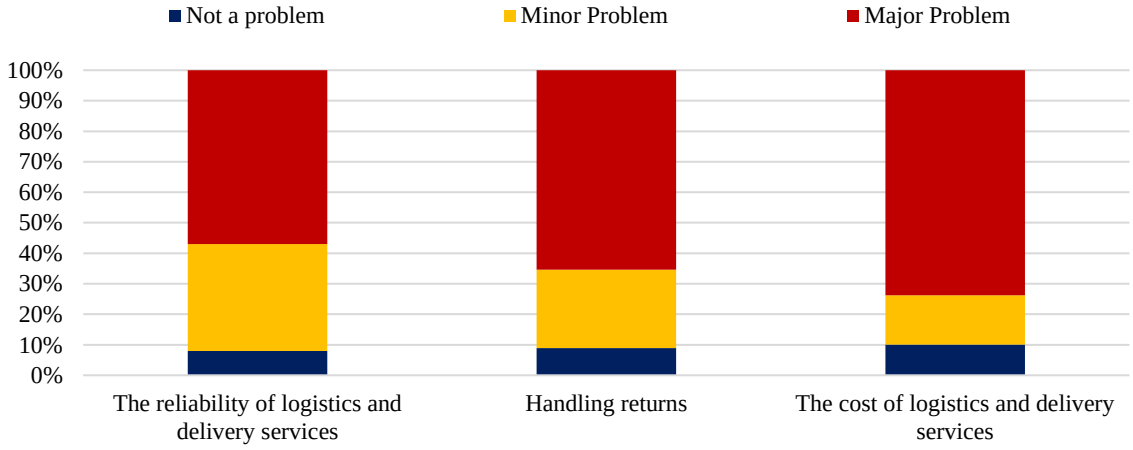
Figure 1.3: APEC MSME survey on the impediments within payments that affect cross-border e-commerce



Source: APEC PSU calculations; APEC Business Advisory Council and University of Southern California, 'Driving Economic Growth Through Cross-Border E-Commerce in APEC: Empowering MSMEs and Eliminating Barriers', Last updated 2015, Last accessed June 23, 2020, https://ncapec.org/docs/ABAC Documents/USC Marshall ABAC 2015 MSMEs.pdf.

Survey respondents also indicated that issues in logistics and delivery services such as those pertaining to cost, reliability and handling of returns have negative implications on cross-border e-commerce (Figure 1.4).

Figure 1.4: APEC MSME survey on the impediments within logistic that affect cross-border e-commerce



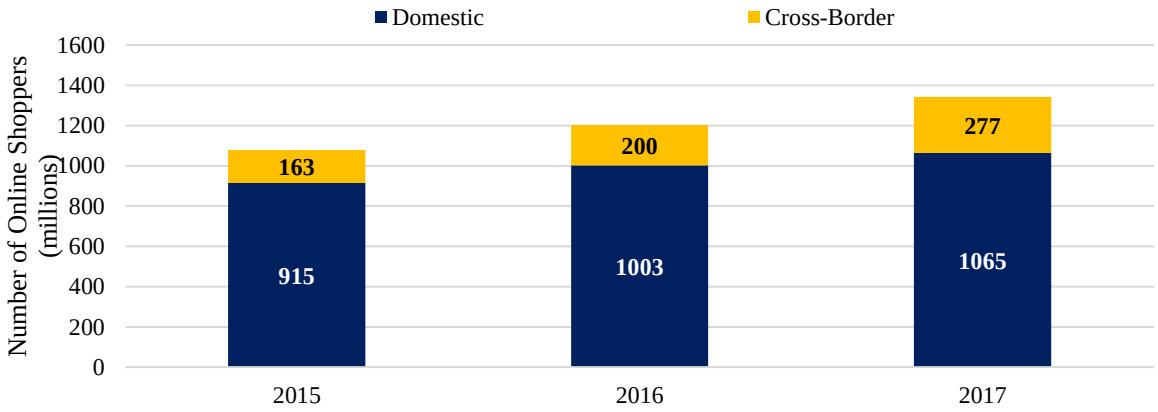
Source: APEC PSU calculations; APEC Business Advisory Council and University of Southern California, 'Driving Economic Growth Through Cross-Border E-Commerce in APEC: Empowering MSMEs and Eliminating Barriers', Last updated 2015, Last accessed June 23, 2020, https://ncapec.org/docs/ABAC Documents/USC Marshall ABAC 2015 MSMEs.pdf.

A study conducted by PSU in 2017, which involved focus group discussions and interviews with major stakeholders in e-commerce in five economies (e.g., MSMEs, marketplace platform operators, payment providers, logistics providers and relevant government agencies), made similar findings. Besides identifying the need to develop robust e-commerce ecosystem which includes enhancing the provision of payment and logistics services, it also highlighted the importance of continuing efforts towards improving the business environment and enhancing customs rules/regulations as well as clearance process among others.[10]

[10] Gloria O. Pasadilla et al, 'Promoting E-commerce to Globalize MSMEs' (Singapore: APEC, October 2017), https://www.apec.org/Publications/2017/11/Promoting-E-commerce-to-Globalize-MSMEs.

An indication that non-supportive regulatory environment and/or differences in cross-border regulatory environment between economies may act as an impediment to e-commerce is the observation by UNCTAD that despite the year-on-year growth of cross-border e-commerce, as inferred from the number of online shoppers engaged in it, majority of e-commerce transactions are still domestic in nature (Figure 1.5).[11,12] Indeed, the share of global online shoppers engaged in cross-border e-commerce was only 20.6 percent in 2017. In contrast, the share of those engaged in domestic e-commerce was about 79.4 percent.

Figure 1.5: Consumers engaged in domestic and cross-border e-commerce



Source: UNCTAD, 'Global E-Commerce Sales Surged to $29 Trillion' (Geneva: UNCTAD, March 2019), Last accessed June 23, 2020, https://unctad.org/en/pages/PressRelease.aspx?OriginalVersionID=505.

The implications of non-supportive regulatory environment on e-commerce could also be observed from the perspective of sellers, specifically in how firms of different sizes have benefitted from e-commerce. For example, while the percentage of e-commerce in the total turnover of firms based in OECD economies has collectively increased from 13.4 percent in 2008 to 18.8 percent in 2017, the percentage of large firms has been relatively higher than of small firms (24.0 versus 8.8 percent).[13] In the APEC region, a survey conducted by the SME Corporation Malaysia in the third quarter of 2016 estimated that less than 26 percent of SMEs were selling products or services online. Another survey conducted in Russia in 2015 showed that only approximately 1 percent of SMEs were involved in e-commerce.[14] In Chinese Taipei, although the economy has 1.3 million MSMEs, less than 36,600 have registered online stores with PChome store, the biggest e-commerce platform in the economy.[15] A recent report by

[11] UNCTAD, 'Global E-Commerce Sales Surged to $29 Trillion' (Geneva: UNCTAD, March 2019), Last accessed June 23, 2020, https://unctad.org/en/pages/PressRelease.aspx?OriginalVersionID=505.

[12] Non-supportive regulatory environment may have implications on domestic e-commerce as well. For example, everything else equal, the vibrancy of domestic e-commerce in an economy with less supportive regulatory environment may be lower when compared to another economy with more supportive regulatory environment.

[13] OECD, 'Unpacking E-commerce: Business Models, Trends and Policies' (Paris: OECD, 2019), Last accessed June 23, 2020, https://www.oecd-ilibrary.org/science-and-technology/unpacking-e-commerce_23561431-en.

[14] UNIDO and Shanghai Academy of Social Sciences, 'E-commerce Development Report of the Small and Medium Sized Enterprises of BRICS Countries' (July 2018), Last accessed June 23, 2020, https://www.unido.org/sites/default/files/files/2018-07/E-commerce%20Development%20Report%20%28SASS%29_09072018.pdf.

[15] Gloria O. Pasadilla and Andre Wirjo, 'Globalization, Inclusion, and E-Commerce: APEC Agenda for SMEs' (Singapore:

Bain & Company showed that the average adoption rate of online retail among MSMEs in ASEAN members is 34 percent, with great divergence across economies (e.g., 14 percent in Laos and 50 percent in Singapore).[16]

While it should be acknowledged that an improved business regulatory environment is vital for firm operations across all sizes and not only MSMEs, these statistics are not surprising considering that literature has shown the burden of the regulatory environment having a greater impact on MSMEs than large enterprises. For example, OECD (2001) noted that on average, MSMEs bore over 5 times the administrative costs per employee as compared to larger companies and found that a reduction in business regulations resulted in an extensive fall in the fixed costs imposed on MSMEs, thereby levelling the playing field in the market.[17] In another report by the OECD, MSMEs were found to usually lack the ability to navigate uncertainties in the regulatory environment, and often have to allocate a higher proportion of resources to administrative functions such as resolving disputes.[18] Tackling these would require policymakers to combine efforts to further streamline regulations for all firms and at the same time, explore mechanisms to support MSMEs in compliance, such as regulatory tiering.[19]

1.2 E-COMMERCE RELATED INITIATIVES BY APEC AND OTHER INTERNATIONAL ORGANIZATIONS

Noting the value of having in place a supportive regulatory environment for e-commerce, APEC and other international organizations such as the United Postal Union (UPU), the United Nations Conference on Trade and Development (UNCTAD), the World Trade Organization (WTO), the World Customs Organization (WCO) and the Organisation for Economic Cooperation and Development (OECD) have undertaken several initiatives to facilitate e-commerce. Table 1.2 below provides a non-exhaustive list of international organizations and related initiatives.[20]

APEC, February 2018), Last accessed June 23, 2020, https://www.apec.org/Publications/2018/02/Globalization-Inclusion-and-E-Commerce---APEC-Agenda-for-SMEs.

[16] Bain & Company, 'Advancing Towards ASEAN Digital Integration', Last updated 2018. Last accessed June 23, 2020, http://cdn.seagroup.com/webmain/static/resource/seagroup/mediaresource/research/Advancing%20Towards%20ASEAN%20Digital%20Integration%20Final%20-%20compressed.pdf.

[17] OECD, 'Businesses' Views on Red Tape: Administrative and Regulatory Burdens on Small and Medium-Sized Enterprises' (Paris: OECD, 2001), Last accessed June 23, 2020, http://www.oecd.org/newsroom/oecdreportcataloguessmallfirmsgripesaboutredtape.htm.

[18] OECD, 'Small, Medium, Strong. Trends in SME Performance and Business Conditions' (Paris: OECD, 2017), Last accessed June 23, 2020, https://read.oecd-ilibrary.org/industry-and-services/small-medium-strong-trends-in-sme-performance-and-business-conditions_9789264275683-en#page4.

[19] Ben Shepherd, Olivier Cattaneo and Charles Tsai, 'Regulatory Reform Case Studies on Improving the Business Environment for Small and Medium Enterprise' (Singapore: APEC, November 2015), Last accessed June 23, 2020, http://publications.apec.org/Publications/2015/11/Regulatory-Reform-Case-Studies-on-Improving-the-Business-Environment-for-Small-and-Medium-Enterprise.

[20] WTO initiatives would be described in Section 3.

Table 1.2: E-commerce-related initiatives by international organizations

No.	International organization	Area	List of non-exhaustive initiatives
1	APEC	Wide-ranging (e.g., regulatory ecosystem, infrastructure)	• APEC Blueprint for Action on Electronic Commerce • APEC Initiative of Cooperation to Promote Internet Economy • APEC Action Agenda for the Digital Economy • APEC Supply-Chain Connectivity Framework Action Plan • APEC Internet and Digital Economy Roadmap • APEC Cross-border E-Commerce Facilitation Framework • APEC Privacy Framework • APEC Cross-Border Privacy Rules System • APEC Online Dispute Resolution Framework • Pathfinder on Permanent Customs Duty Moratorium on Electronic Transmissions, Including Content Transmitted Electronically • Pathfinder on Building Blocks for Facilitating Digital Trade
2	UPU	Logistics, customs	• UPU Electronic Commerce Programme • Customs Declaration System • UPU*Clearing • UPU Postal Customs Guide
3	UNCTAD	Regulatory ecosystem, digital divide	• eTrade for all • eTrade for Women • eCommerce and Law Reform Programme
4	WCO	Customs	• Framework of Standards on Cross-Border E-Commerce • Resolution on the guiding principles for cross-border e-commerce • WCO Immediate Release Guidelines • SAFE Framework of Standards • Revised Kyoto Convention • WCO Customs Risk Management Compendium
5	ASEAN	Wide-ranging (e.g., regulatory ecosystem, infrastructure)	• Work Programme on E-commerce • ASEAN Agreement on Electronic Commerce • ASEAN ICT Masterplan

6	OECD	Wide-ranging (e.g., regulatory ecosystem, taxation)	• Guidelines on the Protection of Privacy and Transborder Flows of Personal Data • OECD/G20 Inclusive Framework on Base Erosion and Profit Shifting (BEPS)

Source: APEC PSU compilations.

APEC

APEC has identified the importance of creating a regulatory environment supporting e-commerce as early as the 1990s. For instance, the **APEC Blueprint for Action on Electronic Commerce** was introduced in 1998 where it set out the principles to promote and develop e-commerce within APEC.[21] The Electronic Commerce Steering Group (ECSG) was established in 1999 to ensure continued cooperation and pursuit of the APEC Blueprint for Action on Electronic Commerce and to perform a coordinating role for e-commerce activities in APEC. Originally established as an APEC Senior Official's Special Task Force, the ECSG was aligned with the Committee on Trade and Investment (CTI) in 2007 to ensure a strong focus on advancing APEC's goal of free and open trade and investment in the region.

In recent times, the region has facilitated e-commerce through various initiatives. One example is the **APEC Cross-border E-Commerce Facilitation Framework** endorsed in 2017. It has the following five main objectives: 1) create a favorable regulatory ecosystem for e-commerce to promote predictability, transparency, security, fair competition and consistency; 2) promote the development of ICT infrastructure to facilitate cross-border e-commerce; 3) encourage and facilitate greater participation of businesses in global commerce, in particular MSMEs; 4) enhance cooperation between the public and private sectors, including on consumer protection; and 5) contribute to trade and investment facilitation in the region, and support the achievement of the Bogor Goals and post-2020 vision. Five working pillars were identified to operationalize these objectives: 1) promoting transparent and predictable legal and regulatory approaches and measures that are business-friendly and coherent to facilitate cross-border e-commerce in the region; 2) enhancing capacity building so that APEC economies can assist MSMEs to increase their cross-border e-commerce participation in global and regional markets; 3) strengthening cross-border data privacy protection through increased implementation of existing APEC programs; 4) facilitating cross-border paperless trade in the region; and 5) addressing emerging and cross-cutting issues in cross border e-commerce.[22]

In 2017, APEC Leaders welcomed the **APEC Internet and Digital Economy Roadmap (AIDER)**, a living document promoting the development and growth of the internet and the digital economy in the region and to highlight potential areas of cooperation among APEC fora. The 11 focus areas that economies should concentrate their work on, but not limited their work

[21] APEC, '1998 Leaders' Declaration' (Singapore: APEC, 1998), Last accessed June 23, 2020, https://www.apec.org/Meeting-Papers/Leaders-Declarations/1998/1998_aelm/apec_blueprint_for.aspx.

[22] APEC, 'Annex A: APEC Cross-Border E-Commerce Facilitation Framework' (Singapore: APEC, 2017), Last accessed June 23, 2020, https://www.apec.org/Meeting-Papers/Annual-Ministerial-Meetings/2017/2017_amm/Annex-A.

to, are: 1) development of digital infrastructure; 2) promotion of interoperability; 3) achievement of universal broadband access; 4) development of holistic government policy frameworks for the internet and the digital economy; 5) promoting coherence and cooperation of regulatory approaches affecting the internet and the digital economy; 6) promoting innovation and adoption of enabling technologies and services; 7) enhancing trust and security in the use of ICTs; 8) facilitating the free flow of information and data for the development of the internet and the digital economy, while respecting applicable domestic laws and regulations; 9) improvement of baseline internet and the digital economy measurements; 10) enhancing the inclusiveness of the internet and the digital economy; and 11) facilitation of e-commerce and advancing cooperation on digital trade.[23]

In 2018, the **APEC Action Agenda for the Digital Economy** commits economies to preparing a comprehensive work programme on the implementation of AIDER with contributions from committees and sub-fora as well as to develop further the digital economy-related work areas. The action agenda also welcomed the establishment of the **Digital Economy Steering Group (DESG)** to preserve the functions of the ECSG and to monitor and report the progress made within focus areas identified in AIDER to Senior Officials.[24]

In the area of trade facilitation, for example, **APEC Supply-Chain Connectivity Framework Action Plan Phase II (SCFAP II)** identified chokepoints to increase business competitiveness (e.g., through the reduction of cost) and improve the reliability of the supply chain. E-commerce is covered under the 5th chokepoint where underdeveloped policy and regulatory infrastructure were identified as impediments to electronic trade.[25]

In the area of infrastructure, for example, the **APEC Connectivity Blueprint** aims to "strengthen physical, institutional, and people-to-people connectivity by taking agreed actions and meeting agreed targets by 2025, with the objective of achieving a seamless and comprehensively connected and integrated Asia Pacific".[26] Initiatives under the physical and institutional pillars are particularly relevant for e-commerce as they aspire to enhance digital connectivity and promote structural reforms to expand the application of safe and trusted ICT and e-commerce environment.

The **Boracay Action Agenda to Globalize MSMEs** calls for ICT and e-commerce to be utilized to promote the internationalization of MSMEs and integrate them into global value chains. It specifically calls for APEC to: 1) cooperate with the APEC Business Advisory

[23] APEC, 'APEC Internet and Digital Economy Roadmap' (2017/CSOM/006, Singapore: APEC, 2017), Last accessed June 23, 2020, https://www.apec.org/-/media/Files/Groups/ECSG/17_csom_006.pdf.

[24] APEC, 'Terms of Reference of the APEC Digital Economy Steering Group (Endorsed)' (Singapore: APEC, 2019), Last accessed June 23, 2020, http://mddb.apec.org/Documents/2019/SOM/SOM3/19_som3_022.pdf.

[25] APEC, '2018 Stocktake: The APEC Supply-Chain Connectivity Framework Action Plan (SCFAP) II 2017–2020' (Singapore: APEC, 2018), Last accessed June 23, 2020, https://www.apec.org/-/media/APEC/Publications/2018/11/2018-CTI-Report-toMinisters/TOC/Appendix-7---Stocktake-of-APEC-Initiatives-for-SCFAP-II.pdf.

[26] APEC. 'Annex D - APEC Connectivity Blueprint for 2015-2025'. (Singapore: APEC, 2014), Last accessed June 23, 2020, https://www.apec.org/Meeting-Papers/Leaders-Declarations/2014/2014_aelm/2014_aelm_annexd.

Council (ABAC) in identifying and promoting strategic e-commerce platforms and innovative business models for MSMEs to support buying and selling activities (business-to-consumer), business matching opportunities (B2B), and online-to-offline (O2O) commerce; 2) implement capacity building to promote international networking and increase cross-border business opportunities for MSMEs by localizing/customizing ABAC's Cross-Border E-Commerce Training (CBET) Programme and other similar platforms; 3) encourage the availability of next-generation high-speed broadband/internet and promote its use by MSMEs; and 4) ensure that policies and regulatory frameworks do not unnecessarily constrain the ability of MSMEs to participate in e-commerce.[27]

The **APEC Privacy Framework** provides guidance and direction to businesses and government entities on common privacy issues.[28] The framework was updated in 2015 to reflect major shifts in business operations and consumer expectations due to technological advancements and the nature of information flows.[29] Building on the Privacy Framework, the **APEC Cross Border Privacy Rules (CBPR) system** seeks to balance the flow of information and data across borders with the need for effective protection of personal information. It is a voluntary certification scheme allowing companies to transfer personal data (inter and intra company) across APEC participants. 9 APEC economies are currently participating in the CBPR system: Australia; Canada; Japan; Korea; Mexico; the Philippines; Singapore; Chinese Taipei; and the United States.[30]

APEC has also introduced a recognition system for personal information processors through the **Privacy Recognition for Processors (PRP) system**.[31] In addition, APEC has promoted cross-border cooperation through its **APEC Cross-border Privacy Enforcement Arrangement (CPEA)** which serves as a mechanism to allow privacy enforcement authorities to share information and assistance for cross-border privacy enforcement.[32] APEC is also exploring the possibility of achieving interoperability between CBPR and the European Union General Data Protection Regulation (EU GDPR), which came into force in May 2018.

Different APEC fora and stakeholders have undertaken projects to contribute towards the above. For example, the Committee on Trade and Investment (CTI) has several ongoing pathfinder initiatives, including: 1) **the Pathfinder on Permanent Customs Duty Moratorium on Electronic Transmissions** which is a commitment by 13 economies to go

[27] APEC. 'Boracay Action Agenda to Globalize MSMEs', Last updated 2015, Last accessed June 23, 2020, https://www.apec.org/Meeting-Papers/Sectoral-Ministerial-Meetings/Trade/2015_trade/2015_mrt_standalone.aspx.

[28] APEC, 'APEC Privacy Framework' (Singapore: APEC, December 2005), Last accessed June 23, 2020, http://publications.apec.org/Publications/2005/12/APEC-Privacy-Framework.

[29] APEC, 'Updates to the APEC Privacy Framework' (2016/CSOM/012app17, Singapore: APEC. 2016), Last accessed June 23, 2020, http://mddb.apec.org/Documents/2016/SOM/CSOM/16_csom_012app17.pdf.

[30] APEC, 'Cross Border Privacy Rules System', CBPRs, Last accessed 19 September 2019, http://cbprs.org/.

[31] APEC. 'APEC Privacy Recognition for Processors System', Last accessed May 28, 2020. http://m.apec.org/~/media/Files/Groups/ECSG/2015/APEC%20PRP%20Rules%20and%20Guidelines.pdf.

[32] APEC. '2019 APEC Economic Policy Report', Last updated 2019, Last accessed June 23, 2020, https://www.apec.org/Publications/2019/11/2019-APEC-Economic-Policy-Report.

make permanent the WTO moratorium;[33] and 2) **the Pathfinder on Building Blocks for Facilitating Digital Trade** which aims to commit members to support works in the identified building blocks covering issues such as enabling cross border data flows, minimizing data localization requirements, IPR protection, customs modernization and digital infrastructure development.[34] CTI has also facilitated the compilation of e-commerce related laws and regulations within member economies and published them in the APEC Trade Repository in 2018. In addition, CTI analyzed the status of APEC members' e-commerce laws/regulations that have implications on the supply chain.[35] PSU also conducted a study to better understand how firms from different sectors use data in their business models; and considering the significant increase in data-related policies and regulations enacted by governments across the world, how such policies and regulations are affecting their use of data and hence business models. The study identified middle-ground approaches that would enable governments to achieve public policy objectives, such as data security and privacy, as well as promote the growth of data-utilizing businesses.[36] Through the 2019 APEC Economic Policy Report, the Economic Committee (EC) elaborated on the twin role of measurement and structural reforms in maximizing opportunities and overcoming challenges of the digital economy.[37] EC has also developed the **APEC Collaborative Framework for Online Dispute Resolution (ODR) of Cross Border Business –to –Business (B2B) Disputes**. It provides a useful guide for businesses (particularly MSMEs) for tapping online dispute resolution for negotiation, mediation and arbitration for business-to-business disputes[38], so as to lower transaction costs for MSMEs and reduce barriers for entry into international trade. In 2019, the Telecommunications and Information Working Group (TELWG) endorsed the **APEC Framework for Securing the Digital Economy**, which provides non-binding principles and strategic recommendation to inform member economies as they develop policy and regulatory frameworks to secure their digital economies and enhance trust in the use of ICTs.[39]

Individual APEC economies have also undertaken economy-level initiatives outside the ambit of APEC to promote e-commerce. One example is the conclusion of trade agreements containing chapters on e-commerce or related topics. The e-commerce chapter of the

[33] APEC, '2019 CTI Pathfinder Initiatives', Last accessed August 5, 2020, http://publications.apec.org/-/media/APEC/Publications/2019/12/2019-CTI-Report-to-Ministers/TOC/Appendix-6---Pathfinder-Initiatives.pdf.

[34] APEC. 'Updated Pathfinder Initiative Proposal on Building Blocks for Facilitating Digital Trade', Last accessed August 5, 2020, http://publications.apec.org/-/media/APEC/Publications/2019/12/2019-CTI-Report-to-Ministers/TOC/Appendix-5---Pathfinder-Initiative---Building-Blocks-for-Facilitating-Digital-Trade.pdf.

[35] APEC, 'Report on Legal and Regulatory Framework on E-Commerce for APEC Supply Chain Connectivity (CTI 23 2017A)'.

[36] APEC PSU, 'Fostering an Enabling Policy and Regulatory Environment in APEC for Data-Utilizing Businesses', Last accessed June 23, 2020, https://www.apec.org/Publications/2019/07/Fostering-an-Enabling-Policy-and-Regulatory-Environment-in-APEC-for-Data-Utilizing-Businesses.

[37] APEC, '2019 APEC Economic Policy Report on Structural Reform and the Digital Economy', Last accessed June 23, 2020, https://www.apec.org/Publications/2019/11/2019-APEC-Economic-Policy-Report.

[38] APEC, 'APEC Collaborative Framework for Online Dispute Resolution (APEC 2019 Second Economic Committee Meeting, Santiago, Chile, 2019)', Last accessed June 23, 2020, http://mddb.apec.org/Documents/2019/EC/EC2/19_ec2_022.pdf.

[39] APEC, 'APEC Framework for Securing the Digital Economy', Last accessed July 24, 2020, https://www.apec.org/Publications/2019/11/APEC-Framework-for-Securing-the-Digital-Economy.

Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP),[40] an agreement signed by 11 APEC economies, provides rules on a range of issues which includes the adoption of legal frameworks on e-commerce (e.g., electronic transaction, online consumer protection and the protection of personal information), cross-border transfer of information by electronic means, location of computing facilities, source code and cooperation on cybersecurity. The United States-Mexico-Canada Agreement (USMCA)[41] Chapter on Digital Trade includes specific rules on intermediary service liability, the facilitation of cross-border data flows, prohibition of data localization, prohibition of customs duties application and other discriminatory measures to digital products, which would have implications on e-commerce.

UNITED POSTAL UNION (UPU)

The UPU is an international forum for cooperation among stakeholders in the postal sector. Its role consists of providing advisory, mediation, liaison services as well as technical assistance. Furthermore, it is involved with international rule making on mail exchanges.[42] Several initiatives have been undertaken to promote a good regulatory environment for e-commerce. For instance, **UPU Electronic Commerce Programme** aims to facilitate cross border trade flows by coordinating and accelerating e-commerce development in the postal sector. Under this programme, a total of five areas are identified, specifically market development, postal electronic services, logistics, interoperability and payment.[43] Additionally, the **Customs Declaration System** (CDS) was introduced to promote the exchange of data as well as calculate required duties and taxes between participating Posts and Customs. By doing so, it aims to increase the efficiency of customs clearance for packages sent. Some ways in which it has done so includes enabling posts to share information through electronic data interchange (EDI) messaging before sending out a package.[44] In addition, it has also introduced the **UPU-WCO (World Customs Organization) Postal Customs Guide** which serves as an information source on postal customs clearance processes as well as creates a common ground for dialogues and discussions between the designated operators of UPU member economies and Customs administrations of the WCO.[45] Finally, **UPU*Clearing** creates a streamlined

[40] Government of Canada, 'n.d. Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)', Last accessed June 23, 2020, https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cptpp-ptpgp/text-texte/index.aspx?lang=eng&_ga=2.153292080.908985840.1591587820-810533718.1591587820.

[41] Office of the United States Trade Representative, 'n.d. United States-Mexico-Canada Agreements'. https://ustr.gov/usmca

[42] Universal Postal Union, 'The UPU', Last accessed 20 December 2019, http://www.upu.int/en/the-upu/the-upu.html.

[43] Universal Postal Union, 'The E-commerce programme', Last updated 2017, Last accessed June 23, 2020, http://www.upu.int/fileadmin/documentsFiles/activities/eCommerce/faqAboutTheUpuECommerceProgrammeEcomproEn.pdf.

[44] Universal Postal Union, 'About Customs', Last accessed 20 December 2019, http://www.upu.int/en/activities/customs/about-customs.html.

[45] Universal Postal Union 'WCO–UPU Postal Customs Guide', Last accessed 5 August 2020, https://www.icao.int/Meetings/AirCargoDevelopmentForum-Togo/Documents/WCO-UPU_PostalCustomsGuide-June2014.pdf.

settlement system by consolidating transactions and requiring debtors to pay a monthly payment. As of March 2018, 47 member economies have participated in the system.[46]

THE UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT (UNCTAD)

UNCTAD has implemented several initiatives on e-commerce. Much of its role has been in ensuring e-commerce regulations and specific implementation plans are in place within economies. Among its key initiatives includes "**eTrade for all**" where it aims to improve the capacity of less developed economies in engaging and benefitting from e-commerce.[47] It has since expanded this initiative to target women under its **"eTrade for Women"** programme, which aims to better empower women, specifically entrepreneurs, through ICTs.[48] In the same vein, its "**eCommerce and Law Reform Programme**" aims to help developing economies establish regulatory regimes to promote electronic transactions by increasing the trust individuals place in online transaction, thereby facilitating e-commerce and protecting its participants.[49]

Furthermore, **UNCTAD's Friends of E-Commerce for Development (FED)** is in the process of putting forward a roadmap focused on key areas relevant to e-commerce. Some important areas included in the roadmap are[50]: 1) identification of strategies for e-commerce readiness; 2) access to ICT infrastructure and services; 3) trade logistics and trade facilitation; 4) e-payment solutions; 5) legal certainty and regulatory frameworks; 6) capacity building and technical assistance; and 7) access to financing. Efforts have also been made to better measure e-commerce and the digital economy through the collection of more accurate statistics on e-commerce and the digital economy to better guide policymaking. In addition to research and data collection, it is involved with the provision of technical assistance.[51]

In terms of easing cross-border transactions, it has launched the **UNCTAD Automated System for Customs Data (ASYCUDA)** to provide an integrated customs management system,

[46] Universal Postal Union, 'UPU*Clearing', Last accessed 20 December 2019, http://www.upu.int/uploads/tx_sbdownloader/brochureUpuClearingEn.pdf.
[47] UNCTAD, 'The eTrade for All Initiative', Last accessed 20 December 2019, https://unctad.org/en/Pages/DTL/STI_and_ICTs/eTrade-for-All.aspx.
[48] UNCTAD, 'eTrade for Women', Last accessed 20 December 2019, https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-eTrade-for-Women.aspx.
[49] UNCTAD, 'eCommerce and Law Reform Programme', Last accessed 20 December 2019, https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation.aspx.
[50] UNCTAD, 'Developing Countries Launch Roadmap for International Trade and Development Policy', Last updated 2017, https://www.ip-watch.org/weblog/wp-content/uploads/2017/04/Press-Release-FED-Ministerial-Meeting-25.04.17-002.pdf?089987.
[51] UNCTAD, 'Measuring E-commerce and the Digital Economy', Last accessed 20 December 2019, https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Measurement.aspx.

modernize customs operations, increase efficiency of trade, improve security, tackle corruption and promote the use of electronic documents.[52]

WORLD CUSTOMS ORGANISATION (WCO)

The WCO is an independent inter-governmental body that aims to improve the efficiency and effectiveness of customs administration. In addition to formulating conventions, it provides technical assistance and capacity building to economies. The WCO has initiated the **Framework of standards on cross-border e-commerce** as well as made efforts towards their implementation. The framework aims to provide baseline standards to help governments create their own e-commerce frameworks including action plans and timelines.[53] Moreover, WCO adopted the **resolution on the guiding principles for cross-border e-commerce**. Based on this resolution, the WCO has developed standards, guidelines and tools for customs clearance and data harmonization.[54]

Additionally, it has introduced the **WCO Immediate Release Guidelines** to help custom authorities reduce the time taken to clear a large number of small or negligible value goods across borders. The guidelines was updated in 2018 to take into consideration the flow of low-value and small electronic commerce goods and services.[55] Furthermore, the **SAFE Framework of Standards** was introduced with multiple objectives such as establishing standards to provide supply chain security and facilitation at a global level, and enabling integrated and harmonized supply chain management for all modes of transport.[56] Other initiatives includes the **Revised Kyoto Convention** to outline governing principles to promote trade facilitation and controls,[57] and the **WCO Customs Risk Management Compendium** to help streamline the operating systems of individual WCO member economies.[58]

---

[52] UNCTAD, 'Customs Automation – ASYCUDA', Last accessed 20 December 2019, https://unctad.org/en/Pages/DTL/TTL/ASYCUDA-Programme.aspx,

[53] WCO, 'Cross-border E-commerce Framework of Standards', Last updated 2018, Last accessed June 23, 2020, http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/activities-and-programmes/ecommerce/wco-framework-of-standards-on-crossborder-ecommerce_en.pdf?db=web.

[54] WCO, 'Resolution of the Policy Commission of the World Customs Organization on the Guiding Principles for Cross-border E-commerce', Last updated 2017, Last accessed June 23, 2020, http://www.wcoomd.org/-/media/wco/public/global/pdf/about-us/legal-instruments/resolutions/policy-commission-resolution-on-cross_border-ecommerce_en.pdf?la=en.

[55] WCO, 'Immediate Release Guidelines', Last accessed 5 August 2020, http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/immediate-release-guidelines.aspx#:~:text=instruments%20and%20tools-,Immediate%20Release%20Guidelines,courier%20and%20express%20mail%20services.

[56] WCO, 'SAFE Frameworks of Standards, 2018 edition', Last accessed 5 August 2020, http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/safe-package/safe-framework-of-standards.pdf?la=en.

[57] WCO, 'The Revised Kyoto Convention', Last accessed 5 August 2020, http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/conventions/pf_revised_kyoto_conv.aspx.

[58] WCO, 'Customs Risk Management Compendium', Last accessed 5 August 2020, http://www.wcoomd.org/en/Topics/Facilitation/Instrument%20and%20Tools/Tools/Risk%20Management%20Compendium.

A joint committee was established by WCO and UPU to create an avenue to collaborate on customs issues regarding the clearance of postal items. To do so, it develops procedures and publications to help guide the domestic and international post-customs work carried out by the organizations.[59] Thus far, it has collaborated to develop electronic messages for the clearance of postal items.[60]

ASSOCIATION OF SOUTHEAST ASIAN NATIONS (ASEAN)

Extensive work on e-commerce is ongoing at ASEAN. It has established a **Work Programme on E-commerce** including eight elements covering a wide range of e-commerce issues such as 1) infrastructure; 2) consumer protection; 3) education and technological competencies; 4) competition; 5) legal frameworks; 6) logistics; 7) security of electronic transactions; and 8) e-commerce frameworks. Each element is supported by multiple initiatives to operationalize work in that area. For instance, five initiatives were designed under the element of infrastructure to better improve region-wide accessibility of broadband infrastructure and the environment of e-marketplace and e-commerce platforms, such as providing affordable international mobile roaming services among ASEAN economies, improving broadband services in rural areas, and developing ASEAN guidelines on accountability and responsibilities of platform providers.[61]

In 2018, ASEAN member economies signed the **ASEAN Agreement on Electronic Commerce**. It acknowledges the value of e-commerce within cross-border trade and investment, and the importance of lowering barriers for businesses particularly SMEs. [62] Other work by ASEAN includes adopting **ASEAN Digital Integration Framework**, **ASEAN ICT Masterplan 2020**, **Master Plan on ASEAN Connectivity 2025**, and **ASEAN Framework for Personal Data Protection**.[63]

ASEAN economies are also collectively parties to trade agreements which include chapters on e-commerce within it, such as the **ASEAN-Australia-New Zealand Free Trade Agreement**[64] and the **Regional Comprehensive Economic Partnership (RCEP)**[65], although the latter has yet to be signed.

---

[59] Universal Postal Union, 'About Customs', Last accessed 20 December 2019, http://www.upu.int/en/activities/customs/about-customs.html.

[60] WCO, 'Cross-border E-commerce', Last accessed 20 December 2019, http://www.wcoomd.org/en/topics/facilitation/activities-and-programmes/ecommerce.aspx.

[61] ASEAN, 'ASEAN Work Programme on Electronic Commerce 2017-2025', Last accessed 20 December 2019, https://asean.org/asean-economic-community/sectoral-bodies-under-the-purview-of-aem/e-commerce/.

[62] ASEAN, 'ASEAN Agreement on Electronic Commerce', Last updated 2019. Last http://agreement.asean.org/media/download/20190306035048.pdf.

[63] ASEAN, 'ASEAN Digital Integration Framework', Last accessed 20 December 2019, https://asean.org/storage/2019/01/ASEAN-Digital-Integration-Framework.pdf.

[64] AANZFTA, 'Chapter 10. Electronic Commerce', Last accessed 5 August 2020, https://aanzfta.asean.org/index.php?page=chapter-10-electronic-commerce/.

[65] ASEAN, 'Regional Comprehensive Economic Partnership (RCEP)', Last accessed 5 August 2020, https://asean.org/?static_post=rcep-regional-comprehensive-economic-partnership.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD)

OECD has played an important role in fostering discussions and addressing various challenges brought by the digital economy. In terms of data privacy, OECD revised its Privacy Guidelines in 2013 and adopted the new **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**. The Guidelines advocate a risk-management approach to privacy protection and calls for improved interoperability of regulations at the global level.[66] On consumer protection, OECD updated its policy recommendations to include emerging trends in e-commerce. New developments include topics on digital content products, payment protection, privacy and security risks, and free goods and services in exchange for consumers' personal data.[67] Moreover, digital technologies have allowed multinational companies to avoid taxes by locating their physical presence in no or low-tax economies while doing business globally. To tackle issues pertaining to taxation, OECD established a **Base Erosion and Profit Shifting (BEPS) Action Plan** in 2013 and introduced 15 Actions in 2015 to provide further guidance on policy instruments at domestic and international levels.[68] Furthermore, **the OECD/G20 Inclusive Framework on BEPS** now has more than 130 members, working toward a consensus-based long-term solution to the tax challenges faced in the digital economy.[69]

1.3 STUDY OBJECTIVE AND METHODOLOGY

In recognition of the importance of e-commerce in global trade, WTO has been undertaking programmes on e-commerce since 1998. Furthermore, in January 2019, several WTO members announced their intention to commence negotiations on trade-related aspects of e-commerce. This study has been designed to contribute to the ongoing process as well as the capacity building activities that may arise from it. It comprises of two main components, namely: (1) the database component; and (2) the case study component. More information on how each can potentially contribute to the WTO process are provided below.

DATABASE OF RELEVANT LAWS AND REGULATIONS

The database component aims to provide a good snapshot of where APEC members are pertaining to each element with implications on e-commerce. To identify the relevant elements, this study will first review public submissions made by WTO member economies in response to the announcement mentioned in the preceding paragraph. Through the review of existing

[66] OECD, 'OECD Privacy Guidelines', Last accessed 20 December 2019, https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm.

[67] OECD, 'Consumer Protection in E-commerce' (Paris: OECD, 2016), Last accessed June 23, 2020, https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf.

[68] OECD, 'BEPS Actions', Last accessed 30 December 2019, https://www.oecd.org/tax/beps/beps-actions/.

[69] OECD, 'Programme of Work to Develop a Consensus Solution to the Tax Challenges Arising from the Digitalisation of the Economy', Last accessed June 23, 2020, https://www.oecd.org/tax/beps/programme-of-work-to-develop-a-consensus-solution-to-the-tax-challenges-arising-from-the-digitalisation-of-the-economy.pdf.

literature as well as the submissions, this study attempts to determine the key areas of negotiation and pose relevant questions. For example, under the area of electronic authentication/signature, questions would include: (1) if a specific economy regulates electronic/digital contract, identification and signature, and if so; (2) whether the applicable laws/regulations are technology neutral; and (3) whether they recognize foreign authentication services. Where applicable, it has and will look into whether a specific economy has adopted international guidelines/initiatives. In the case of electronic authentication/signature, this would include among others: (1) UNCITRAL Model Law on Electronic Commerce; (2) UN Convention on the Use of Electronic Communications in International Contracts; and (3) UNCITRAL Model Law on Electronic Signature. The study will then populate the database using economy-specific information obtained from various sources including official documents, reports of other international organizations, and public information found online. Through deeper analysis of the database, the study hopes to enable policymakers to better understand the differences in situations and approaches across economies pertaining to key areas for e-commerce. This will hopefully provide more clarity on where APEC economies stand on these areas and therefore, encourage deeper discussions both at APEC and WTO. Additionally, it is hoped that the study can serve as starting point for the formulation and conduct of information sharing and capacity-building activities among APEC members.

CASE STUDIES

Despite the importance of the information provided by the database, they may not give a holistic picture of the situation. For example, although the database allows one to find out quickly if a particular economy has ratified the WTO Trade Facilitation Agreement (TFA), it is challenging to capture in details what the economy has introduced to operationalize the TFA. Moreover, the fact that the database captures the regulatory environment at a point in time means that it does not allow useful economy-level experiences to be recorded and shared. For instance, it would be interesting to understand the motivation for revising existing regulations or introducing new regulations, the process of doing so as well as how the revision/introduction has contributed to the e-commerce landscape in the economy. Furthermore, it would be worthwhile to better understand how the evolving COVID-19 situation has had implications on e-commerce and related aspects.

The case study component would hopefully remedy some of the shortcomings of the database and hence complement it. In other words, while the primary objective of the case study component is fairly similar to that of the database component, that is, to provide more clarity on variation in situations and approaches across economies and hence potential information sharing and capacity building activities, it is hoped that this component would also shed more details on the motivations and the practicalities of these approaches, hence further enriching the discussions at APEC and WTO.

1.4 STRUCTURE OF THE REPORT

This report has been structured as follows:

- **Section 2** provides information on the technicalities behind trade-related aspects of e-commerce.
- **Section 3** provides an overview of the current state of discussions on trade-related aspects of e-commerce at international settings, with a focus on those being undertaken under the ambit of WTO. It will also identify issues that will likely form part of the WTO agreement.
- **Section 4** provides an analysis of the database component on elements covered under the six focus areas (elaborated on in Section 3).
- **Section 5** comprises of a series of economy case studies covering different focus areas.
- **Section 6** concludes and provides some themes for the capacity building activities.
- **Annex A** contains the database of laws and regulations.

2 TECHNICALITIES BEHIND TRADE RELATED ASPECTS OF E-COMMERCE

2.1 DEFINING E-COMMERCE

As mentioned earlier, there is currently no agreed definition of "e-commerce". In the policy sphere, two prevalent definitions exist. The OECD defines e-commerce transaction as "the sale or purchase of goods or services, conducted over computer networks by methods specifically designed for the purpose of receiving or placing of orders"[70], while the WTO's work programme on e-commerce defines e-commerce as the "production, distribution, marketing, sale, delivery of goods and services by electronic means".[71] Yet, in light of the fast-paced evolution of technology and the migration of many offline economic activities to the online realm, it is possible that the definition of e-commerce might evolve in the future to cover new areas.

While e-commerce transactions are supported by computer networks or electronic means, it is the *internet* that has significantly enabled e-commerce to grow. Its use is now ubiquitous through the adoption of mobile technology, online banking, and other features of digital markets that are part of our everyday lives. One similarity across these technologies is their reliance on internet infrastructure. As such, it is important to understand how the internet has allowed e-commerce to happen, and which characteristics of the internet architecture should be considered when regulating e-commerce. A brief technical overview of this architecture is elaborated below.

2.2 THE INTERNET AS THE ENABLER OF E-COMMERCE

HOW THE INTERNET FUNCTIONS

The internet is the *network of networks*. This means that the internet is a system that allows independent, smaller computer networks to communicate with one another. These independent computer networks can be controlled by different actors (i.e., private or public) and can be made either accessible or restricted. This would vary and depend upon each specific network. However, should the independent computer network want to communicate with another network (i.e., send data packets), it has to do so through the means of the *Internet Protocol (IP)*. The IP uses *packet switching*, which allows self-contained packets of data to be operated as separate units, routing them from source to destination via unique identifiers.[72] Each data packet resembles an envelope containing source and destination addresses. By means of this,

[70] OECD, 'A Borderless World: Realizing the Potential of the Global Electronic Commerce' (Paris: OECD, 2013).
[71] WTO, 'Ministerial Declaration on Global E-Commerce 1998', Adopted by the General Council on 25 September 1998 (World Trade Organization (WTO), September 30, 1998).
[72] Andrew Butterfield, Gerard Ekembe Ngondi, and Anne Kerr, eds., 'Datagram' in A Dictionary of Computer Science (Oxford University Press, 2016), Last accessed June 23, 2020, https://www.oxfordreference.com/view/10.1093/acref/9780199688975.001.0001/acref-9780199688975-e-1222.

data packets can be routed and transmitted across networks, hence avoiding congestions or problems in the networks.[73] This technical functioning has implications on the characteristics of the internet (e.g., its distributed and end-to-end architecture) and corresponding activities including e-commerce.

CHARACTERISTICS AND PRINCIPLES OF THE INTERNET ARCHITECTURE

The internet was envisioned by its original architects with some of the following characteristics:

Packet switching in a distributed environment

As described above, packet switching is fundamental to how the internet works. It is made possible by the distributed architecture of the internet where there is no single point of control. This makes the internet less vulnerable to incidents as compared to when centralized networks are used.[74] In the event that a specific route within which a transmitted data packet encounters issues (e.g., certain submarine cables are affected by a natural disaster), another route can be used instead. Likewise, a route made unusable by cyberattacks can be substituted by another. This can be maximized by locating routers across the world. However, there is a risk that the internet is charting towards a centralized scenario as a result of the control increasingly imposed on server locations. By doing so, there could exist restrictions to access certain content in some jurisdictions, some of which are required for legitimate public policy objectives.

Openness

Openness refers to networks that are not divided by policies or regulations (e.g., by the existence of firewalls), where two endpoints should be able to communicate and exchange data packets with any other device. For instance, "any internet user can exchange email with more than two billion other global internet users, entrepreneurs can launch services such as eBay and Amazon (…); and people from all across the world can connect with others".[75] All of these are enabled by protocols, which are the rules allowing computers to speak to each other (and will be further explained below). Additionally, openness refers to the way those protocols are developed and to their non-proprietary nature, allowing for spontaneous innovation.[76]

---

[73] T Socolofsky and C Kale, 'RFC 1180: A TCP/IP Tutorial' (Internet Engineering Task Force, January 1991), Last accessed June 23, 2020, https://www.ietf.org/rfc/rfc1180.txt.

[74] Paul Baran, 'On Distributed Networks', IEEE Transactions on Communications Systems, 1964.

[75] Jonah Force Hill, 'Internet Fragmentation: Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers', Science, Technology, and Public Policy Program, Belfer Center for Science and International Affairs (Harvard Kennedy School, May 2012), Last accessed June 23, 2020, https://www.belfercenter.org/sites/default/files/legacy/files/internet_fragmentation_jonah_hill.pdf.

[76] CIGI and Chatman House, 'One Internet: Global Commission on Internet Governance', Last updated 2016, vi, Last accessed June 23, 2020, https://www.cigionline.org/sites/default/files/gcig_final_report_-_with_cover.pdf.

End-to-end

This indicates that the intelligence of the network resides at the ends, not within the network.[77] In other words, the internet just routes and transmits data packets, without knowing or investigating the content. It does not know if a data packet is a video, text, or audio; whether it infringes copyright; whether it has harmful content, etc. As a result, it cannot discriminate or differentiate traffic. It is up to the applications at the end of the network to do so. Some have interpreted this characteristic to mean that the network does not think and therefore, intelligence resides at the "end", at the level of applications.[78] However, others have interpreted this as the network being transparent, hence allowing applications to be easily built on top of it and potentially reach a worldwide audience.[79] In other words, the economics and network effects of internet transparency are the driving force behind the global reach of applications such as the World Wide Web (WWW).[80]

Layered Architecture

The functioning of the internet is based on a technical architecture that follows a layering principle. Each underlying layer has a certain technical function, which usually determines the correct working of layers at higher levels.[81] The internet's layered architecture enables those working on one layer, to ignore the inner workings of other layers, reducing coordination cost and accelerating innovation.[82] As a result, anyone can innovate at the higher levels of the layered model, without having to invest in the bottom layers.

The layering approach can vary in conceptualization, but with regard to networks, two technical models prevail. These are:

(i) *Open Systems Interconnection Reference Model (OSI model)*[83]: a model of seven different layers (physical network, data link, network, transport, session, presentation and application); and

(ii) *Transmission Control Protocol/Internet Protocol (TCP/IP) model*: a model with four distinct layers (link, internet, transport, application).

---

[77] Jerome H Saltzer, David Reed, and David Clark, 'End-to-End Arguments in System Design', ACM Transactions on Computer Systems 2 (1984), Last accessed June 23, 2020, http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf.

[78] Lawrence Solum and Minn Chung, 'The Layers Principle: Internet Architecture and the Law' (University of San Diego School of Law, Public Law and Legal Theory Research Paper No. 55, 2003), 15, Last accessed June 23, 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=416263.

[79] Lawrence Lessig, 'Code and Other Laws of Cyberspace (New York: Basic Books, 2000)'.

[80] Solum and Chung, 'The Layers Principle: Internet Architecture and the Law', 64.

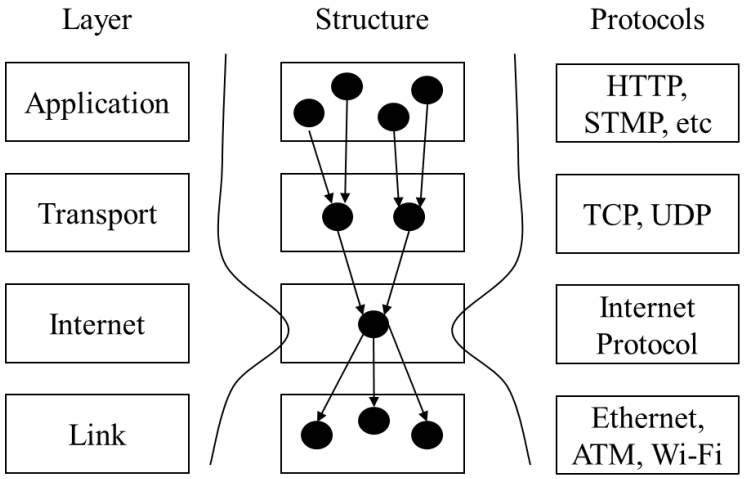
[81] Barbara van Schewick, 'Internet Architecture and Innovation (Cambridge, Massachusetts; London, England: The MIT Press, 2010)', 88–89.

[82] Christopher S Yoo, 'Protocol Layering and Internet Policy', University of Pennsylvania Law Review 161, 2013: 1770.

[83] 'ISO - 35.100 - Open Systems Interconnection (OSI)', Last accessed June 23, 2020, https://www.iso.org/ics/35.100/x/.

While both models are valid, the TCP/IP is "the obligatory standard to be used by any system connecting to the internet" (Figure 2.1).[84] It has been conceptualized as an hourglass model.[85] This conceptualization emphasizes the importance of the internet layer and the IP. The crucial role played by the IP is to allow layers to talk to each other, hence enabling data flow.

Figure 2.1: The TCP/ IP Model



Source: Adapted from Thomas-Quentin Maillart, "Mechanisms of Internet Evolution and Cyber Risk" (ETH Zurich, 2011), based on Barbara van Schewick, Internet Architecture and Innovation (Cambridge, Massachusetts; London, England: The MIT Press, 2010), 89.

INTERNET'S LAYERED ARCHITECTURE APPLIED TO POLICYMAKING

While the actual number of technical layers applied to policymaking varies according to different authors,[86] this report will adopt a four-layered model following CIGI and Chatman House's report.[87] It is as represented in Figure 2.2 below.

Figure 2.2: Different layers of Internet structure for policymaking

Content Layer (e.g., text, speech, music)
Application Layer (e.g., World Wide Web)
Logical Layer (e.g., internet protocols)
Infrastructure Layer (e.g., telecommunication networks)

Source: CIGI and Chatman House, 'One Internet: Global Commission on Internet Governance', 3.

[84] Andrew Butterfield, Gerard Ekembe Ngondi, and Anne Kerr, eds., 'TCP/IP', in A Dictionary of Computer Science (Oxford University Press, 2016), Last accessed June 23, 2020, https://www.oxfordreference.com/view/10.1093/acref/9780199688975.001.0001/acref-9780199688975-e-5310?rskey=JYraeS&result=1.

[85] Jonathan Zittrain, 'The Future of the Internet and How to Stop It (New Haven, CT: Yale University Press, 2008)', 70; van Schewick, Internet Architecture and Innovation, 89.

[86] The conceptualization of how the internet's layering principle applies to policymaking varies (See: Lessig 2000, Werbach 2002, Solum and Chung 2003, UNCTAD 2006, Zittrain 2008, Yoo 2013). Some policy reports follow a fourth layered approach. See: UNCTAD, 'Information Economy Report 2006: The Development Perspective'; OECD, "Economic and Social Benefits of Internet Openness," OECD Digital Economy Papers (OECD Publishing, 2016). while other experts follow a simplified three layers approach Lessig, Code and Other Laws of Cyberspace; Zittrain, The Future of the Internet and How to Stop It.

[87] CIGI and Chatman House, 'One Internet: Global Commission on Internet Governance'.

At the bottom is the infrastructure layer over which data would flow. This corresponds to the link layer of the TCP/IP model but also includes physical hardware. In the middle, the logical layer corresponds to the internet layer of the TCP/IP model, containing only the IP. One level above, the application and transport layers of the TCP/IP model are merged into one, the application layer. Finally, at the top is the content layer, which is not originally envisioned in the TCP/IP model. Below is a brief explanation of those layers, and the protocols contained in those layers.

Infrastructure layer

The physical layer allows for the transmission of data and is composed of the hardware over which data packets are carried. This includes a range of communication media such as telephone lines, fiber optic cables, satellites, microwaves, wireless links, and electric grids.

The management of data flow is undertaken by routers, which are pieces of computer hardware examining the IP address of an incoming data package and forwarding it to its destination address on a best effort basis (i.e., without any guarantee that the data packets will arrive at the final destination).

The physical layer is closely related to physical networks, and in particular, telecommunication networks, which are typically managed by Internet Service Providers (ISPs). Telecommunication is a topic regulated at both the domestic level (by the respective regulatory authorities) and the international level (e.g., the ITU and the WTO via the reference paper on basic telecommunications). Two important policy issues associated with this layer are interconnection and universal access.

Logical layer

The logical layer includes the Internet Protocol (IP), other internet resources (e.g., the Domain Name System), and a variety of internet protocols (e.g., TCP).

The Domain Name System (DNS)

In order to be reachable, computers and other resources must have unique addresses (e.g., IP addresses). However, since it would be difficult to remember each numerical IP address on the internet, the Domain Name System (DNS) was created to solve this problem. The DNS is a highly distributed Internet directory service that allows the use of domain names that are easy to remember instead of numerical IP addresses.

The DNS protocol is divided into Generic Top Level Domains (gTLDs), which are available to anyone for any use (e.g., com, net, org, mil); Sponsored Top Level Domains (sTLD), which rely on special registries acting as sponsors and establishing and enforcing rules restricting the eligibility of registrants (e.g. asia, gov, edu, int); Geographic gTLD, reserved for geographical, geopolitical, ethnic, linguistic or cultural community; Country Code Top Level Domains

(ccTLDs), reserved for economies or territories, and Internationalized Domain Names (IDNs), which allow the domain name to be in local languages and scripts (Arabic, Chinese, among others).

Protocols

Protocols represent a set of rules or steps. In the internet, they are used for establishing ways that will allow computers to talk to each other, determine how data packets are sent, received, forwarded, etc. Although other protocols are widely used as well, the most important protocol is the IP.

- IP

The IP transmits data by breaking it into smaller sized, labeled data packets, which are then sent to a specific destination. Each computer along the way will act as a router that only looks at the destination address. It then passes the data packets along until it reaches the intended recipient.

- Border Gateway Protocol (BGP)

The routing of data packets also occur via the BGP, which is the protocol enabling routers belonging to different organizations to select paths for data transmission across the internet. Some incidents that can alter the normal functioning of this routing protocol is when governments block access to a certain website. This can be enabled by dropping all data packets intended to arrive at a specific destination or re-routing them.[88] For instance, in 2008, YouTube became globally unreachable after a Pakistani ISP altered a BGP route in an attempt to block access to this site in Pakistan.[89]

- Transmission Control Protocol (TCP) and User Datagram Protocol (UDC)

As IP does not guarantee that data packets will arrive at the final destination, or how they will arrive, transport protocols built on top of the IP are crucial. For instance, TCP ensures data packets arrive in the correct order, and if any data package is lost, the protocol will request for that specific package to be sent again.[90] While TCP is the most widely used transport protocol, it is not the only one. Another available protocol is the UDC, which prioritizes speed instead of correct transmission of data packets. This works well for video and audio data

Importantly, neither TCP nor UDP are designed to look inside the content of data packets. One of the techniques allowing one to look inside the data packets is the Deep Packet Inspection (DPI), which in some cases is used to enable the prioritization of certain type of content over

[88] Hari Balakrishnan, 'How YouTube Was Hijacked' (Massachusetts Institute of Technology - Department of Electrical Engineering and Computer Science, May 2009), Last accessed February 5, 2020, http://web.mit.edu/6.02/www/s2012/handouts/youtube-pt.pdf.

[89] Brad Stone, 'Pakistan Cuts Access to YouTube Worldwide', The New York Times, February 26, 2008. Last accessed February 5, 2020, https://www.nytimes.com/2008/02/26/technology/26tube.html.

[90] Socolofsky and Kale, 'RFC 1180: A TCP/IP Tutorial', Last updated 1991, Last accessed June 23, 2020, https://www.ietf.org/rfc/rfc1180.txt.

another. Traffic management practices of this type would technically lead to some data packets travelling at a lower or higher speed than others. A way to avoid looking inside the package is through the use of encryption.

Other protocols

Among other important protocols, it is worthwhile to mention the Hypertext Transfer Protocol (HTTP), which one can see at the start of the address in the web browser, and the Hypertext Markup Language (HTML). Both software solutions support several browsing programs such as Microsoft Internet Explorer, Google, Chrome and Yandex. Other critical protocols are the Simple Mail Transfer Protocol (SMTP), which supports e-mail; File Transfer Protocol (FTP), for transferring files from one server to another; and Real-Time Transport Protocol (RTP), for streaming audio and video content. All these applications run within the end host, not within the network.[91] Thus, the IP does not know whether data being transmitted is HTTP, HTML, SMTP, FTP, RTF or of any other type.[92]

Application layer

Often, the internet is misunderstood to be the WWW, but the latter is just an application of the internet, which allows users to "surf" through millions of websites.[93] Websites are documents created using HTML, one of the protocols mentioned above. The "surfing" through the WWW occurs because websites are interconnected via hyperlinks, which is the main element of HTML. Examples of other applications include e-mail, mobile apps, search engines and social media. All these applications are essential to today's functioning of e-commerce but they also raise regulatory challenges (see Table 2.1).

Content layer

While the previous layers might be invisible to internet users, it is in this layer that data packets can be interpreted as text, speech, music, pictures and videos and consumed by people.[94] Therefore, many policy issues may be associated with this layer (e.g., the regulation of harmful content, spam). Content in this layer is viewed through a policy lens applied by some agreed-upon authority.[95] In some cases, there might be regulations or laws against displaying harmful content; whereas in others, platforms would self-regulate what content they display.

[91] Yoo, 'Protocol Layering and Internet Policy', 1743.
[92] Solum and Chung, 'The Layers Principle: Internet Architecture and the Law', 14–15.
[93] Each application has a different set of standards, developed by organizations such as the World Wide Web Consortium (W3C) or the Moving Picture Expert Group (MPEG) for video and audio standards.
[94] Solum and Chung, 'The Layers Principle: Internet Architecture and the Law', 28.
[95] Vinton G. Cerf, 'The Upper Layers of the Internet', Communications of the ACM 61, no. 11 (November 2018), Last accessed June 23, 2020, https://cacm.acm.org/magazines/2018/11/232189-the-upper-layers-of-the-internet/fulltext.

INTERNET ARCHITECTURE AND E-COMMERCE – AN ILLUSTRATION

Internet architecture allows firms of all sizes to participate

The internet's open architecture and the reliance on technologies such as packet switching have transformed it from its original research-focused origin to a conduit for online everyday marketplaces. Indeed, e-commerce transaction comprises multiple transmission messages (data packets) between various agents (e.g., buyer, seller, platform providers, and logistics providers). In essence, it is a multiplication of the transmission of data packets between multiple end-points. Furthermore, by relying on the internet architecture, which does not require investments in the physical layer, business of any size are able to participate in global digital marketplaces (via the application layer), or can do so by relying in the outsourcing of otherwise costly processes, such as in-house data storage, now facilitated by cloud computing. Therefore, the outlook for greater e-commerce adoption depends ultimately on preserving the internet's open architecture.[96]

Internet architecture allows for new e-commerce applications

Moreover, the same layered architecture allows for new future applications. Its value will depend on precisely transmitting data packets in an open platform and the possibility of a wide adoption around the world. The growth of some leading tech companies can be attributed to these characteristics of the internet.

But, the internet's architecture also bring challenges

While the internet's openness is prominently accepted as positive, the wide adoption of the internet as a major channel for commerce has made necessary the discussion of challenges originating from the internet's very own architecture. For instance, the end-to-end nature of the internet has posed some security dilemmas that led to ongoing efforts to address them. As mentioned before, the internet's technical architecture allows any data packet to flow across the network, without special security safeguards. Accordingly, the burdens to keep the network safe and secure are placed at the end-points, not in the network itself. This can be challenging in a time of constant cyberattacks. Additionally, there are privacy and trust issues that need to be tackled in a way that respects the internet's open architecture, while at the same time, promotes innovation.

This poses questions on how to regulate without causing internet fragmentation, which could occur with respect to the technological underpinnings of the internet, government policies and commercial aspects.[97] For instance, technical fragmentation could "impede the ability of

[96] OECD, 'Economic and Social Benefits of Internet Openness', 36. Last accessed June 23, 2020, https://www.oecd-ilibrary.org/science-and-technology/economic-and-social-benefits-of-internet-openness_5jlwqf2r97g5-en.

[97] William J. Drake, Vinton G. Cerf, and Wolfgang Kleinwächter, 'Internet Fragmentation: An Overview', Future of the Internet Initiative White Paper (World Economic Forum (WEF), January 2016), 14–15, Last accessed June 23, 2020, http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

systems to fully interoperate and exchange data packets and of the Internet to function consistently at all end points". Certain government policies may "constrain or prevent certain uses of the Internet to create, distribute, or access information resources" and unregulated commercial practices could "constrain or prevent certain uses of the Internet to create, distribute or access information resources".[97] Discussions related to these challenges can be conceptualized within the layered architecture presented above.

Limitations of layering model

Although the layering model offers a good method to match the internet architecture with policy issues, it is not a prescriptive advice on how to regulate. The reason is that in some cases, policy issues can be cross-cutting and involve more than one layer (e.g., market access for goods and services). Additionally, the boundaries between layers can be unclear, and may change with technological developments. On top of that, there might be aspects that cannot be covered by the layered approach, but are important to e-commerce (e.g., trade facilitation). Despite all these shortcomings, for the purposes of simplification, a table summarizing how the different aspects currently being discussed at the WTO e-commerce negotiations match the internet's layered model is shown in Table 2.1 below.

Table 2.1: Layers of Internet's Structure and WTO e-commerce negotiations

<table>
<tr><th colspan="2">Technical layered models</th><th>Subjects and protocols</th><th colspan="2">Conceptual layered models</th><th>WTO e-commerce negotiations</th><th>Cross-cutting issues</th></tr>
<tr><td>OSI model</td><td>TCP/IP</td><td></td><td>CIGI (2016)</td><td>APEC (2016)</td><td></td><td rowspan="5">Goods and services market access, cybersecurity, network security</td></tr>
<tr><td rowspan="2"></td><td rowspan="3"></td><td rowspan="2"></td><td></td><td>Economic and social layers</td><td>Consumer protection, Open data</td></tr>
<tr><td rowspan="2">Content</td><td rowspan="2">Content</td><td rowspan="2">SPAM, Protection of Intellectual Property Rights (IPRs), Source code protection, Content regulations</td></tr>
<tr><td>Application</td><td>www, browser email, streaming media</td><td rowspan="3">Application</td><td rowspan="3">Application</td><td rowspan="3">Data protection, privacy, Cross border data flows Intermediary liability, Electronic authentication/ payment/ invoicing,</td></tr>
<tr><td>Presentation</td><td>DNS, SMTP, HTTP, FTP</td></tr>
</table>

Session					Principles on access to and use of internet for digital trade	
Transport	Transport	TCP, UDP				
Network	Internet	IP (e.g., IPv4, IPv6)	Logical	Logical		
Link	Link	Ethernet, Wi-Fi	Infrastructure	Infrastructure	Access, Telecom regulation, Costs, Server localization, Cross-border data flows	
		CSMA, async, sonet				
Physical		Copper, fiber radio				

Source: Author's elaboration based on: UNCTAD, 'Information Economy Report 2006: The Development Perspective', 2008.; Gloria Pasadilla et al., "Facilitating Digital Trade for Inclusive Growth: Key Issues in Promoting Digital Trade in APEC" (Singapore: APEC PSU 2016).

3 NEGOTIATIONS ON E-COMMERCE AT WTO

3.1 WTO PROGRAMME ON E-COMMERCE

The work on e-commerce at the WTO can be traced back to the 1998 WTO Geneva Ministerial Conference, where WTO members adopted the "Declaration on Global Electronic Commerce". [98] Recognizing that global e-commerce was growing and creating new opportunities for trade, the 1998 Declaration called on the WTO General Council (GC) to establish a "comprehensive work programme to examine all trade-related issues relating to the global electronic commerce". It also called upon members "to continue their current practice of not imposing customs duties on electronic transmissions". Furthermore, the 1998 Declaration defined "electronic commerce" as the production, distribution, marketing, sale or delivery of goods and services by electronic means.

Acknowledging the cross-cutting nature of e-commerce, the WTO GC established the framework for the work program, mandating the four councils – the Council for Trade in Goods (CTG), Council for Trade in Services (CTS), Council for Trade Related Aspects of Intellectual Property (TRIPS Council), and the Committee on Trade and Development (CTD) – to examine the treatment of e-commerce in their respective legal frameworks.[99]

Between 2001 and 2003, discussions which are centered on the cross-cutting issues took place. WTO members focused largely on: 1) the classification of content of electronic transmission, i.e., whether electronically transmitted products were goods or services; 2) development-related issues, such as the availability of certain technologies for a number of developing economies; and 3) fiscal implications of e-commerce, in particular, the long-term impact of the moratorium on electronic transmissions.[100] However, some of these issues did not play a significant role in the Ministerial Conferences following the establishment of the work programme: Doha in 2001; Hong Kong, China in 2005; Geneva in 2009 and 2011; Bali in 2013; and Nairobi in 2015.

Yet, some aspects have been discussed sporadically. For instance, electronically delivered software has been included in the Hong Kong, China Ministerial Conference in 2005 and in the Geneva Ministerial Conference in 2009. E-commerce from the perspective of development (e.g., access to e-commerce by MSMEs) were also discussed during the Geneva Ministerial Conference in 2011. The development dimension was reiterated by some members during the Bali Ministerial Conference in 2013, along with topical issues such as cloud computing, the protection of confidential data, privacy and consumer protection.

[98] WTO, 'Ministerial Declaration on Global E-Commerce 1998, Adopted by the General Council on 25 September 1998' (September 30, 1998).
[99] WTO, 'Work Programme on Electronic E-Commerce: Background Information by the Secretariat' (February 6, 2015).
[100] WTO, 'Dedicated Discussion on Electronic Commerce under the Auspices of the General Council on 15 June 2001: Summary by the Secretariat of the Issues Raised' (July 6, 2001).

The rapid development of the digital economy has spurred the interest of WTO members to reinvigorate discussions around e-commerce, beyond the aspects previously mentioned. After the Nairobi Ministerial Conference in 2015 and towards the Buenos Aires Ministerial Conference in 2017, some WTO members submitted different e-commerce proposals to the WTO GC. Moreover, during the Buenos Aires Ministerial Conference, a group of delegations[101] issued a joint statement putting on the table a proposal for exploratory works towards future WTO negotiations on trade-related aspects of e-commerce, with participation open to all WTO members.[102] In the same joint statement, WTO members also agreed to continue the Work Programme on Electronic Commerce established in 1998.

In 2018, different proposals were submitted to advance the objectives of the 2017 joint statement. Additionally, nine meetings were held during the same year to discuss trade-related aspects of e-commerce. A detailed analysis of only the publicly available proposals by WTO members during this time as well as the topics covered was developed by Garcia-Israel and Grollier.[103] Broadly, the discussion of the issues during 2018 encompassed four main themes: 1) enabling digital trade/e-commerce; 2) openness and digital trade/e-commerce; 3) trust and digital trade/e-commerce; and 4) cross-cutting issues, including development, transparency and cooperation.[104]

3.2 CURRENT WTO NEGOTIATIONS ON E-COMMERCE

Building upon previous discussions, on 25 January 2019, in the margins of the World Economic Forum in Davos, 76 WTO members (which account for 90 percent of global trade[105]) issued a joint statement confirming the intention to commence negotiations to put in place global rules on e-commerce. According to the 2019 joint statement, the negotiations "will seek to achieve a high standard outcome that builds on existing WTO agreements and frameworks with the participation of as many WTO Members as possible". The negotiation process is open to all WTO members interested in joining.

---

[101] Albania; Argentina; Australia; Bahrain; Brazil; Brunei Darussalam; Cambodia; Canada; Chile; Colombia; Costa Rica; European Union; Guatemala; Hong Kong, China; Iceland; Israel; Japan; Kazakhstan; Korea; Kuwait; Lao PDR; Liechtenstein; the former Yugoslav Republic of Macedonia; Malaysia; Mexico; Moldova; Montenegro; Myanmar; New Zealand; Nigeria; Norway; Panama; Paraguay; Peru; Qatar; Russian Federation; Singapore; Switzerland; Chinese Taipei, Penghu, Kinmen and Matsu; Turkey; Ukraine; United States; and Uruguay.

[102] WTO, 'Joint Statement on Electronic Commerce', WT/MIN(17)/60 (December 13, 2017), Last accessed June 23, 2020, https://www.wto.org/english/news_e/news17_e/minis_13dec17_e.htm.

[103] Garcia-Israel, Katya and Julien Grollier, 'Electronic Commerce Joint Statement: Issues in the Discussion Phase' (CUTS International, October 2019), Last accessed June 23, 2020, http://www.cuts-geneva.org/pdf/1906-Note-RRN-E-Commerce%20Joint%20Statement1.pdf.

[104] 'World Trade Organization Annual Report 2019' (Geneva, Switzerland: 2019), Last accessed June 23, 2020, https://www.wto.org/english/res_e/booksp_e/anrep19_e.pdf.

[105] Albania; Argentina; Australia; Bahrain, Kingdom of; Brazil; Brunei Darussalam; Canada; Chile; China; Colombia; Costa Rica; El Salvador; European Union; Georgia; Honduras; Hong Kong, China; Iceland; Israel; Japan; Kazakhstan; Korea; Kuwait, the State of; Lao PDR; Liechtenstein; Malaysia; Mexico; Moldova, Republic of; Mongolia; Montenegro; Myanmar; New Zealand; Nicaragua; Nigeria; Norway; Panama; Paraguay; Peru; Qatar; Russian Federation; Singapore; Switzerland; Chinese Taipei; Thailand; the former Yugoslav Republic of Macedonia; Turkey; Ukraine; United Arab Emirates; United States; and Uruguay.

Some likely issues to be negotiated as identified in public submissions are described within section 3.4 below. Many submissions remain restricted. Several aspects related to the current discussion on e-commerce draw from rules already adopted in previous free trade agreements (FTAs). The current WTO negotiations on e-commerce have also been endorsed in other forums. For instance, in June 2019, during the G-20 meeting in Japan, G-20 leaders launched the "Osaka Declaration on Digital Economy" to demonstrate the commitment of G-20 members to promote international policy discussions and rulemaking on trade-related aspects of e-commerce, inter alia, at the WTO.[106]

3.3 THE AGREEMENT IN SHORT

It is still early to discuss the exact nature and legal architecture of the agreement that would be the outcome of the e-commerce negotiations, especially in light of the current COVID-19 pandemic and the postponement of the negotiations. Yet, according to the 2019 joint statement, members have considered whether the agreement could take the form of a plurilateral trade agreement. This means, an issue-based agreement involving a set of WTO members, not all of them.[107] However, there are also submissions calling for a non-plurilateral agreement.[108]

3.4 LIKELY ISSUES TO BE NEGOTIATED (AS IDENTIFIED IN PUBLIC SUBMISSIONS)

Since the intention to begin negotiations on trade-related aspects of e-commerce were first announced in January 2019,[109] WTO members submitted various documents (e.g., in the form of joint communication, non-papers) to communicate the negotiating approach as well as elements that they believe should be included and discussed in the exploratory work and eventual agreement. In fact, some of these documents were dated as early as April 2018.[110]

As the objective of this project is to support the WTO negotiations, it is sensible to review submissions to determine the elements that are likely to be included. It is worthwhile to indicate that this section has only referred to a subset of submissions (i.e., publicly available information)

---

[106] G-20, 'Osaka Declaration on Digital Economy', n.d. Last accessed February 5, 2020, https://www.wto.org/english/news_e/news19_e/osaka_declration_on_digital_economy_e.pdf.

[107] A plurilateral agreement can be: (i) closed, meaning, accruing benefits only to those WTO members that are parties of the agreement, or (ii) a "critical mass" agreement negotiated by a subset of WTO members, whose benefits are extended to all members on a Most Favored Nation (MFN) basis. Specifically on the latter, a critical mass would imply that the agreement covers more than 80% of world trade, or that about 160 WTO members are part of it. See: Rudolf Adlung and Hamid Mamdouh, 'Plurilateral Trade Agreements: An Escape Route for the WTO?', WTO Staff Working Paper (World Trade Organization (WTO), Economic Research and Statistics Division, January 25, 2017), Last accessed February 5, 2020, https://doi.org/10.30875/cdf5e42c-en.

[108] INF/ECOM/49.

[109] WTO, 'Joint Statement on Electronic Commerce', WT/L/1056, (January 25, 2019), Last accessed February 5, 2020, https://trade.ec.europa.eu/doclib/docs/2019/january/tradoc_157643.pdf.

[110] WTO, 'Joint Initiatives', Last accessed 18 May 2020, https://docs.wto.org/dol2fe/Pages/FE_Browse/FE_B_009.aspx?TopLevel=10785#/.

because not all submissions are publicly available.[111] Correspondingly, there may be issues which are not covered. Nevertheless, several submissions noted the importance of ensuring that the negotiating agenda endeavors to be coherent, ambitious and comprehensive (i.e., covers all relevant aspects of e-commerce).[112] To avoid fragmentation, there is the view by some that it is imperative for members to build general and overarching international principles.[113] At the same time, some submissions also noted that considering the multi-layered nature of e-commerce and variation in members' interests, a flexible approach may be needed.[114] Besides suggesting that members be allowed to identify the components/elements that they are prepared to adopt, some submissions indicated that the negotiations should attempt to balance a reasonable/pragmatic level of ambition with due consideration given to members' right to regulate for different legitimate public policy objectives.[115]

While the opportunities and challenges faced by each member may be specific and dependent on multiple factors including its level of development and legal systems, a review of these submissions pointed to the inclusion of elements, which are similar and can be categorized into the focus areas below. However, the categorization is not intended to constrain discussions on any specific element to a particular area, but rather to organize information gleaned from the submissions. Despite the intent to delineate issues covered under each focus area, there are overlaps. For example, the issue of whether a certain form of electronic payment is permitted/regulated can be covered under 'electronic payment' as well as 'competition'. Similarly, the issue of personal data security can be covered under 'consumer protection', 'data protection and privacy', and 'cybersecurity/network security'. Submissions may also differ from each other with regards to the exact terms used. Last but not least, the elements indicated are not exhaustive and likely to be revised/updated as negotiations continue and more documents are released.

FOCUS AREA A: ELECTRONIC TRANSACTION FRAMEWORK

Electronic authentication (i.e. e-contract/e-signature/e-identification)

The nature of e-commerce means that any agreement between buyer and seller is likely to be agreed upon electronically. Elements required to prove the legality of a contract, such as signature and identity of the signatory, would have to be in electronic format as well. However, legal recognition of e-contracts (including electronic transferable records) and their elements varies across economies. For example, domestic legislation in some economies may still require a physical signature for all cases. As such, many submissions noted the importance of allowing contracts to be concluded electronically, and ensuring that e-contract as well as its elements have the same legal effects as their paper counterparts, including their admissibility

[111] The current section 3.4 has taken into consideration submissions made publicly available as of 26 June 2020.
[112] INF/ECOM/1, INF/ECOM/5, INF/ECOM/8, INF/ECOM/22
[113] INF/ECOM/4
[114] INF/ECOM/3, INF/ECOM/49
[115] INF/ECOM/19

as evidence in legal proceedings.[116] Some submissions also indicated the need to ensure that domestic frameworks for electronic contracting cohere with international best practices.[117] In addition, other submissions mentioned the importance of having e-authentication and trust services since they are essential to ensure the authenticity and integrity of online transactions among others.[118] Considering that e-authentication and digital certificates may be provided by foreign providers, several submissions advocated the usefulness of mutual recognition and interoperability.[119] Some submissions recommended that policies and regulations should not prohibit parties to an electronic transaction from mutually determining the appropriate electronic methods to be used (i.e., policies and regulations should be technology neutral).[120] Where members may specify that a certain standard/certification be used, it was suggested that such requirements be objective, transparent and non-discriminatory.[121]

Electronic payment

In contrast to cash payment, electronic payments are monetary transactions conducted over electronic networks. They constitute an integral part of e-commerce as they are usually offered as one possible payment option and in many cases, can be the only option available to potential buyers. From the perspective of sellers, being able to offer the preferred forms of payment to potential buyers could go a long way in increasing the conversion rate and securing the order. From the perspective of buyers, lack of preferred forms of payment may simply mean that they would be unable to pay for the products. There are many forms of electronic payment and related offerings, including mobile payments, e-money and e-wallets. In economies where the share of population having bank accounts and/or credit cards is low, popular forms of payment have included a mix of cash and electronic payments, where buyers make their purchases online and then head to nearby convenience stores or post offices to complete the transactions. With the developments and innovations in financial technologies (fintech), the boundaries of electronic payment continues to be stretched. Recognizing this, several submissions noted that regulations should be flexible (i.e., aim to promote innovation and ensure accessibility to various payment options), which is in line with the rapid advancement of technology and business models.[122] More specifically, some submissions indicated the importance of allowing non-discriminatory access to infrastructure and services necessary for operation of the payment systems as well as ensuring interoperability between different payment systems.[123] However, the fact that such payment systems are linked to the financial system requires that they are properly regulated to minimize the risks to businesses and consumers. In this regard, several

[116] INF/ECOM/3, INF/ECOM/6, INF/ECOM/10, INF/ECOM/14, INF/ECOM/17, INF/ECOM/19, INF/ECOM/22 INF/ECOM/25, INF/ECOM/27/Rev.1, INF/ECOM/34
[117] INF/ECOM/14, INF/ECOM/25, INF/ECOM/34
[118] INF/ECOM/14
[119] INF/ECOM/6, INF/ECOM/14, INF/ECOM/17, INF/ECOM/25, INF/ECOM/27/Rev.1, INF/ECOM/34
[120] INF/ECOM/10, INF/ECOM/22, INF/ECOM/25, INF/ECOM/27/Rev.1, INF/ECOM/34
[121] INF/ECOM/17, INF/ECOM/22, INF/ECOM/27/Rev.1, INF/ECOM/34
[122] INF/ECOM/4, INF/ECOM/17
[123] INF/ECOM/17

submissions noted that regulations should also ensure reliability, quality and safety of such options.[124]

Electronic invoicing

Timely payment of invoices is an important issue for sellers and businesses, particularly SMEs, because payment overdue may create cash flow challenges. Electronic invoicing (e-invoicing) has been offered as a possible solution because it allows for faster delivery, processing and payment of invoices. Besides being less expensive to process than paper invoices, the removal of manual handling also brings advantages such as fewer errors and minimizing the risk of fake or compromised invoices. Acknowledging this, several submissions indicated that it would be important for members to recognize e-invoicing standards, which would enhance the efficiency, accuracy and reliability of e-commerce transactions.[125] Noting that e-invoicing systems may differ between members, submissions mentioned about the need to share best practices, mutually recognize and encourage interoperability of various systems.[126] One way of doing so would be to base regulations pertaining to e-invoicing systems on international systems, guidelines and past recommendations (if any).

Trade facilitation

While digital technology and tools have facilitated e-commerce, a significant share of products (e.g., physical goods) are not digitally delivered. This means overcoming obstacles related to non-digital trade remains critical for the digital economy to operate efficiently. For example, similar to firms involved in traditional trade, e-commerce platforms and vendors may find it challenging to comply with complex border processes. Indeed, the popularity of e-commerce (where high volume, low value parcels are the norm) has made more pertinent the discussions on whether current practices, approaches and regulations are capable of responding. Recognizing this, submissions proposed various ways that trade facilitation can be improved.[127] One way is the use of free zones and customs warehouses to facilitate cross-border e-commerce.[128] Another is through paperless trading provisions where trade administration documents (e.g., phytosanitary certificates, the Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES) permits, airway bills) are available and accepted electronically.[129] Besides lowering financial costs, electronic exchange of data and documents between customs authorities can facilitate better risk assessment and expedite clearance of goods.[130]

---

[124] INF/ECOM/17
[125] INF/ECOM/25, INF/ECOM/36, INF/ECOM/41
[126] INF/ECOM/25, INF/ECOM/36, INF/ECOM/41
[127] INF/ECOM/1, INF/ECOM/5
[128] INF/ECOM/19
[129] INF/ECOM/2, INF/ECOM/6, INF/ECOM/14, INFECOM/15, INF/ECOM/17, INF/ECOM/19, INF/ECOM/27/Rev.1, INF/ECOM/27/Rev.1/Add.1, INF/ECOM/36
[130] INF/ECOM/15, INF/ECOM/25

A related consideration is that implementing single window systems to enable documents to be submitted concurrently to different agencies and other stakeholders, such as logistics service providers and port operators, minimizes resources and time.[131] Similarly, noting that there may be variations in single window systems between members, submissions encouraged the need to develop interoperability between systems.[132] The use of technology in trade facilitation features significantly in many submissions. For example, blockchain could ensure compliance with international and domestic legal requirements related to protection and confidentiality of exchanged data and information. Submissions also encouraged the use of technology to expedite clearance and release of goods. These include embedded technologies (e.g., sensors on vehicles), risk management technologies (e.g., data analytics, artificial intelligence) and non-intrusive cargo inspection technologies.[133]

Taxation and customs duties

Recognizing that taxation and customs duties increase costs and may have negative implications on transactions, WTO members have agreed not to impose customs duties on electronic transmissions since 1998. In terms of nature and procedures, however, this moratorium is temporary and has to be continually renewed (currently until the twelfth WTO Ministerial Conference). Thus, several submissions proposed that a permanent moratorium be agreed to provide greater certainty to businesses and consumers.[134] Specifically on de minimis (i.e., the value below which goods can be shipped into the economy before taxes and duties are assessed), some submissions noted the importance of having reasonable thresholds to facilitate the movement of packages across borders.[135]

FOCUS AREA B: OPENNESS AND CROSS-BORDER RELATED ISSUES

Cross-border data flows

Data plays an important role in different aspects of the e-commerce value chain. For merchandise sellers who are based overseas, it is likely that data and information pertaining to buyers would have to flow across borders to sellers for further processing (e.g., preparing of postal labels). For payment services providers, data is integral in every step involved in processing a transaction. Data analytics could lead to more targeted offerings. In such cases, sellers and/or platforms usually employ the services of centralized data analytics centres for efficiency reasons and to improve the accuracy of such analytics (which tend to increase with the number of available data points). Other uses of data analytics include detecting anomalies, combating fraud and providing enterprise solutions. However, economies may put in place requirements that restrict cross-border data flows (including data localization) for various

[131] INF/ECOM/15, INF/ECOM/27/Rev.1/Add.1
[132] INF/ECOM/27/Rev.1/Add.1
[133] INF/ECOM/27/Rev.1/Add.1
[134] INF/ECOM/2, INF/ECOM/5, INF/ECOM/6, INF/ECOM/10, INF/ECOM/14
[135] INF/ECOM/5

legitimate public policy objectives such as data protection and security. Noting that the GATS general and security exceptions may not address members' concerns regarding their right to regulate certain issues in the digital environment, some submissions proposed considering ways to address concerns which can lead to restrictions on data flows. These include issues pertaining to data privacy, jurisdiction and the ability to enforce domestic laws.[136] Moreover, submissions indicated the importance for members to reach agreement on principles to ensure secure and free flow of data.[137] Specifically, several submissions noted that any such agreement should balance the need to ensure that measures are least trade restrictive and at the same time, fulfil valid public policy objectives.[138]

Competition

Competition and competition-related policies constitute a critical aspect of e-commerce. For example, increased competition has tremendous impact on prices and coverage in the telecommunications sector, which is the backbone/supporting infrastructure for accessing e-commerce. Enhanced competition in other sectors such as banking/payment and logistics services can also lead to improved offerings at more competitive prices, hence lowering the costs of transactions. Additionally, competition is one the main drivers of business and technological innovation, enabling firms including those in e-commerce to enhance and improve their existing products and service quality, while developing new products and services. Specifically in the context of online platforms, submissions noted that there should be regulations to ensure that they do not abuse their market position.[139] There are also discussions among members on new approaches to competition policies covering issues such as data portability and non-discriminatory access.[140]

Principles on access to and use of internet for digital trade

Similar to how roads are built to allow people to move from one point to another, the internet allows data and information to be transmitted digitally from one point to another. In this regard, submissions noted the importance of ensuring that the internet should remain free and open for all legitimate commercial and development purposes. In other words, with some exceptions (e.g., domestic security or public interest), members should agree not to impose restrictions on access to any particular websites or services both domestically and across borders.[141] Network management rules regulate the internet. In this regard, some submissions indicated that suppliers responsible for the transmission, switching or routing should be responsible for preserving the stability, safety and functionality of the internet. In addition, some submissions

[136] INF/ECOM/3, INF/ECOM/17
[137] INF/ECOM/4, INF/ECOM/5, INF/ECOM/22
[138] INF/ECOM/9, INF/ECOM/17, INF/ECOM/25, INF/ECOM/27/Rev.1, INF/ECOM/34
[139] INF/ECOM/17, INF/ECOM/27/Rev.1
[140] INF/ECOM/3
[141] INF/ECOM/4, INF/ECOM/5, INF/ECOM/9, INF/ECOM/12, INF/ECOM/17, INF/ECOM/22, INF/ECOM/25, INF/ECOM/27/Rev.1., INF/ECOM/34

indicated that these suppliers should abide by the principle of network neutrality for all internet users (i.e., treat equally any data package without distinction on content, origin, destination, service, terminal or application).[142]

Intermediary liability, IP-related and online content related regulations[143]

The advent of e-commerce has made the protection of intellectual property rights (IPR) more pertinent yet challenging at the same time. As distribution channels have become available to almost everyone with internet access, it has become easier to illegally distribute copies of copyrighted materials and counterfeit products along with legal ones. Noting that intermediaries may not have specific knowledge or control of the products offered in their platforms, some submissions suggested that rules balance on one hand, the need to ensure rigorous and timely enforcement of IPR (which could include obligation of intermediaries to take down infringing content) and on the other hand, ensure that storing, processing or transmitting content does not make intermediaries legally liable.[144]

Not related to IPR enforcement, other issues related to IPR raised by some economies include: 1) a reference to the importance of increasing the level of transparency regarding remuneration of copyright and related rights;[145] 2) a suggestion for members to assert the principle that exceptions and limitations available in physical formats should also be made in the digital environment;[146] as well as 3) considering the relationship between the use of technological protection measures and the enjoyment of copyright limitations and exceptions.[147]

Beyond IPRs, many economies tend to have regulations to control the kind of information that can be accessed publicly. These are usually applicable to online media including e-commerce platforms, and enacted for valid public policy objectives such as domestic security, cultural sensitivities and moral reasons. However, noting that a free and open internet can enable users to take advantage of the wealth of information and services, a submission proposed that rules be established to ensure that governments do not arbitrarily block, filter or monitor online content, or require intermediaries to do so.[148]

Open data

Governments across the world are custodian of large amount of public data such as those on public transport, weather and other statistical information. Analysis of these data could promote

[142] INF/ECOM/3, INF/ECOM/12, INF/ECOM/17, INF/ECOM/22, INF/ECOM/27/Rev.1
[143] Note that issues such as disclosure of source codes, trade secrets and algorithms are discussed in Focus Area F on market access.
[144] INF/ECOM/5
[145] INF/ECOM/14, INF/ECOM/16, INF/ECOM/17
[146] INF/ECOM/16, INF/ECOM/17
[147] INF/ECOM/16, INF/ECOM/17
[148] INF/ECOM/17

innovation and lead to improved provision of services. Recognizing this, several submissions proposed that members facilitate public access and use of these data.[149] These can potentially include making them available in machine-readable, open formats that can be searched, retrieved, used and redistributed among others.

FOCUS AREA C: CONSUMER PROTECTION AND PRIVACY ISSUES

Consumer protection

Regardless of whether a transaction is conducted electronically or not, consumer protection is likely to feature prominently in the decision-making process of potential buyers. Indeed, consumer protection is arguably more important in e-commerce because there is often no face-to-face interaction between buyer and seller. Acknowledging this, submissions noted the importance of members putting in place regulations to protect online customers from fraudulent and deceptive commercial activities.[150] Some submissions also elaborated on the need to ensure that the level of protection should be commensurate with those provided for in other forms of transactions (e.g., offline) if not more.[151] Several submissions expanded on the definition of such activities, including making misrepresentations regarding the material qualities, price, suitability for purpose, quantity or origin of goods or services; advertising goods or services for supply without intention to supply; failing to deliver products or provide services to consumers after they have been charged; and charging or debiting consumers' financial, telephone or other accounts without authorization. Noting that e-commerce may be cross-border in nature, several submissions proposed the importance of cooperation between consumer protection agencies as well as other relevant agencies/bodies.[152] Furthermore, in the event that sellers are exposed to such activities, submissions indicated that it would be good for consumers to have access to effective mechanisms for redress.

Unsolicited commercial electronic messages/spam

Spam generally refers to unsolicited commercial messages sent to a large number of recipients or posted in a large number of places[153], although it should be noted that there is currently no agreed definition of spam. The nature through which spam is circulated (e.g., in the form of emails, text or multimedia messages, and voice calls) means that it may be associated with and have negative implications on e-commerce such as undermining consumer trust and confidence. In this regard, submissions proposed that members adopt measures to protect consumers from spam.[154] While the details would have to be worked out during the negotiations, these can

[149] INF/ECOM/4, INF/ECOM/5, INF/ECOM/14

[150] INF/ECOM/2, INF/ECOM/6, INF/ECOM/10, INF/ECOM/12, INF/ECOM/17, INF/ECOM/21, INF/ECOM/22, INF/ECOM/29, INF/ECOM/34

[151] INF/ECOM/12, INF/ECOM/17, INF/ECOM/19, INF/ECOM/21, INF/ECOM/25, INF/ECOM/27/Rev.1, INF/ECOM/29

[152] INF/ECOM/6, INF/ECOM/10, INF/ECOM/12, INF/ECOM/17, INF/ECOM/22, INF/ECOM/25, INF/ECOM/27/Rev.1, INF/ECOM/29, INF/ECOM/34

[153] Merriam-Webster, 'spam', accessed 2020. https://www.merriam-webster.com/dictionary/spam.

[154] INF/ECOM/2, INF/ECOM/6, INF/ECOM/10, INF/ECOM/14, INF/ECOM/17, INF/ECOM/19, INF/ECOM/22, INF/ECOM/25, INF/ECOM/27/Rev.1, INF/ECOM/29, INF/ECOM/34

potentially include requiring recipient's consent prior to sending direct marketing communications, providing consumers with the option to opt-in or out, making spam clearly identifiable, and/or providing recourse/redress mechanisms if applicable measures are not complied with by the senders.

Data protection and privacy

Data is critical in the digital economy, including in e-commerce. For example, from the perspective of platforms (and sellers by extension), accurate data about their customers allow orders to be delivered to the right individual and location. Data analytics also allows businesses to target offerings to the needs and preferences of customers, potentially increasing their likelihood of returning. From the perspective of buyers, data such as delivery addresses and credit card numbers constitute some of the information needed by sellers to process their orders. Having such information along with those pertaining to preferences and purchase histories in advance improves efficiency and makes for a smoother experience. However, the increasing dependency on data requires the information to be protected and secured because leakage can affect the economy significantly and have implications on customer trust. Recognizing this, several submissions called for a balanced approach towards data-related regulations and noted members' right to regulate for valid public policy objectives, such as adopting and maintaining regulations to protect personal information.[155] Acknowledging the variation in members' approach, submissions called for them to consider principles and guidelines of relevant international bodies, and to develop mechanisms to promote compatibility (i.e., interoperability), thereby reducing complexity to businesses.[156]

FOCUS AREA D: CYBERSECURITY/NETWORK SECURITY

Cybersecurity/network security

Cybersecurity incidents may affect the trust and confidence individuals have in e-commerce. Recognizing this, submissions mentioned the need for members to strengthen their capabilities to prevent and respond to such incidents.[157] Generally, cybersecurity-related regulations are aimed at ensuring that various stakeholders, including businesses, put in place a certain level of protection to minimize data leakage and safeguard its integrity. They may also include requirements such as contingency measures in the event of attacks and disasters, and access of information to law-enforcement agencies. However, noting that over-regulation may restrict trade and have negative implications on the economy, submissions proposed the value of adopting a risk-based approach to regulations.[158] It is worthwhile to indicate that while data privacy and security as well as network security/cybersecurity are discussed separately, the two issues often overlap. Indeed, while some economies have stand-alone regulations on network

[155] INF/ECOM/1, INF/ECOM/6, INF/ECOM/12, INF/ECOM/17, INF/ECOM/19, INF/ECOM/22, INF/ECOM/25, INF/ECOM/27/Rev.1, INF/ECOM/29, INF/ECOM/34, INF/ECOM/39
[156] INF/ECOM/17, INF/ECOM/25, INF/ECOM/27/Rev.1, INF/ECOM/34
[157] INF/ECOM/6, INF/ECOM/14, INF/ECOM/17, INF/ECOM/19, INF/ECOM/27/Rev.1
[158] INF/ECOM/5

security/cybersecurity, the privacy regulations in some economies can include cybersecurity requirements.

FOCUS AREA E: INFRASTRUCTURE-RELATED ASPECTS

Telecommunications

Telecommunications serve as the backbone infrastructure necessary to access the internet, which in turn allow individuals to access a range of services such as making and receiving digital payments, and using e-commerce as transaction channel. Despite individuals increasingly having access to telecommunications services and hence the internet, it remains out of reach to a significant share of the global population. For example, the International Telecommunication Union (ITU) indicated that only 53.6 percent (4.1 billion people) were using the internet, where access can be via a fixed or mobile network [159] Within APEC, the numbers were slightly higher with 63.2 percent of its population having internet access as of 2018.[160] Recognizing this, several submissions noted the importance to continue work on promoting connectivity and bridging the digital divide, and some pointed to having a competitive telecommunications sector as one possible step to achieving it. [161] Some submissions also indicated the value of members adopting and/or updating the WTO Telecommunication Reference Paper and its underlying components (such as those pertaining to competitive safeguards, interconnection, universal service, licensing and authorization, independent regulator, and allocation and use of scarce resources) into members' GATS schedule, and one member has proposed to add new components (e.g., essential facilities and resolution of disputes).[162]

FOCUS AREA F: MARKET ACCESS

Goods and services market access

Besides telecommunications services, there are other enabling services which can potentially contribute to the smooth functioning of the e-commerce value chain such as financial/payment, computer and logistics services. In addition, the end-to-end provision of services require wider market access. Noting these, several submissions indicated that negotiations should address market access commitments in wider range of services sectors as well. [163] Moreover, considering that services classifications which form the foundation of specific commitments

[159] ITU, 'New ITU data reveal growing Internet uptake but a widening digital gender divide', 5 November 2019, Last accessed June 23, 2020, https://www.itu.int/en/mediacentre/Pages/2019-PR19.aspx. For the detailed description of the statistics, please refer to: https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ITCMEAS-2014-PDF-E.pdf.

[160] APEC, '2019 APEC Economic Policy Report – Structural Reform and Digital Economy', 2019. Last accessed June 23, 2020, https://www.apec.org/-/media/APEC/Publications/2019/11/2019-APEC-Economic-Policy-Report/2019-AEPR---Full-Report.pdf.

[161] INF/ECOM/1, INF/ECOM/4, INF/ECOM/5, INF/ECOM/6, INF/ECOM/14, INF/ECOM/19, INF/ECOM/22

[162] INF/ECOM/3, INF/ECOM/5, INF/ECOM/12, INF/ECOM/14, INF/ECOM/22, INF/ECOM/43

[163] INF/ECOM/4, INF/ECOM/6, INF/ECOM/11, INF/ECOM/22

under GATS may not be fit for the digital economy, submissions indicated the need for members to look into this.[164]

Specifically on ICT-related goods, restrictions on access to key technologies, parts and components can be detrimental to the development of the digital economy including e-commerce. This is particularly so considering that devices such as mobile phones and computers constitute the hardware component that facilitate user access. In this regard, a submission noted that eliminating related tariffs would allow businesses and consumers to access technology at lower costs.[165] Submissions identified joining the WTO Information Technology Agreement and its expansion as one avenue to do so.[166]

In certain circumstances, governments may require access to proprietary information for valid public policy objectives. For example, some economies may require businesses to disclose proprietary information such as source codes, trade secrets and algorithms prior to granting market access. Several submissions recognized that while governments have the right to put in place regulations to achieve legitimate objectives, they should not mandate access to such information.[167] Moreover, some submissions proposed that members do not require or restrict the adoption of certain encryption standards and other technologies (i.e., members adhere to principle of technological neutrality) in their products.[168]

If not already specified in the respective focus areas and elements, implicit in the above discussions are the call from many submissions for members to ensure that laws, policies and regulations are transparent.[169] One submission specifically called for the consolidated negotiating text for this WTO process (i.e., the Joint Statement Initiative) to be made available publicly.[170] Some submissions noted that where possible, relevant stakeholders should be given the opportunity to comment on new and revised policies prior to implementation.[171] Submissions also indicated the value of making public and reporting on e-commerce related policies and regulations.[172] Finally, recognizing that there are variations in policies and regulations across members, some submissions mentioned that it would be useful to cooperate on various fronts, which include information exchange, interoperability and possibly, harmonization of policies and regulations.[173]

[164] INF/ECOM/5
[165] INF/ECOM/6
[166] INF/ECOM/11, INF/ECOM/34
[167] INF/ECOM/4, INF/ECOM/5, INF/ECOM/14, INF/ECOM/17, INF/ECOM/22, INF/ECOM/25, INF/ECOM/34
[168] INF/ECOM/4, INF/ECOM/5, INF/ECOM/17
[169] INF/ECOM/3, INF/ECOM/15, INF/ECOM/17, INF/ECOM/19, INF/ECOM/27/Rev.1, INF/ECOM/27/Rev.1/Add.1, INF/ECOM/34
[170] INF/ECOM/42/Rev.2
[171] INF/ECOM/15, INF/ECOM/17
[172] INF/ECOM/4, INF/ECOM/17
[173] INF/ECOM/4, INF/ECOM/17, INF/ECOM/19, INF/ECOM/27/Rev.1, INF/ECOM/29

4 STATE OF POLICIES, LAWS AND REGULATIONS AFFECTING E-COMMERCE TRANSACTIONS IN APEC ECONOMIES

This section provides an analysis by focus areas of the information collected in the database of laws and regulations. As indicated earlier in section 3.4, the categorization is not intended to constrain discussions of any specific element to a particular focus area, but rather to organize the information collected. Likewise, the issues covered here is an elaboration of those discussed in section 3.4, which has only referred to a subset of submissions made at the WTO (i.e., publicly available information). Correspondingly, there may be issues which are not covered. Moreover, information collected in the database may not be exhaustive despite PSU's best endeavors. As such, the analysis in this section may be constrained/limited by the database. Finally, due to the amount of information in the database, PSU seeks economies' understanding that not all can be accommodated in this section.

4.1 FOCUS AREA A: ELECTRONIC TRANSACTION FRAMEWORK

DIGITAL/E-COMMERCE STRATEGIES

Several APEC economies have introduced digital and digital-related strategies to foster the digital economy. Reflective of the cross-cutting nature of digital issues, these strategies tend to involve a whole-of-government approach, while also engaging stakeholders such as businesses, workers and consumers. In some economies, initiatives with implications on e-commerce are embedded within the wider strategies mentioned. However, there have also been cases where economies have introduced standalone strategies on e-commerce. This section provides a summary of some of these strategies.

Brunei Darussalam's Digital Government Strategy 2015 – 2020 has identified six programs, namely: 1) advancing digital services; 2) implementing universal access for government systems; 3) strengthening security; 4) enhancing stakeholder engagement; 5) optimizing digital assets; and 6) developing enterprise information management capability. While centered on leveraging digital technologies and tools to enhance public service delivery, there are elements that could have positive implications on e-commerce once fully implemented. For example, one of the potential outputs identified in the second program (on implementing universal access for government systems) is the development of One ID, a digital identification system for both citizens and businesses. This could lead to a more trusted digital space for consumers to engage in e-commerce transactions. Similarly, the digital management of government revenue collection proposed under the first program (on advancing digital services) could pave the way for greater adoption of e-invoicing, and hence further streamline online transactions.[174]

Canada's Digital Charter has identified ten principles to guide the government's work in harnessing digital and data transformation, namely: 1) universal access; 2) safety and security;

[174] Brunei Darussalam, 'Digital Government Strategy', Last accessed June 23, 2020, http://www.digitalstrategy.gov.bn/Themed/index.aspx.

3) control and consent; 4) transparency, portability and interoperability; 5) an open and modern digital government; 6) a level playing field; 7) data and digital for good; 8) strong democracy; 9) being free from hate and violent extremism; and 10) strong enforcement and real accountability. Specifically on the first principle of providing universal access, it has been noted that the 2019 Budget will deliver CAD5 to 6 billion in new investments towards building a connected Canada, where all Canadian homes and businesses would be connected to the internet with enhanced speeds of 50/10 Mbps by 2030.[175] When fully implemented, this initiative would allow more people to access digital solutions and tools, including e-commerce. On the third principle of control of data, the government is currently exploring how the privacy ecosystem can be modernized to provide Canadians with more confidence in taking advantage of digital opportunities, which may lead to greater participation in e-commerce as well.

Indonesia's E-Commerce Roadmap (2017 – 2019) has identified eight key areas to support the development of e-commerce in the Indonesian economy, namely: 1) funding; 2) taxation; 3) consumer protection; 4) education and human resources; 5) telecommunication infrastructure; 6) logistic; 7) cybersecurity; and 8) establishment of a coordinating function.[176] In addition, the separate Making Indonesia 4.0 Roadmap, which guides the economy's transition into the Fourth Industrial Revolution[177], has identified ten priorities, namely: 1) reforming material flow; 2) redesigning industrial zones; 3) embracing sustainability; 4) empowering SMEs; 5) building nationwide digital infrastructure; 6) attracting foreign investments; 7) upgrading human capital; 8) establishing an innovation ecosystem; 9) incentivizing technology investment; and 10) re-optimizing regulations and policies. Notably, priority 4 involves encouraging 3.7 million MSMEs to apply digitization technologies in their business activities,[178] which could then encourage MSMEs to expand into e-commerce markets. On a similar note, priority 9 involves the implementation of tax exemptions and subsidies for technological adoption.

In 2015, the United States highlighted a Digital Economy Agenda focused around opportunities like promoting trust online, ensuring access, and promoting innovation.[179] This is consistent with the 2018 U.S. National Cyber Strategy's goal of promoting an open, interoperable, reliable, and secure Internet.[180] Similarly, Chile's Digital Transformation Strategy (2018-2022)

[175] Canada, 'Canada's Digital Charter in Action: A Plan by Canadians, for Canadians', Last accessed June 23, 2020, https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00109.html.

[176] Indonesia, 'E-Commerce Roadmap (2017 – 2019)', Last accessed June 23, 2020, https://eoasis.rajahtann.com/eoasis/lu/pdf/2017-08-Indonesia_E-Commerce.pdf.

[177] The Fourth Industrial Revolution refers to how technologies like artificial intelligence, autonomous vehicles and the Internet of Things are merging with humans' physical lives, blurring the lines between physical and digital realms. (Source: https://www.cnbc.com/2019/01/16/fourth-industrial-revolution-explained-davos-2019.html).

[178] Indonesia, 'Making Indonesia 4.0 Roadmap', Last accessed June 23, 2020, https://www.kemenperin.go.id/download/19347.

[179] The United States, 'Digital Economy Agenda', Last accessed June 23, 2020, https://www.ntia.doc.gov/files/ntia/publications/alan_davidson_digital_economy_agenda_deba_presensation_051616.pdf.

[180] The United States, 'National Cyber Strategy', Last accessed June 23, 2020, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

recommends fostering digital inclusion through modernizing digital infrastructure, increasing digital literacy and enhancing the use of digital government services.[181]

Singapore's Digital Economy Framework for Action, launched in 2018, seeks to enable businesses to digitally transform, empower workers through new digital competencies, and create digitally connected ecosystems.[182] This plan is a key element that supports the Smart Nation vision and complements the 23 Industry Transformation maps, and outlines a plan of action to enhance Singapore's digital competitiveness and become a global node in Asia. It encourages private-public collaboration and partnership to strengthen local digital capabilities, deepen innovation and facilitate global access to the Digital Economy. The framework is focused around three pillars of growth, namely: 1) accelerate digital transformation of existing sectors; 2) grow Singapore's competitiveness by fostering new ecosystems enabled by digital; and 3) develop the next generation digital industry as an engine of growth.

The Philippines' E-Commerce Roadmap (2016 – 2020) sets the target of e-commerce contributing 25 percent to the economy's GDP by 2020. It specifies infrastructure, innovation, investment, information flow, intellectual capital and integration as priorities to achieve this target.[183] In Chinese Taipei, the Digital Nation & Innovative Economic Development Program 2017 – 2025 (DIGI+) focuses on developing digital innovation infrastructure and cultivating an innovation ecosystem that is digital economy-ready.[184] The second layer of DIGI+ further focuses on providing a facilitative regulatory environment for e-commerce. In China, the latest Five-year Development Plan (2016 – 2020) has a section dedicated to e-commerce, which aims to: 1) support development of e-commerce infrastructure; 2) promote innovation and adoption of e-commerce in key areas; and 3) promote development of comprehensive experimental zones for cross-border e-commerce in cities like Hangzhou.[185]

ELECTRONIC AUTHENTICATION (I.E. E-CONTRACT/E-SIGNATURE/E-IDENTIFICATION)

An increasing number of contractual agreements between buyers and sellers are being completed electronically. APEC economies generally recognize e-contracts as valid and enforceable like paper contracts through their domestic laws. In the event of contractual disputes, electronic records indicating formation of e-contracts are also admissible as evidence before the courts of APEC economies. For example, Singapore courts generally allow

[181] Chile, 'Digital Transformation Strategy (2018-2022)', Last accessed June 23, 2020, https://digital.gob.cl/doc/estrategia_transformacion_digital_2019_v1.pdf.

[182] Singapore, 'Digital Economy Framework for Action', Last accessed July 24, 2020, https://www.imda.gov.sg/-/media/Imda/Files/SG-Digital/SGD-Framework-For-Action.pdf.

[183] The Philippines, 'E-Commerce Roadmap (2016 – 2020)', Last accessed June 23, 2020, https://www.dti.gov.ph/trabaho/e-commerce/eco-news/dti-launches-ph-e-commerce-roadmap-2016-2020/.

[184] Chinese Taipei, 'Digital Nation & Innovative Economic Development Program 2017-2025 (DIGI+)', Last accessed June 23, 2020, https://www.digi.ey.gov.tw/en/cp.aspx?n=258274B98D400B77.

[185] China, 'Five-year Development Plan (2016 – 2020)', Last accessed June 23, 2020, https://en.ndrc.gov.cn/policyrelease_8233/201612/P020191101482242850325.pdf.

electronic records to be admitted as evidence indicating the formation of e-contracts electronically. However, electronic records alone may be insufficient to meet all the formality requirements for wills, negotiable instruments and disposition of interest in immovable property (whether by contract or otherwise).[186] In Hong Kong, China, the courts permit the admissibility of electronic records as evidence to prove the formation of e-contracts with similar exceptions as Singapore.[187]

Notwithstanding that contracts may be completed electronically, signatures remain a mandatory feature to prove the legality of contractual agreements. At the international level, the United Nations Commission on International Trade Law (UNCITRAL) has developed a model law on electronic signatures which can be used as a guide by any interested economy when developing their e-signature laws domestically (see Box 4.1 below). Specifically among APEC economies, analysis has shown that most APEC economies have laws regulating e-signatures.

E-signatures are usually affixed to data, for the purpose of authenticating content encapsulated in the data. In the context of e-commerce, such data may comprise of online completed forms and payment information[188]; as an illustration, a buyer making a purchase on an e-commerce platform may have perused multiple webpages when customizing his/her chosen product and choosing delivery options to receive the said product. To ensure finality in transactions, e-signature laws in several APEC economies including Canada;[189] China;[190] Indonesia;[191] Korea;[192] New Zealand;[193] Singapore;[194] and Viet Nam[195] impose a requirement for changes to such data to be detectable after entry of an e-signature.

[186] Singapore, 'Evidence Act', Last amended 1997, Section 116A, https://sso.agc.gov.sg/Act/EA1893.

[187] Hong Kong, China, 'Electronic Transactions Ordinance', Last amended 2017, Section 9, Last accessed June 23, 2020, https://www.elegislation.gov.hk/hk/cap553.

[188] Docusign, 'What are digital signatures', Last accessed June 23, 2020, https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq.

[189] Canada, 'Personal Information Protection and Electronic Documents Act', Last amended 2018, Section 48, Last accessed June 23, 2020, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/.

[190] China, 'Electronic Signature Law of the People's Republic of China', Last amended 2015, Article 13, Last accessed June 23, 2020, https://www.wipo.int/edocs/lexdocs/laws/en/cn/cn105en.pdf.

[191] Indonesia, 'Law Concerning Electronic Information and Transactions', Last amended 2016, Article 11, Last accessed June 23, 2020, https://www.whitecase.com/publications/alert/indonesian-electronic-information-and-transactions-law-amended.

[192] Korea, 'Act on the Consumer Protection in Electronic Commerce', Last amended 2016, Article 5, Last accessed June 23, 2020, https://elaw.klri.re.kr/eng_service/lawView.do?hseq=38513&lang=ENG.

[193] New Zealand, 'Contract and Commercial Law Act 2017', Last amended 2017, Section 226, Last accessed June 23, 2020, http://www.legislation.govt.nz/act/public/2017/0005/21.0/DLM6844033.html.

[194] Singapore, 'Electronic Transactions Act' Last amended 2011, Section 18, Last accessed July 13, 2020. https://sso.agc.gov.sg/Act/ETA2010.

[195] Viet Nam, 'Law on E-Transactions', Last amended 2001, Article 22, Last accessed June 23, 2020, https://www.wto.org/english/thewto_e/acc_e/vnm_e/WTACCVNM43_LEG_5.pdf.

Box 4.1: Model Law on Electronic Signatures (MLES)

The main elements

The MLES is directly derived from Article 7 of the UNCITRAL Model Law on Electronic Commerce, which states that where the law requires a signature from a person, that requirement is met by an electronic signature if:

1. The electronic signature identifies the signatory and indicates the signatory's approval of the information contained in the electronic signature, and
2. The electronic signature is as reliable as is appropriate for the purpose for which the electronic signature was generated or communicated, in light of all the circumstances, including any relevant agreement.

The MLES elaborates on the reliability of an electronic signature and its ability to indicate a signatory's approval of the information contained in an electronic signature.

The adoption process

Unlike an international convention, MLES as model legislation does not impose a requirement on members to notify UNCITRAL upon their enactment of the MLES, or domestic legislation influenced by the MLES. Furthermore, members have complete ambit to modify or leave out MLES provisions in incorporating the text of the model legislation into their legal systems. Among APEC economies, Australia; Brunei Darussalam; China; Malaysia; Peru; the Philippines; Thailand and Viet Nam have informed UNCITRAL of their adoption of the MLES.

Source:

- UNCITRAL, 'Guide to the Enactment of UNCITRAL Model Law on Electronic Signatures', https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures

Features of e-signature

In line with its purpose as a method of authentication, a valid e-signature would need to meet certain requirements that are generally stated in the e-signature laws of APEC economies. For example, the e-signature laws of Australia[196]; Canada[197]; Indonesia[198]; New Zealand[199]; and

[196] Australia, 'Electronic Transactions Act 1999', Last amended 2011, Section 10, Last accessed June 23, 2020, https://www.legislation.gov.au/Details/C2011C00445.

[197] Canada, 'Personal Information Protection and Electronic Documents Act', Last amended 2018, Section 48, Last accessed June 23, 2020, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/.

[198] Indonesia, 'Law Concerning Electronic Information and Transactions', Last amended 2016, Article 11, Last accessed June 23, 2020, https://www.whitecase.com/publications/alert/indonesian-electronic-information-and-transactions-law-amended.

[199] New Zealand, 'Contract and Commercial Law Act 2017', Last amended 2017, Section 226, Last accessed June 23, 2020, http://www.legislation.govt.nz/act/public/2017/0005/21.0/DLM6844033.html.

Thailand[200] require that an e-signature should identify the signatory and indicate the signatory's intention in respect of data communicated, while being appropriate for its purpose. Specific stipulations, such as signatories having sole control over the technology or process used to associate e-signatures to data and hence the power or ability to share data, have been made as part of this requirement in the e-signature laws of the economies stated.

Another requirement is as to the form of e-signatures. In Brunei Darussalam, e-signatures are defined as letters, characters, numbers or other symbols in digital form associated with an electronic record, and executed with the intention of authenticating electronic records.[201] In the United States, an e-signature refers to an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.[202] Similarly, an e-signature in Hong Kong, China, can be constituted by any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted for the purpose of authenticating or approving the electronic record.[203]

Additionally, e-signature laws of various APEC economies require potential e-signature recipients to be engaged prior to, or during its use. In Hong Kong, China, for example, the recipient's consent would have to be sought regarding the method used by the signatory to provide the e-signature.[204] In the Philippines, the recipient should be authorized and able to verify the signatory's e-signature before deciding whether to proceed with the transaction.[205] Whereas in Malaysia, the recipient should be made aware if the signatory has either breached a duty as a subscriber, or unlawfully held onto the private key used to affix the digital signature.[206]

Simple versus enhanced e-signatures

The terms 'e-signature' and 'digital signature' are often used interchangeably in the laws of APEC economies. However, within the laws on e-signatures/digital signatures in APEC economies, a distinction between simple and enhanced e-signatures/digital signatures has

[200] Thailand, 'Electronic Transactions Act (2001)', Last amended 2019, Section 4, Last accessed June 23, 2020, https://www.bot.or.th/English/PaymentSystems/OversightOfEmoney/RelatedLaw/Documents/et_act_2544_Eng.pdf.
[201] Brunei Darussalam, 'Electronic Transactions Act 2001', Last amended 2008, Section 2, Last accessed June 23, 2020, http://www.agc.gov.bn/AGC%20Images/LOB/PDF/Electronic%20Transactions%20(chp.196).pdf.
[202] The United States, 'Electronic Signatures in Global and National Commerce Act', Last amended 2000, Section 106, Last accessed June 23, 2020, https://www.govinfo.gov/content/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf.
[203] Hong Kong, China, Electronic Transactions Ordinance', Last amended 2017, Section 2, Last accessed June 23, 2020, https://www.elegislation.gov.hk/hk/cap553.
[204] Hong Kong, China, 'Electronic Transactions Ordinance', Last amended 2017, Section 6, Last accessed June 23, 2020, https://www.elegislation.gov.hk/hk/cap553.
[205] The Philippines, 'Institutionalising the Certification Scheme for digital signatures and directing the application of digital signatures in e-government services', Last accessed June 23, 2020, https://www.officialgazette.gov.ph/2009/06/15/executive-order-no-810-s-2009/.
[206] Malaysia, 'Digital Signature Act 1997', Last amended 2006, Section 62, Last accessed June 23, 2020, http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20562.pdf.

consistently been made. Generally, the enhanced versions of e-signatures/digital signatures embed Public Key Infrastructure (PKI) into the signing process to enable identification of both the recipient and signatory through the generation of two long numbers known as a private key and a public key. In practice, what this usually means is that the recipient and signatory must have a registered digital certificate issued by an approved certification service provider.[207]

For example, in Russia, a simple e-signature entails the use of codes, passwords or other means to confirm the fact of formation of e-signatures, whereas the enhanced e-signature (known as a 'qualified e-signature' in the translated Russian e-signature law) refers to an e-signature that has a qualified certificate and conforms to additional security requirements. In Hong Kong, China, only a simple e-signature is required to be attached to, or logically associated with, an electronic record for the purpose of identifying a signatory and indicating the signatory's authentication or approval of the information contained in the form of the electronic record.[208] On the other hand, the use of an enhanced e-signature (known as a 'digital signature' in the e-signature law of Hong Kong, China) must be supported by a recognized certificate, generated within the validity of that certificate, and used in accordance with the terms of that certificate.[209] Whereas in the Philippines, enhanced e-signatures appear to be required whenever e-signatures are permitted as a substitute for paper-based signatures, given that its e-signature law requires all e-signatures to use a digital certificate.[210]

Economies generally distinguish certification/authentication service providers approved to certify the e-signatures into two categories, namely: local service providers and foreign service providers. Specifically for the latter category, some economies have included provisions in their laws and regulations to recognize foreign certification/authentication service providers. For example, Brunei Darussalam's e-signature law indicates that the Minister of Finance may recognize certification authorities outside Brunei Darussalam that satisfy certain prescribed requirements published in the Government Gazette.[211] Peru's e-signature law states that certificates issued by foreign providers shall have the same legal validity and effectiveness, provided such certificates are recognized by the competent administrative authority.[212] In Chinese Taipei, the relevant e-signature law notes that under the principles of reciprocity and equivalent secure requirements, a certificate issued by a foreign certification service provider shall be equivalent to the one issued by a domestic certification service provider, provided that

[207] Docusign, 'Understanding digital signatures', Last accessed June 23, 2020, https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq.
[208] Hong Kong, China, 'Electronic Transactions Ordinance', Last amended 2017, Section 6, Last accessed June 23, 2020, https://www.elegislation.gov.hk/hk/cap553.
[209] Hong Kong, China, 'Electronic Transactions Ordinance', Last amended 2017, Section 6, Last accessed June 23, 2020, https://www.elegislation.gov.hk/hk/cap553.
[210] The Philippines, 'Republic Act No. 8792: An Act Providing for the Recognition and Use of Electronic Commercial and Non-Commercial Transactions and Documents', Last accessed June 23, 2020, https://www.gppb.gov.ph/laws/laws/RA_8792.pdf.
[211] Brunei Darussalam, 'Electronic Transactions Act', Last amended 2008, Article 43, Last accessed June 23, 2020, http://www.agc.gov.bn/AGC%20Images/LOB/PDF/Electronic%20Transactions%20(chp.196).pdf.
[212] Peru, 'Digital Signatures and Certificates Law (Law 27269)', Last amended 2011, Article 11, Last accessed June 23, 2020, https://www.certificadodigitalsunat.com/ley-27269-ley-firmas-certificados-digitales-peru/.

the foreign certification service provider has been permitted by the competent administrative authority as well.[213]

Besides the use of e-signatures or digital signatures, another method of authentication would be digital identification (see Box 4.2), which is at various stages of development in several APEC economies.

Box 4.2: Digital Identification

Digital identification (digital ID) refers to the digital representation of an individual or entity through the consolidation of various attributes, that allow the individual or entity to be sufficiently distinguished within a digital context. Such attributes can range from basic details like an individual's birth-related information and social security number, to more composite data sets like his/her online search behavior.

While the main objective for the conception of digital ID is usually to facilitate and improve the efficiency of public service delivery by governments, a robust digital identity framework may have positive externalities on the e-commerce ecosystem. For instance, digital ID systems may increase the overall security of electronic transactions. By providing an alternative means of authentication for potential consumers, it also increases the accessibility of digital solutions, including e-commerce, to a wider segment of the society. Many APEC economies have implemented, or are in the midst of implementing, their digital ID regulations and related initiatives. These economies include Australia; Brunei Darussalam; Chile; Hong Kong, China; Indonesia; Japan; Malaysia; Mexico; Peru; Philippines; Chinese Taipei and Thailand.

Sources:

- McKinsey, 'Digital identification: A key to inclusive growth", Last accessed June 23, 2020. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth
- Australian Government Digital Transformation Agency, 'Digital Identity', Last accessed June 23, 2020, https://www.dta.gov.au/our-projects/digital-identity
- Brunei Darussalam Government, 'Digital Government Strategy', Last accessed June 23, 2020, http://www.digitalstrategy.gov.bn/Themed/index.aspx
- Gob Digital Chile, 'Estrategia de Transformacion Digital del Estado', Last accessed June 23, 2020, https://digital.gob.cl/doc/estrategia_transformacion_digital_2019_v1.pdf
- Hong Kong, China's Gov HK, 'Electronic Authentication and Digital Certificates', Last accessed June 23, 2020, https://www.gov.hk/en/residents/communication/infosec/digitalcert.htm
- Indonesia, 'Regulation about requirements and procedures for population registration and civil recording', Last accessed June 23, 2020, https://setkab.go.id/wp-content/uploads/2018/10/Perpres-Nomor-96-Tahun-2018-2.pdf
- Morinobu Shigeki, 'My Number: Portal to a Digital Society', Last accessed June 23, 2020, https://www.nippon.com/en/currents/d00201/my-number-portal-to-a-digital-society.html

[213] Chinese Taipei, 'Electronic Signatures Act', Last amended 2001, Article 15, Last accessed June 23, 2020, https://law.moj.gov.tw/ENG/LawClass/LawHistory.aspx?pcode=J0080037

- Malaysia's MyGovernment, 'National Digital Identity Initiative', Last accessed June 23, 2020, https://www.malaysia.gov.my/portal/content/30592
- World Bank Group, 'ID4D Country Diagnostic', Last accessed June 23, 2020, http://documents.worldbank.org/curated/en/886301524689452577/ID4D-Country-Diagnostic-Mexico.pdf
- Peru, 'Legislative Decree No. 1412', Last accessed June 23, 2020, https://cdn.www.gob.pe/uploads/document/file/353216/decreto-legislativo-que-aprueba-la-ley-de-gobierno-digital-decreto-legislativo-n-1412-1691026-1.pdf
- The Philippines, 'Republic Act No. 11055', Last accessed June 23, 2020, https://psa.gov.ph/system/files/kmcd/RA11055_PhilSys.pdf
- Thailand, 'Amendment to the Electronic Transaction Act (No. 4)', B.E. 2562 (2019), Last accessed June 23, 2020, https://www.bakermckenzie.com/en/insight/publications/2019/04/amendment-to-thai-electronic-transaction-act
- Taipei Times, ' Electronic ID cards to be released in October 2020', Last accessed June 23, 2020, https://www.taipeitimes.com/News/taiwan/archives/2019/05/17/2003715282

ELECTRONIC PAYMENT (E-PAYMENT)

Many APEC economies have laws and regulations affecting e-payments, either directly or indirectly. Oftentimes, there is no single e-payments law to speak of, but rather "patchwork quilts" of legislation operating synergistically to regulate e-payments. Such "patchwork quilts" result from among others, the need for secondary legislation to implement primary legislation, as well as the cross-cutting nature of e-payments.

The term 'e-payment' arguably covers all non-physical financial transactions. However, for the purpose of the laws and regulations of APEC economies, it is worthwhile to note that e-payments are defined to varying levels of specificity. Some economies have adopted a fairly broad definition of e-payment, although they may refer to it in other terms such as 'payment system', 'payment instrument' and 'electronic funds transfer'. For example, Brunei Darussalam[214], Malaysia[215] and the Philippines[216] define 'payment instrument' broadly as any instrument, whether tangible or intangible, that enables the transfer of funds. Thailand's e-payment law defines 'payment system' as any arrangement for the transfer of funds, clearing or settlement.[217] The United States defines 'electronic funds transfer' as a transfer of funds that is initiated through an electronic terminal, telephone, computer (including on-line banking) or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer's account; a non-exhaustive list of examples includes point-of-sale transfers, automated teller machine transfers, transfers initiated by telephone, and transfers resulting from debit card transactions.[218]

[214] Brunei Darussalam, 'Payment and Settlement Systems (Oversight) Order 2015', Last amended 2015, Section 2, Last accessed June 23, 2020, http://www.agc.gov.bn/AGC%20Images/LAWS/Gazette_PDF/2015/EN/S036.pdf.

[215] Malaysia, 'Financial Services Act 2013', Last amended 2013, Section 2, Last accessed June 23, 2020, https://www.bnm.gov.my/documents/act/en_fsa.pdf.

[216] The Philippines, 'National Payment System Act', Last amended 2018, Section 4, Last accessed June 23, 2020, https://www.officialgazette.gov.ph/downloads/2018/10oct/20181030-RA-11127-RRD.pdf.

[217] Thailand, 'Payment System Act', Last amended 2018, Chapter 2, Last accessed June 23, 2020, https://www.bot.or.th/English/PaymentSystems/PSA_Oversight/Pages/default.aspx.

[218] The United States, 'Regulation E, Electronic Fund Transfer Act, 12 C.F.R. 1005 (2009)', Last accessed September 18, 2020, https://www.federalreserve.gov/boarddocs/supmanual/cch/efta.pdf.

Box 4.3: E-payments and COVID-19

While e-payments have already been gaining traction in recent years, the COVID-19 pandemic has been a major catalyst for a surge in its use as a means of transacting between parties. The contactless nature of e-payments assuages concerns about virus transmission through physical cash transactions, while also circumventing the inability of people to withdraw cash in APEC economies that have imposed lockdown measures.

Reflecting virus transmission concerns, China, Korea and the United States have implemented "quarantine" policies for banknotes, keeping them in safes for a duration equivalent to the incubation period of the virus before release into circulation. In Singapore, a major bank, DBS, has reported a significant decline in cash withdrawals and a corresponding increase in e-payment transactions, likely resulting both from people's inability to access bank branches physically, and reduced frequency of cash replenishment during the "circuit-breaker" partial lockdown period.

Additionally, the closures of brick-and-mortar shops, as part of containment measures across economies, have led consumers to turn to e-commerce as an alternative means to carry out their purchases of both essential and non-essential items. Accordingly, the rise in volume of e-commerce transactions has also precipitated the increased use of e-payments. As a case in point, DBS has also noted the doubling of cashless transactions in Singapore through its various e-payment applications from January to March 2020, as compared to the same period in 2019. In Malaysia, the use of contactless payments and adoption of e-wallets have similarly been on the rise, with some e-payment players seeing subscriber numbers double in April 2020 alone. Even in economies where the existing share of non-cash payments is significant, such as Korea (54.9 percent in 2019), COVID-19 is expected to further accelerate the adoption of e-payments.

Sources:

- Forbes, 'COVID-19 accelerated e-commerce growth '4 to 6 years'', Last accessed June 23, 2020, https://www.forbes.com/sites/johnkoetsier/2020/06/12/covid-19-accelerated-e-commerce-growth-4-to-6-years/#4c79184600fa
- Forbes, 'WHO Encourages Use of Contactless Payments due to COVID-19', Last accessed June 23, 2020, https://www.forbes.com/sites/rogerhuang/2020/03/09/who-encourages-use-of-digital-payments-due-to-covid-19/#3142cfaa41eb
- GlobalData, 'COVID-19 will further push non-cash payments in South Korea', Last accessed June 23, 2020, https://www.globaldata.com/covid-19-outbreak-will-further-push-non-cash-payments-in-south-korea/
- The Straits Times, 'More people go cashless, e-payment volume soars amid COVID-19 crisis', Last accessed June 23, 2020, https://www.straitstimes.com/tech/more-people-go-cashless-e-payment-volume-soars-amid-covid-19-crisis
- The Straits Times, 'Coronavirus pandemic has steepened adoption curve of e-wallets in Malaysia', Last accessed June 23, 2020, https://www.straitstimes.com/asia/se-asia/coronavirus-pandemic-has-steepened-adoption-curve-of-e-wallets-in-malaysia

Notwithstanding the variations in definition, the basic mechanics of e-payments are fairly similar across the range of available options. Three main groups of stakeholders are usually involved, namely: 1) users/consumers; 2) businesses/merchants; and 3) service providers (e.g., banks, third-party organization). Payments are transferred from the first group (i.e., users/consumers) to the second group (i.e., businesses/merchants) through the facilitation of service providers. In this regard, one of the objectives of laws and regulations affecting e-payments is to ensure the propriety of such transfers.[219]

Consumer protection in e-payments

Specifically on consumer protection provisions in e-payment laws, such provisions can generally be grouped into the two broad categories of "pre-transaction" and "post-transaction" provisions. Examples of "pre-transaction" provisions can be found in the e-payment law of Chinese Taipei, which requires service providers to furnish details of their consumer protection measures in "internal business guidelines and business procedure" (a document that service providers have to submit as part of their process of obtaining approval to provide e-payment services).[220] In Indonesia, the relevant e-payment regulation lists certain consumer protection principles that have to be adhered to by service providers when dealing with transactions, including fairness and reliability, transparency, protection of consumer data/ information and effective handling and settlement of complaints.[221] Whereas in Peru, the e-payment law prohibits merchants from requiring consumers to pay additional amounts that go beyond the prices already fixed through an e-payment system.[222]

An example of a "post-transactions" provision can be seen in Australia's e-payment law, which provides timelines for complaint procedures initiated by consumers; a service provider must either complete the investigation and advise the user of the outcome in writing, or advise the consumer of the need for more time to complete its investigation in writing within 21 days of receiving a complaint from a consumer.[223] Canada's e-payment regulation requires service providers to make replacement payments to intended recipients if payments have yet to reach them by the payment date.[224]

---

[219] Corvus Pay, 'The stakeholders and the transaction flow in e-commerce', Last accessed June 23, 2020, https://www.corvuspay.com/en/blog/2018/09/19/the-stakeholders-and-the-transaction-flow-in-ecommerce/.

[220] Chinese Taipei, 'The Act Governing Electronic Payment Institutions', Last amended 2018, Article 10, Last accessed June 23, 2020, https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=G0380237.

[221] Indonesia, 'Bank Indonesia Regulation No. 18/40/PBI/2016 Concerning Operation of Payment Transaction Processing', Last amended 2016, Article 24(2), Last accessed June 23, 2020, https://eservice.insw.go.id/files/ecommerce/7.%20Regulation%20of%20BI%20No%2018.40.PBI.2016%20on%20Concerning%20the%20implementation%20of%20payment%20transaction.pdf.

[222] Peru, 'Consumer Protection and Defense Code (Law No. 29571)', Last amended 2010, Last accessed June 23, 2020, https://www.indecopi.gob.pe/documents/20195/177451/CodigoDProteccionyDefensaDelConsumidor[1].pdf/934ea9ef-fcc9-48b8-9679-3e8e2493354e.

[223] Australia, 'ePayment Code', Last amended 2016, Section 38(4), Last accessed June 23, 2020, https://download.asic.gov.au/media/3798542/epayments-code-published-29-march-2016.pdf.

[224] Canada, 'Electronic Payments Regulations SOR/98-129', Last amended 1998, Section 7, Last accessed June 23, 2020, https://laws-lois.justice.gc.ca/eng/regulations/sor-98-129/page-1.html.

In the event of unauthorized transactions, e-payment laws of APEC economies usually have provisions to assign liability for losses between buyers, sellers and service providers. As a case in point, Australia's e-payment law provides a list of circumstances where users will not be liable for losses arising from unauthorized transactions. These include, among others, the use of a forged, faulty, expired or cancelled device, identifier or pass code; transactions performed after the service provider has been informed about the misuse/lost of a device; or the breach security of passcode security.[225] Whereas in Korea, the e-payment law provides that the service provider shall be liable for indemnifying the user for the loss if it is due to 1) forgery/alteration of means of access; or 2) an incident caused in the course of electronically transmitting/processing conclusion of a contract or transaction request among others.[226]

Provisions on dispute resolution regarding e-payments exist in some laws and regulations. In Japan for example, a list of designated dispute resolution organizations to which stakeholders can turn has been prescribed.[227] In Australia, users who are unsatisfied with the outcome of their complaint (as mentioned previously in the discussion of "pre-transaction" provisions) may then escalate their dispute through an external dispute resolution scheme, such as the Financial Ombudsman Service or the Credit and Investments Ombudsman, provided the service provider belongs to such a scheme.[228] Russia's federal e-payment law states that a service provider should provide for the possibility of pre-trial and/or arbitration settlement of disputes between payment system participants and payment infrastructure service providers, in accordance with the payment system rules.[229]

To ensure that provisions can be enforced, APEC economies have sections in their laws and regulations prescribing powers of oversight and enforcement to specific government institutions, in most cases, their central banks. Specifically in the area of supervision for example, Bangko Sentral ng Pilipinas is conferred with supervisory and regulatory powers for the purpose of ensuring the stability and effectiveness of the monetary and financial system. It also has the authority to issue directives to e-payment participants, and to request e-payment service providers to provide reports on their operations and activities.[230] On consumer protection, the Monetary Authority of Singapore is empowered to issue notices in writing to e-payment participants to comply with its e-payments law, if it deems such a notice necessary for the protection of consumers or in the interest of the public or a section of the public; for

[225] ibid 67.

[226] Korea, 'Electronic Financial Transactions Act', Last amended 2013, Article 9, Last accessed June 23, 2020, https://www.fsc.go.kr/downManager?bbsid=BBS0085&no=106341 .

[227] Japan, 'Payment Services Act', Last amended 2009, Articles 99 to 101, Last accessed June 23, 2020, http://www.japaneselawtranslation.go.jp/law/detail/?id=3078&vm=02&re=02.

[228] ibid 67.

[229] Russia, 'Federal Law of the Russian Federation On Digital Signatures (No.63)', Last amended 2016, Last accessed June 23, 2020, https://cis-legislation.com/document.fwx?rgn=32989.

[230] The Philippines, 'National Payment Act', Last amended 2018, Sections 5 and 6, Last accessed June 23, 2020, https://www.officialgazette.gov.ph/downloads/2018/10oct/20181030-RA-11127-RRD.pdf.

ensuring the integrity and proper management of a designated payment system; or for ensuring the integrity of the e-money stored in a payment account.[231]

Fintech regulatory sandboxes

To further encourage the development and adoption of newer technologies in the payment sector, some APEC economies have introduced fintech regulatory sandboxes, a regulatory approach of allowing time-bound testing of innovations under a regulator's oversight. Therefore, fintech regulatory sandboxes allow the testing of technology-enabled financial products and services under a controlled set of rules, supervisory requirements and safeguards, in preparation for such products and services being regulated under formal regulatory frameworks eventually.[232]

For example, the regulatory sandbox in Australia is designed to allow businesses to test products and services without holding the usual Australian financial services license or Australian credit license.[233] In Hong Kong, China, banks licensed and regulated by the Hong Kong Monetary Authority (HKMA) can apply to launch pilot trials of new Fintech initiatives in the HKMA's Fintech Supervisory Sandbox, while, firms licensed by the Hong Kong Securities and Futures Commission (SFC) and start-up firms that intend to be licensed by the SFC may apply to be in another sandbox operated by the SFC. Finally, insurers authorised by the Hong Kong Insurance Authority (IA) can make applications under the IA's insurtech sandbox. The relevant regulatory/supervisory sandboxes are also linked up, meaning that if a firm in Hong Kong, China intends to conduct a pilot trial of a cross-sector fintech product, it may apply for the most appropriate sandbox and the relevant regulator will be the primary point of contact for liaising with the other regulators so that the firm can access the other sandboxes concurrently.[234]

Any registered financial technology operator (FTO) in Indonesia can apply to be placed in the regulatory sandbox. While the Bank of Indonesia reserves the right to impose other criteria in determining which FTOs and their corresponding products, services, and technologies may be placed in the sandbox, FTOs targeted by the sandbox include those with activities involving services, technology or financial business models that are non-exclusive and beneficial to the society.[235] Besides exempting financial institutions and fintech companies from specific

---

[231] Singapore, 'Payment Services Act 2019', Last amended 2019, Section 102, Last accessed June 23, 2020, https://sso.agc.gov.sg/Acts-Supp/2-2019/Published/20190220?DocDate=20190220.

[232] Economic Times, 'Regulatory Sandbox and Fintech Innovation', Last accessed June 23, 2020, https://economictimes.indiatimes.com/markets/stocks/news/regulatory-sandbox-and-fintech-innovation/articleshow/69107031.cms?from=mdr.

[233] Australia, 'Australia extends fintech sandbox remit after long wait', Last accessed June 23, 2020, https://www.finextra.com/newsarticle/35275/australia-extends-fintech-sandbox-remit-after-long-wait.

[234] Hong Kong, China, 'Fintech Supervisory Sandbox', https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech/fintech-supervisory-sandbox-fss/.

[235] Indonesia, 'BI introduces FinTech 'sandbox' to support innovation', https://id.rajahtannasia.com/media/2990/ahpclientupdate-2january2018.pdf.

regulations during the sandbox duration, Bank Negara Malaysia provides the opportunity for participating firms to engage and share information on the technological services that may help shape a more practical regulatory framework in future.[236]

In the Philippines, the Securities and Exchange Commission regulates aspects of fintech operations that have to do with cryptocurrency and related activities, while the Bangko Sentral ng Pilipinas regulates fintech activities consisting of mobile financial services (including mobile-lending activities, and money or value-transfer services). Both have maintained a relatively open approach to firms or entities seeking to conduct pilot testing of fintech products or services not otherwise regulated under prevailing legislation under a quasi-regulatory sandbox regime.[237] In Thailand, the regulatory sandbox has also been used as a testing ground for technologies that could find wide application in the traditional banking sector such as biometric technology for electronic know your customer (KYC) processes.[238]

The Monetary Authority of Singapore (MAS) has two types of sandboxes. The FinTech regulatory sandbox was launched in 2016[239] while Sandbox Express was set up in 2019 to enhance the overall sandbox approach.[240] Both were set up to strengthen the engagement between firms and MAS on innovative ideas as well as regulatory clarifications relating to them, and facilitate meaningful experimentation. While the regulatory sandbox is fully customisable and applicable to any activity that is regulated by MAS, Sandbox Express provides a faster option for firms conducting certain regulated activities to test their product or service, by relying on standard disclosures and pre-defined rules.[241]

GATS commitments in financial sector

The integral role of payment services in facilitating transactions requires the financial sector within which they are usually regulated to be competitive. All APEC economies have made GATS schedules of commitments in the financial sector.[242] Some economies have also made additional commitments in their preferential trade agreements (PTAs).[243] However, analysis of the OECD Services Trade Restrictiveness Index (STRI) database for commercial banking

[236] Malaysia, 'Malaysia's Fintech Sandbox Gets Crowded', https://www.finews.asia/finance/25850-fintech-sandbox-gets-crowded-in-malaysia.
[237] Regulation Asia, 'Philippines Fintech Push Makes It An Interesting Market To Watch', https://www.regulationasia.com/philippines-fintech-push-makes-it-a-compelling-market-to-watch/.
[238] Bangkok Bank Innohub, 'Where Fintech Ideas Meet BOT Regulations', https://www.bangkokbankinnohub.com/regulatory-sandbox/.
[239] Monetary Authority of Singapore, 'MAS Issues "Regulatory Sandbox" Guidelines for FinTech Experiments', https://www.mas.gov.sg/news/media-releases/2016/mas-issues-regulatory-sandbox-guidelines-for-fintech-experiments.
[240] Monetary Authority of Singapore, 'MAS Launches Sandbox Express for Faster Market Testing of Innovative Financial Services', Accessed 6 August 2020, https://www.mas.gov.sg/news/media-releases/2019/mas-launches-sandbox-express-for-faster-market-testing-of-innovative-financial-services.
[241] Monetary Authority of Singapore, 'Overview of Regulatory Sandbox', Accessed 5 August 2020, https://www.mas.gov.sg/development/fintech/regulatory-sandbox.
[242] World Trade Organisation, 'GATS', https://i-tip.wto.org/services/.
[243] Ibid.

showed that the extent of liberalization at MFN level continues to vary between economies covered. In terms of restrictiveness score, they range between 0.166 and 0.489 with 0 being the least restrictive and 1 being the most restrictive. Breaking down the overall score into the different category of restrictions showed that regulations affecting foreign entry to be the main contributing restriction. As an example, while foreign investment is possible in Indonesia, it is subject to a special license from the Financial Services Authority. There are also regulations affecting cross-border data flows.[244] Other restrictions among APEC economies include those acting as barriers to competition and those pertaining to regulatory transparency.[245]

ELECTRONIC INVOICING ("E-INVOICING")

E-invoicing entails the electronic exchange of invoice information between businesses, or between businesses and consumers, upon completion of a transaction. It is relatively more efficient as compared to the traditional, paper-based invoicing method, which is both labour-intensive and prone to human errors. Noting this, some APEC economies have mandated or encouraged their adoption through laws and regulations.

For example, Chile's e-invoicing law establishes the mandatory use of electronic invoices, alongside other electronic tax documents such as invoice settlement, debit and credit notes and purchase invoices.[246] As for China's e-invoicing law, it states that an e-invoice should have the same legal effect as a traditional paper invoice, and requires business operators to issue paper or electronic invoices or other documents for commodities sold or services provided by them.[247]

In Chinese Taipei, the e-invoicing regulation provides that business entities may issue e-invoices to the purchaser.[248] Over in the Philippines, e-invoicing is mandatory for taxpayers engaged in the export of goods and services and e-commerce up until 1 January 2023.[249] As for Viet Nam, the relevant e-invoicing law provides that organisations, enterprises and individuals selling goods and services are required to issue e-invoices to their buyers.[250]

---

[244] Indonesia, 'GATS/SC/43', https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=10332,11366,37274,16557&CurrentCatalogueIdIndex=3&FullTextHash=&HasEnglishRecord=True&HasFrenchRecord=True&HasSpanishRecord=True.

[245] OECD, 'Services Trade Restrictiveness Index Simulator', https://sim.oecd.org/.

[246] Chile, 'Electronic Invoicing Law', Last amended 2014, Article 54, https://www.leychile.cl/Navegar?idNorma=6369&idParte=8675460&idVersion=2014-11-01.

[247] China, 'E-Commerce Law of the People's Republic of China', Last amended 2018, Article 14, https://www.izvoznookno.si/Dokumenti/E-commerce%20Law%20of%20the%20People%E2%80%99s%20Republic%20of%20China.pdf.

[248] Chinese Taipei, 'Regulations Governing the Use of Uniform Invoices', Last amended 2019, Article 7-1, https://law.moj.gov.tw/ENG/LawClass/LawParaDeatil.aspx?pcode=G0340082&bp=3.

[249] The Philippines, 'Tax Reform for Acceleration and Inclusion (TRAIN) Act', Last amended 2020, https://www.bir.gov.ph/images/bir_files/internal_communications_1/TRAIN%20matters/RA-10963-RRD.pdf.

[250] Viet Nam, 'Prescribing Electronic Invoices For Sale of Goods and Provision of Services', Last amended 2016, Article 2, http://www.vietnamlawdata.com/law-on-bill-in-vietnam/decree-119-2018-nd-cp-prescribing-electronic-invoices-for-sale-of-goods-and-provision-of-services-vietnam.

While domestic laws in the area of e-invoicing are integral to facilitating the use of e-invoices, interoperability of e-invoices across economies is a necessary supplement to domestic legal frameworks because of the cross-border nature of trade transactions in today's interconnected trade ecosystem. Multilateral e-invoicing frameworks that apply uniformly across jurisdictions can facilitate interoperability of e-invoices across economies. One example is the Pan-European Public Procurement On-Line (PEPPOL), a framework that provides a set of technical specifications to make the disparate e-invoicing systems across Europe interoperable.[251]

Despite the European origins of PEPPOL, various non-European economies have also adopted the PEPPOL interoperability framework. Among APEC economies, Australia, Canada, New Zealand, Singapore and the United States have already adopted the PEPPOL standard.[252] The Infocomm Media Development Authority (IMDA) in Singapore is the first PEPPOL Authority outside of Europe, and has launched the network in January 2019. Moreover, the adoption of PEPPOL by Australia and New Zealand has taken place pursuant to the Trans-Tasman Electronic Invoicing Arrangement, a bilateral agreement between the governments of Australia and New Zealand to create and maintain a common Australia and New Zealand e-invoicing approach, so as to improve business productivity and reduce business costs for the governments and industries of both economies.[253]

TRADE FACILITATION

While e-payment transactions may be completed online, physical goods would still have to be transported physically from vendors to consumers. All APEC economies have ratified the WTO Trade Facilitation Agreement, which entered into force on February 2017 and contains provisions to expedite the movement, release and clearance of goods, including goods in transit. In addition, the Agreement sets out measures for effective cooperation between customs and other appropriate authorities on trade facilitation and customs compliance issues.[254] The sub-sections below discuss some of the initiatives undertaken by economies to facilitate trade. These include the adoption of paperless trading and blockchain technology, implementation of Authorized Economic Operator (AEO) programs and introduction of single windows.

Paperless trading

Paperless trading refers to the digitization of information flows involved in cross-border trade of goods and services. It entails the transformation of traditional paper-based documentation exchange processes into electronic exchanges of information. By using electronic documentation in lieu of paper-based documentation, challenges inherent in the exchange of paper-based documentation – including, but not limited to, documents going missing, delays

[251] PEPPOL, 'What is PEPPOL', https://peppol.eu/what-is-peppol/.
[252] PEPPOL, 'PEPPOL reach and country profiles', https://peppol.eu/what-is-peppol/peppol-country-profiles/.
[253] Australian Government, 'Tran-Tasman Electronic Invoicing Arrangement', https://treasury.gov.au/trans-tasman-electronic-invoicing-arrangement.
[254] World Trade Organisation, 'WTO Trade Facilitation Agreement', https://www.tfafacility.org/ratifications.

in certifying documentation etc. – may be averted, thereby enhancing the time and cost efficiencies of doing business.[255] Seventeen (17) APEC economies have prepared Paperless Trading Individual Action Plan (IAPs) to chart their progress in driving paperless trading. These include Australia; Canada; Chile; China; Hong Kong, China; Indonesia; Japan; Korea; Malaysia; Mexico; Peru, the Philippines; Singapore; Chinese Taipei; Thailand; United States; and Viet Nam.[256]

In addition, the Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific is a United Nations treaty aimed at accelerating digital trade through paperless trading procedures. The Framework Agreement is accessible to all 53 member economies of the United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP), and is designed for economies at all levels of economic development to develop their capacities to engage in cross-border paperless trade. Two APEC economies, namely China and the Philippines, have since signed the Framework Agreement in 2017 and 2019 respectively.[257]

Blockchain technology

Blockchain technology refers to a time-stamped series of immutable records of data that is managed by a cluster of computers not owned by any single entity. Each of these blocks of data (i.e., block) is secured and bound to each other using cryptographic principles (i.e. chain), which gives rise to the portmanteau "blockchain". Blockchain networks need not be bound by the oversight of central authorities, since each blockchain network is a shared and immutable ledger, with the network information open for anyone and everyone to view. Hence, anything that is built on the blockchain is transparent by nature, and all participants involved are accountable for their actions despite the absence of oversight by central authorities.[258]

Blockchain initiatives for trade facilitation have been driven by either the public sector, private sector, or public-private partnerships. Korea's Development Plan for Digital Trade has identified several technologies, including blockchain that may be used to transform the trade environment and strengthen exports for the economy – for example, financial institutions will be able to access relevant documents shared on a blockchain platform by businesses, in order to facilitate access to trade finance by these businesses. Similarly, export bonds will be shared using the same blockchain platform to enable financial institutions to check for duplicate issuance.[259] Similarly, the Australian Border Force has developed the Inter-Government

[255] World Economic Forum, 'Paperless Trading: How Does It Impact the Trade System', https://www.weforum.org/whitepapers/paperless-trading-how-does-it-impact-the-trade-system.

[256] APEC, 'Paperless Trading Individual Action Plan', https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Digital-Economy-Steering-Group/Paperless-Trading-Individual-Action-Plan.

[257] United Nations Economic and Social Council, 'Promoting cross-border paperless trade in Asia and the Pacific' https://www.unescap.org/sites/default/files/CTI_3_item%204%20-%20Cross-border%20paperless%20trade_E_0.pdf.

[258] BuiltIn, 'Blockchain 101', https://builtin.com/blockchain.

[259] Coindesk, 'South Korea aims to put Trade Finance on the Blockchain by 2021', https://finance.yahoo.com/news/south-korea-aims-put-trade-130036777.html.

Ledger to allow for electronic sharing of documents between participating economies,[260] while the People's Bank of China is spearheading a blockchain trade finance platform and has acquired funding worth RMB32.35 million to undertake key R&D projects over the next three years.[261]

Examples of trade-facilitating blockchain initiatives led by the private sector include New Zealand's TradeWindow. Through its use of distributed ledger technology, a single trading window is provided to all parties involved in an export transaction. Edits can only be made with approval of majority of network participants, hence significantly reducing the risk of fraud. In addition, costs are significantly reduced due to the instantaneous sharing of documentation, while the risk of fraud and cyber security threats is diminished.[262] In Hong Kong, China, a blockchain-based trade finance platform known as eTradeConnect was launched by twelve major banks. The objective is to improve trade efficiency, build better trust among trade participants, reduce risks and facilitate access to financing by leveraging the features of blockchain technology.[263] In addition, a blockchain-powered digital shipping platform jointly built by IBM and A.P. Moeller-Maersk, known as TradeLens, has been launched in Indonesia and Russia. TradeLens digitizes formerly paper-based shipping processes, thus offering all parties involved full transparency of cargo movements as well as real-time actionable supply chain information.[264]

In Singapore, the Infocomm Media Development Authority of Singapore (IMDA) has spearheaded the TradeTrust initiative, a digital utility that comprises a set of globally-accepted standards and frameworks to facilitate the trusted interoperability of digital documents used in international trade and logistics. TradeTrust operates on the Ethereum network and provides participants with proof of authenticity, and provenance of trade documentation as well as an electronic method to handle transferable instruments that is legally valid. To promote public private partnership, IMDA has released the TradeTrust software under open-source terms and continues to engage partners to join its effort in enhancing trade digitalisation. ICC TradeFlow is one of the first platforms built on TradeTrust. Co-developed by ICC and trade tech firm Perlin, it is a blockchain-powered platform through which businesses can visually map trade flows, issue instructions to partners, and analyse trade actions in real time. Businesses can also

[260] Australian Government, Department of Industry, Science, Energy and Resources, 'The National Blockchain Roadmap: Progressing towards a blockchain-empowered future', https://www.industry.gov.au/sites/default/files/2020-02/national-blockchain-roadmap.pdf.

[261] Crowdfund Insider, 'People's Bank of China Acquires $4.7 Million in Funding to Further Develop Blockchain-based Trade Finance Platform', https://www.crowdfundinsider.com/2020/03/158535-peoples-bank-of-china-acquires-4-7-million-in-funding-to-further-develop-blockchain-based-trade-finance-platform/.

[262] Scale-up New Zealand, 'Trade Single Window', https://new-zealand.globalfinder.org/company_page/trade-window

[263] Global Trade Review, 'eTradeConnect links up with CargoSmart and PwC to improve access to trade finance', https://www.gtreview.com/news/fintech/etradeconnect-links-up-with-cargosmart-and-pwc-to-improve-access-to-trade-finance/.

[264] TradeLens, 'New members set stage for next wave of TradeLens growth', https://www.tradelens.com/post/new-members-set-stage.

upload, verify, and modify trade documents on the platform, as well as act upon instructions from trading partners.[265]

Authorised Economic Operator (AEO)

The WCO defines an AEO as a party involved in the international movement of goods in whatever function that has been approved by or on behalf of a domestic customs administration as complying with WCO or equivalent supply chain security standards.[266] If an exporter has supply chain partners (e.g., carriers, forwarders) that have been pre-screened and approved, it is likely that transported items are deemed to be of lower risk. Ultimately, these items could enjoy expedited clearance times, fewer examinations and better communication between supply chain partners.

Based on information from WCO's Compendium of AEO programmes and IDB's AEO in APEC economies report, twenty (20) APEC economies had either operational AEO programmes or AEO programmes under development, namely: Australia; Brunei Darussalam; Canada; Chile; China; Hong Kong, China; Indonesia; Japan; Korea; Malaysia; Mexico; New Zealand; Peru; the Philippines; Russia; Singapore; Chinese Taipei; Thailand; the United States; and Viet Nam[267]. Implementation of the AEO system in some of these economies is influenced by the Framework of Standards to Secure and Facilitate Global Trade (SAFE Framework), focusing on strengthening cooperation between and among customs administrations; for example, through the exchange of information, mutual recognition of controls, mutual recognition of AEOs and mutual administrative assistance.[268]

Single Window Systems

Single window systems enable parties involved in trade and transport to lodge standardised information and documents with a single entry point to fulfil all import, export and transit-related regulatory requirements. Various APEC member economies have created single windows within their own economies. For example, Hong Kong, China's Trade Single Window serves as a one-stop electronic platform for the trading community to lodge import

[265] International Chamber of Commerce, 'ICC TradeFlow blockchain platform launches to simplify trade processes', https://iccwbo.org/media-wall/news-speeches/icc-tradeflow-blockchain-platform-launches-to-simplify-trade-processes/.

[266] Those standards relate to the following areas: 1) demonstrated compliance with customs requirements; 2) satisfactory system for management of commercial records; 3) financial viability; 4) consultation, cooperation and communication; 5) education, training and awareness; 6) information exchange, access and confidentiality; 7) cargo security; 8) conveyance security; 9) premises security; 10) personnel security; 11) trading partner security; 12) crisis management and incident recovery; and 13) measurement, analysis and improvement.

[267] World Customs Organization, 'Compendium of Authorized Economic Operator Programmes', http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/safe-package/aeo-compendium.pdf?db=web and Inter-American Development Bank, 'AEO in APEC Economies - Opportunities to expand Mutual Recognition Agreements and the inclusion of SMEs', http://mddb.apec.org/Documents/2019/SCCP/WKSP/19_sccp_wksp1_005.pdf.

[268] World Customs Organisation, 'Authorized Economic Operator', https://www.unescap.org/sites/default/files/01-AEO%20Concept%20and%20TWO%20TFA-Toshihiko%20Osawa.pdf.

and export trade documents with the relevant authorities.[269] Chile is part of a set of economies currently working with the Inter-American Development Bank to spearhead the development of blockchain solutions for single windows in the Latin American region.[270]

As noted within the study on International Single Window's by the Australian Department of Immigration and Border Protection in 2016[271], not many economies have implemented Single Windows that are consumerate with international standards for reasons such as cost and technological know-how. Considering the potential challenges that may arise from building a common system for all participating economies, it could be more sensible to work on the interoperability among existing systems instead. The benefits of ensuring the interoperability of the Single Window Systems include: 1) greater regional integration; 2) better risk analysis due to the sharing of information; 3) allows for advance security declaration; 4) better infrastructure use-planning should the size of expected arrivals be known earlier; and 5) allows for illicit activity to be combatted more easily[272]. Recognizing this, efforts have been taken to better streamline the single window systems around the Asia-Pacific region. For example, the ASEAN Single Window creates an interoperable environment which connects and integrates single windows of individual ASEAN members. As of December 2019, all APEC member economies that are also ASEAN members, namely Brunei Darussalam; Indonesia; Malaysia; the Philippines; Singapore; Thailand; and Viet Nam, have joined the live operation of ASEAN Single Window.[273]

Another initiative to enhance interoperability across domestic single windows is the Inter-American Network of International Trade Single Windows. This initiative is backed by the Pacific Alliance, which is a regional integration initiative comprising four Latin American economies, three of which are APEC economies – namely Chile, Colombia, Mexico and Peru. The main objective of the Pacific Alliance is to increase the free circulation of goods, services, capital, and people across its member economies and wider Asia-Pacific region, and the potential interoperability across domestic single windows will help to increase the seamlessness of the said trade movements.[274]

TAXATION AND CUSTOMS DUTIES

Assessing and collecting duties and taxes requires significant time and resources for many economies. To facilitate the process, economies have generally set de minimis thresholds for

[269] Trade Single Window, 'About Trade Single Window', https://www2.tradesinglewindow.hk/portal/en/about_tsw/index.html.

[270] Inter-American Development Bank, 'Global Alliance to Promote the Use of Blockchain in Latin America and the Caribbean', https://www.iadb.org/en/news/global-alliance-promote-use-blockchain-latin-america-and-caribbean.

[271] Australian Department of Immigration and Border Protection, 'International Single Window Study – Final Report', 2016.

[272] UNECE, 'Single Window Interoperability', 2017, http://www.unece.org/fileadmin/DAM/trade/Publications/ECE-TRADE-431E_Rec36.pdf.

[273] ASEAN, 'What is the ASEAN Single Window', https://asw.asean.org/.

[274] APEC PSU, 'Study on Single Window Systems' International Interoperability: Key Issues for Its Implementation', https://www.apec.org/-/media/APEC/Publications/2018/8/Study-on-Single-Windows-Systems/218PSUStudy-on-Single-Windows-Systems.pdf.

imports. While e-commerce transactions of relatively small values would typically not be subject to customs duties, some e-commerce transactions may still incur customs duties if they exceed the de minimis thresholds. Table 4.1 below summarizes the de minimis thresholds set by APEC economies.

Table 4.1: De minimis value of APEC economies

Member Economy	De Minimis Value
Australia	AUD 1,000
Brunei Darussalam	BND 400
Canada	CAD 20
Chile	USD 30
Indonesia	USD 3
Japan	USD 92
Republic of Korea	KRW 150,000
Malaysia	USD 119
Mexico	USD 117
New Zealand	NZD 1,000
Papua New Guinea	PGK 25
Peru	USD 200
The Philippines	PHP 10,000
Russia	RUB 5,000
Singapore	SGD 400
Chinese Taipei	NTD 2,000
Thailand	THB 1,500 (domestic post) / THB 40,000 (international post)
The United States	USD 800
Viet Nam	VND 1,000,000

Source: Compilations by APEC PSU.

There is currently a moratorium on the imposition of customs duties on electronic transmissions agreed at the WTO.[275] While it was intended to be in place until the 12th WTO Ministerial Conference in June 2020, the conference is currently on hold due to the COVID-19 pandemic. Additionally, APEC economies have gone beyond by binding the WTO moratorium in their FTAs/RTAs. In total, 15 APEC economies have entered into agreements containing the moratorium since 2008.[276] Examples of these agreements include the Singapore-Australia Free

[275] WTO General Council, 'WTO members agree to extend e-commerce, non-violation moratoriums', https://www.wto.org/english/news_e/news19_e/gc_10dec19_e.htm.

[276] APEC, 'Pathfinder Initiative Proposal for a Permanent Customs Duty Moratorium on Electronic Transmissions, Including Content Transmitted Electronically', http://publications.apec.org/-/media/APEC/Publications/2016/11/2016-CTI-Report-to-Ministers/TOC/Appendix-26-Pathfinder-on-Permanent-Customs-Duty-Moratorium-on-Electronic-Transmissions-Including-Co.pdf.

Trade Agreement (SAFTA),[277] US-Singapore Free Trade Agreement[278], US-Australia Free Trade Agreement[279], European Union-Korea Free Trade Agreement,[280] the CPTPP,[281] and the USMCA.[282]

4.2 FOCUS AREA B: OPENNESS AND CROSS-BORDER ISSUES

CROSS-BORDER DATA FLOWS

Regulations on cross-border data flows establish conditions under which data exports of personal data can occur and/or are allowed.[283] While this study only evaluates cross-border flows of personal data, there are cases in economies, such as Mexico, where regulation for transfers of personal data apply horizontally (i.e., regardless of whether the data transfer is domestic or cross-border).

Twenty (20) out of the 21 APEC economies have some form of requirements for cross-border transfers of personal data, found either in data protection laws, cyber security laws, sectoral or state-level regulation. The only exception is Papua New Guinea, where there is a lack of information regarding requirements for cross-border data transfers.

In all other cases, despite the nuances and variations, transfers can be broadly classified as: 1) transfers based on consent, 2) transfers based on the existence of similar levels of protection and consent, and 3) transfers based on the accountability of the business operator that is transferring the data. This classification is only provided as a reference, as there may be overlaps in the way economies regulate data transfers. An overview is presented below.

Transfers based on consent

Mexico requires the consent of data subjects (via a privacy notice) for data transfers to be carried out. Despite this general rule, consent is not required when: 1) the transfer is enabled by a law or treaty to which Mexico is a party; 2) it is an intra-company transfer; 3) it is part of

[277] Singapore-Australia Free Trade Agreement, Chapter 14 Electronic Commerce, https://www.enterprisesg.gov.sg/-/media/esg/files/non-financial-assistance/for-companies/free-trade-agreements/Singapore-Australia-FTA/Legal-text/Chapter-14/Chapter-14-Electronic-Commerce.

[278] Enterprise Singapore, US-Singapore Free Trade Agreement, https://www.enterprisesg.gov.sg/non-financial-assistance/for-singapore-companies/free-trade-agreements/ftas/singapore-ftas/ussfta.

[279] Australian Government, Department of Foreign Affairs and Trade, Australia-United States FTA, https://www.dfat.gov.au/trade/agreements/in-force/ausfta/Pages/australia-united-states-fta.

[280] Sacha Wunsch-Vincent and Arno Hold, Towards coherent rules for digital trade: Building on efforts in multilateral versus preferential trade negotiations, https://www.wti.org/media/filer_public/53/69/5369b2b8-bfdc-4b95-808b-35cbc22dadb7/wunsch_hold_wp_final_11-07-08.pdf.

[281] Comprehensive and Progressive Agreement for. Trans-Pacific Partnership, Chapter 14 Electronic Commerce, https://www.mfat.govt.nz/assets/Trans-Pacific-Partnership/Text/14.-Electronic-Commerce-Chapter.pdf.

[282] Office of the United States Trade Representative, 'n.d. United States-Mexico-Canada Agreements'. https://ustr.gov/usmca

[283] This analysis is focused on regulations regarding personal data. Regulations about non-personal data (e.g. machine data) do not form part of the current analysis.

the fulfilment of a legal relationship between the data subject and the data controller; and/or 4) it is necessary to protect the public interest or enforce justice, among others.[284] Chile also requires the consent of the data subject in order to transfer data.[285] Similarly, under Korea's Personal Information Protection Act[286] and the Act on Promotion of Information and Communications Network Utilization and Information Protection,[287] consent is a prerequisite to transfer data abroad. However, this is subject to exceptions, such as when there are private sector safeguards in place.

Transfers based on consent and/or similar levels of protection, among others

Japan regulates cross-border transfers in the Act on the Protection of Personal Information (APPI) of 2003, amended in 2015 and implemented in 2017.[288] The APPI allows data transfers to economies with similar levels of protection as Japan;[289] or when the third-party to receive the data conforms to standards contained in Japan's APPI.[290] These standards can be satisfied by internal agreements or memorandums of understanding between the provider of the data (the business operator) and the recipient of the data, or where the recipient has obtained accreditation under international frameworks, such as the APEC's CBPR system (to which Japan is a part of).

Brunei Darussalam does not have a comprehensive data protection law, but since 2014 has put in place a Data Protection Policy which is applicable only to the public sector. This policy sets out scenarios in which cross-border data transfers may occur. Specifically, Principle XI of the Data Protection Policy allows agencies to transfer data when: 1) the recipient economy is subject to a law, binding scheme or contract which contains principles reflecting a similar level of protection as in Brunei Darussalam; 2) the data subject has given consent for the data transfer; 3) the transfer is necessary for the performance of a contract; 4) the transfer is necessary for the conclusion or performance of a contract; or 5) reasonable steps have been taken to ensure that the transferred data will not be held, used or disclosed by the recipient of the data inconsistently with Brunei Darussalam's data protection principles.[291]

---

[284] Mexico, Federal Law on the Protection of Personal Data in the Possession of Individuals, 2010, Article 37 http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf.

[285] Chile, Law 19628 on the protection of the private life, Last amended 2012, Article 4, https://www.leychile.cl/Navegar?idNorma=141599.

[286] Korea, Personal Information Protection Act – Law No. 10465, 2011, Last amended 2020, Article 17, https://www.privacy.go.kr/eng/laws_view.do?nttId=8186&imgNo=1.

[287] Korea, Act on Promotion of Information and Communications Network Utilization and Information Protection, Law No. 3848 of 1987, Last amended 2017, Article 63, https://elaw.klri.re.kr/eng_service/lawView.do?hseq=38422&lang=ENG.

[288] Japan, Act on the Protection of Personal Information (2003), Article 24, http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf.

[289] Those jurisdictions that are deemed to have similar levels of protection are set out in a list of economies.

[290] Tomoki Ishiara, 'Japan' in The Privacy, Data Protection and Cybersecurity Law Review, 6th ed. (London: Law Business Research Ltd, 2019), https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-6/1210043/japan.

[291] Brunei Darussalam has established 11 data protection principles: (i) Accountability and responsibility for data protection; (ii) specifying purposes; (iii) consent; (iv) collection of data; (v) use; (vi) disclosure and retention of data; (vi) accuracy of

Thailand, under the recently enacted Personal Data Protection Act of May 2019, allows personal data transfers to economies where similar standards of protection are offered. This requirement is waived if: 1) the data subject has given consent and the data administrator (the business operator) has given proper notification; 2) the transfer is necessary for the performance of a contract between the data administrator and the data subject; 3) the transfer is necessary to protect the vital interest of the data subject, although there is no guideline to elaborate on the definition of "vital interest". Intra-company cross-border transfers of data are regulated within Section 29 of the Personal Data Protection Act.[292]

Peru also has requirements for cross-border transfers of data. Article 15 of the Peruvian Data Protection Law[293] establishes that data transfers can only take place if the destination economy offers similar levels of protection as the one provided by the Peruvian Data Protection Law. If this requirement is not met, cross-border data transfers can take place, only if:[294] 1) there is an applicable international treaty; 2) the transfer is with regards to international judicial cooperation; 3) the transfer is required for the fulfilment of a contractual relationship; and 4) when the data subject has given his/her consent.

In New Zealand, cross-border transfers of personal data are restricted to where personal information will be protected by comparable safeguards to the New Zealand Privacy Act. This includes where a jurisidiction has privacy laws that, overall, provide comparable safeguards, or through a contractual agreement which protects the information. An individual can also authorise overseas disclosures after being explicitly informed that personal information may not be protected by comparable safeguards to those in the Privacy Act 2020. A transfer may be prohibited by the Privacy Commissioner on reasonable grounds that the third economy does not have comparable safeguards as New Zealand, and the transfer is likely to contravene the basic principles contained in the OECD privacy guidelines.[295]

Similarly, Malaysia has a system whereby data can only be transferred if the economy receiving it is included in a whitelist, which contains economies having laws in force offering similar levels of protection or ensuring an equivalent adequate level of protection as those found in the Malaysian Act.[296]

In the case of Russia, Article 12 of the Federal Law on Personal Data establishes that in the event of a cross-border transfer of data, the data operator must check that the data subjects'

---

data; (vii) safeguards for data; (viii) Openness about data protection policies and procedures, (ix) individual access and correction; (x) challenge to compliance; (xi) trans-border data transfers.

[292] Thailand, Personal Data Protection Act, 'B.E. 25620', 2019, Section 28, https://www.mazars.co.th/Home/Doing-Business-in-Thailand/Legal/Personal-Data-Protection-Act-Published.

[293] Peru, Personal Data Protection Act, 'Law 29733', 2011, http://www.pcm.gob.pe/transparencia/Resol_ministeriales/2011/ley-29733.pdf.

[294] Cross-border data transfers can also occur for cross-border banking transactions, or when the transfer is carried out for the protection, prevention, diagnosis or medical treatment of the data holder.

[295] New Zealand, Privacy Act 2020, Section 193, http://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23673.html.

[296] Malaysia, Personal Data Protection Act, 2010, Section 129, http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20709%2014%206%202016.pdf.

rights are adequately protected in the recipient economy before the transfer. All economies that are party to the European Convention on Personal Data from 1981 (Convention 108) are considered to be economies having an adequate level of protection of data subjects. The data protection agency, Roskomnadzor, has approved a list of economies that are not party to Convention 108 but are, nonetheless, considered to be safe destinations. These economies include Qatar; Costa Rica; Japan; Singapore; Mali; Gabon; Kazakhstan; South Africa; Canada; Israel; New Zealand; Mongolia; and Peru. Transfers to other destinations are allowed if the data subject has given his/her consent, among other grounds.

Transfers based on accountability

In Canada, consent is not explicitly required under the Personal Information Protection and Electronic Documents Act (PIPEDA).[297] Instead, organizations and businesses bear the responsibility for the protection of personal information transfers under each individual outsourcing arrangement. Thus, the organization transferring data should ensure that a comparable level of protection, as the one existing in Canada, is available for personal information.

The Philippines Data Privacy Bill of 2012[298] requires the principle of accountability to be adhered for transfers of personal data in its Section 21. This means that it is the business operator's responsibility to ensure that the data being transferred (either domestically or internationally) is treated in accordance with the provisions of the Philippines' Data Privacy Bill. Achieving this can be done through the use of contracts or other reasonable means.

Similarly, according to Singapore's Personal Data Protection Act,[299] an organisation may transfer personal data overseas if it has taken appropriate steps to comply with the Data Protection Provisions while the personal data remains in its possession or is under its control. In the event that the personal data is transferred to a recipient in an economy or territory outside Singapore, the organisation need to ensure that the recipient is bound by legally enforceable obligations to provide to the personal data transferred a standard of protection that is comparable to that under the PDPA.

Under Australia's Privacy Principles, set out in Schedule 1 of the Privacy Act,[300] cross-border transfers can only occur when the entity disclosing the data takes reasonable steps to ensure that the entity receiving the data does not breach Australia's Privacy Act Principle 8. According

[297] Canada, Personal Information Protection and Electronic Documents Act (PIPEDA), 'S.C. 2000, C.5', 2000, https://www.parl.ca/DocumentViewer/en/36-2/bill/C-6/royal-assent/page-19#1.
[298] The Philippines, Data Privacy Bill of 2012, 'Republic Act 10173', 2012, https://www.privacy.gov.ph/data-privacy-act/
[299] Singapore, 'Personal Data Protection Act, 2012', https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-9-Oct-2019.pdf?la=en.
[300] Australia, 'Privacy Act - Act No. 119 of 1988', Last amended 2016, Schedule 1:8, https://www.legislation.gov.au/Details/C2020C00025.

to Section 16C of the same Act, the entity disclosing the information is accountable when the overseas recipient mishandles the information.

Other cases

The United States does not generally have any regulations which restrict cross-border data transfers at the federal or state level.[301] On the other hand, sectoral legislation could restrict certain transfers. This can be the case with electronic protected health information (ePHI), which is regulated by the Health Insurance Portability and Accountability Act (HIPAA) of 1996, though ePHI may be stored outside the United States when applicable requirements are met.[302,303]

Under Article 22 of Indonesia's Ministerial Regulation No. 20 of 2016 concerning Protection of Personal Data in Electronic Systems,[304] operators of electronic systems domiciled in Indonesia and planning to transfer personal data outside of the economy must coordinate with the relevant authorities by reporting certain information relating to the transfer. In addition, in regards to e-commerce, Regulation No. 80 of 2019 on Trading through Electronic Systems[305] stipulates that personal data cannot be transferred offshore, unless the receiving economy is deemed, by the Ministry of Trade, as having the same level of personal data standards and protection as Indonesia.

Chinese Taipei regulates cross-border data transfers in the Personal Data Protection Act (PDPA) of 1995. According to Article 21 of the Act, cross-border data transfers can be restricted where major domestic interests are involved or where an international treaty or agreement so stipulates, or where the economy receiving the personal data lacks proper regulations on protection of personal data and the data subjects' rights and interests may consequently be harmed, or where the cross-border transfer of the personal data to a third economy is carried out to circumvent the PDPA.[306] This negative formulation is unique in the economies analyzed.

---

[301] California Department of Justice, 'California Consumer Privacy Act (CCPA): Fact Sheet', n.d. https://oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf.

[302] The United States, Health Insurance Portability and Accountability Act (HIPAA), 'Pub. L. 104-191', 1996, https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf.

[303] https://www.hhs.gov/hipaa/for-professionals/faq/2083/do-the-hipaa-rules-allow-a-covered-entity-or-business-associate-to-use-a-csp-that-stores-ephi-on-servers-outside-of-the-united-states/index.html.

[304] Indonesia, 'Minister of Communication and Informatics Regulation No. 20 of 2016 concerning Personal Data Protection in Electronic System ("MCI 20/2016")', https://www.makarim.com/en/news/detail/legal-advisory/547/new-regulation-on-the-protection-of-personal-data-key-provisions.

[305] Indonesia, 'Regulation No. 80 of 2019 on Trading Through Electronic Systems', 2019, https://jdih.setneg.go.id/viewpdfperaturan/P18728/PP%20Nomor%2080%20Tahun%202019.

[306] Chinese Taipei, 'Personal Data Protection Act', 2015, https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=I0050021.

Section 33 of Hong Kong, China's Personal Data (Privacy) Ordinance[307] sets a general prohibition against transfer of personal data outside Hong Kong, China, except in specified circumstances, which are detailed under section 33(2) of the Ordinance and elaborated in the Guidance on Personal Data Protection in Cross-border Data Transfer.[308] Those specified circumstances include, among others, a "whitelisted" set of economies, or economies with substantial similar levels of protection, or situation where the data subject has provided written consent.

Under Article 37 of China's Cybersecurity Law,[309] transfer of data abroad can only occur via "security assessments". On 13 June 2019, the Cyberspace Administration of China issued for comment the draft "Measures for Security Assessment for Cross-border Transfer of Personal Information," under which cross-border transfers would also be allowed if there is contract between the data sender and the intended recipient, and where the data subject has given express and informed consent. Viet Nam's Law on Cybersecurity[310] requires domestic and foreign suppliers of telecommunications networks and other internet and other value-added services to store personal and other data onshore.

Membership of cross-border instruments: APEC's CBPR, EU Equivalence status and Convention 108

Some economies are also part of international frameworks that regulate or facilitate cross-border data transfers. This section examines the membership of APEC economies to mechanisms that facilitate cross-border personal data transfers. Currently there are nine participating economies in the Cross-Border Privacy Rules (CBPR) system (see Box 4.4).[311] These are Australia; Canada; Japan; Korea; Mexico; the Philippines; Singapore; Chinese Taipei; and the United States. On the other hand, Singapore and the United States are members of the Privacy Recognition for Processors (PRP) system.[312]

Box 4.4: APEC Cross-Border Privacy Rules (CBPR) System

The CBPR system is a voluntary certification scheme that allows companies to transfer personal data (inter- and intra-company) in a safe and trusted manner across jurisdictions. The scope of the CBPR applies to the controllers of personal information (i.e., information

[307] Hong Kong, China, 'Personal Data (Privacy) Ordinance', 1995, https://www.elegislation.gov.hk/hk/cap486!en@2018-04-20T00:00:00. Currently, section 33 of the Ordinance has not yet commenced operation.

[308] Office of the Privacy Commissioner for Personal Data, 'Guidance on Personal Data Protection in Cross-border Data Transfers', 2014, https://www.pcpd.org.hk/english/resources_centre/publications/guidance/files/GN_crossborder_e.pdf.

[309] People's Republic of China, 'Cybersecurity Law of the People's Republic of China', 2017.

[310] Viet Nam, Law on Cybersecurity, 'Law No 24/018/QH14', 2018, Article 26.3, https://thuvienphapluat.vn/van-ban/cong-nghe-thong-tin/Luat-an-ninh-mang-2018-351416.aspx.

[311] 'What Is the Cross-Border Privacy Rules System?' APEC, April 15, 2019, Accessed February 6, 2020, https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System.

[312] Michael Rose, 'United States Becomes First Economy to Offer Asia-Pacific Economic Cooperation Privacy Trustmark to Data Processors', Tradeology (blog), December 29, 2017, https://blog.trade.gov/2017/12/29/united-states-becomes-first-economy-to-offer-asia-pacific-economic-cooperation-privacy-trustmark-to-data-processors/.

about an identified or identifiable individual). It essentially certifies that a company complies with the 50 CBPR requirements that implement the APEC Privacy Framework, which is composed of four parts: i) preamble and objectives; ii) scope and coverage; iii) nine information privacy principles; and iv) domestic and international implementation. The nine APEC information privacy principles are: 1) accountability; 2) notice; 3) choice; 4) collection limitation; 5) integrity of personal information; 6) uses of personal information; 7) security safeguards; 8) access and correction; and 9) preventing harm.

In order to take part, APEC economies must demonstrate that they comply with the CBPR requirements. Once an economy's participation is approved, companies established in this economy can apply for CBPR certification through an Accountability Agent.

The same logic applies to the Privacy Recognition for Processors (PRP) system, which certifies that processors (i.e., those who do not collect personal data themselves, but process personal data on behalf of the controller) have the ability to provide effective implementation of a controller's privacy obligations related to the processing of personal information.

Source:

- Authors' own elaboration based on M.C. Vásquez Callo-Müller, 'GDPR and CBPR: Reconciling Personal Data Protection and Trade' (Singapore: Asia-Pacific Economic Cooperation Policy Support Unit, October 2018), https://www.apec.org/Publications/2018/10/GDPR-and-CBPR---Reconciling-Personal-Data-Protection-and-Trade

Mexico is the only APEC economy that is also part of Convention 108 (see Box 4.5),[313] which is a Treaty under the auspices of the Council of Europe, but open to non-members.

Box 4.5: Convention 108 - Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

Convention 108 protects the right to privacy of individuals with respect to personal data which is automatically processed. It also imposes some restrictions on cross-border transfers of personal data to non-Parties to the Convention, except when they require an adequate level of protection. In 2018, the Convention was amended by a new protocol, which imposes further restrictions to cross-border data transfers. The new protocol has yet to enter into force but it amends Article 12 (now Article 14) of the Convention.

The new Article 14 establishes that, in principle, "a Party shall not, for the sole purpose of the protection of personal data, prohibit or subject to special authorization the transfer of such data to a recipient who is subject to the jurisdiction of another Party to the Convention". However, this does not restrict the freedom of a Party to limit the transfer of personal data to another Party for other purposes, such as domestic security, defense, public safety, or other

[313] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981), https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=uEI8cPXB.

important public interests (including protection of secrets). Moreover, transfer can also be restricted if "there is a real and serious risk that the transfer to another Party, or from that other Party to a non-Party, would lead to circumventing the provisions of the Convention", or a "Party is bound by harmonized rules of protection shared by States belonging to a regional international organization". The latter refers to organizations that seek deeper levels of integration.

Source:

- Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981), https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=uEI8cPXB
  'Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data', Council of Europe Treaty Series (Council of Europe, October 10, 2018)

Four APEC economies have adequacy decisions granted by the European Commission. These are Canada, since 2002; Japan, since 2019; New Zealand, since 2012; and the United States, limited to the Privacy Shield Framework of 2016.[314] This means that these economies are deemed to have similar levels of personal data protection to those found at the European Union level. This enables personal data to flow freely between the European Economic Area (i.e. EU members plus Norway, Lichtenstein and Iceland) and these APEC economies.

LOCATION OF COMPUTING FACILITIES (INCLUDING FINANCIAL COMPUTING FACILITIES)

Requirements regarding the location of computing facilities may call for servers or data hosting solutions to remain onshore or in local computing facilities, hence possibly restricting cross-border transfers. This limits the options for the use of cloud computing services, therefore potentially increasing the cost of doing business.

Some APEC economies have requirements in this regard. In fact, some have regulations which are applicable to personal data collected by the public sector as well as public operators. For instance, it was found that some provinces of Canada have localization requirements for personal data under public sector within their legislation. This is the case of Alberta and Quebec, which restrict the transfer of personal data collected by the public sector outside Canada. Other restrictions apply in British Columbia, Nova Scotia, and Ontario.[315] In Indonesia, Article 20.2 of Government Regulation No. 71 of 2019 regarding Operation of Electronic System and

[314] European Commission, 'Adequacy Decisions', Accessed February 6, 2020, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[315] Server Cloud Canada, 'When Your Data Must Stay in Canada', 2017, Accessed February 6, 2020, https://www.servercloudcanada.com/2017/10/privacy-law-canada/.

Transactions (GR 71)[316] provides that 'Public Electronic System Operators' must place their electronic systems and data in Indonesia if the technology is available in the economy.

Another set of data retention and storage requirements among APEC economies is found in cybersecurity laws. This is the case of Article 26.3 of Viet Nam's Cybersecurity Law,[317] which contains an obligation for domestic and foreign enterprises providing services on telecommunication networks or internet or value-added services[318] in Viet Nam's cyberspace to store such data in Viet Nam for the period prescribed by the government. A second example is Article 37 of the Cybersecurity Law of the People's Republic of China,[319] according to which operators of a critical information infrastructure are explicitly required to store personal information and important data collected and generated during their operations within the economy.

[316] Indonesia, Government Regulation No. 71 of 2019 regarding Operation of Electronic System and Transactions (GR 71) (which amends Government Regulation No. 82 of 2012 Concerning Electronic System and Transaction Operation), 2019, https://jdih.kominfo.go.id/produk_hukum/view/id/695/t/peraturan+pemerintah+nomor+71+tahun+2019+tanggal+10+oktober+2019.

[317] Viet Nam, Law on Cybersecurity, 'Law No 24/018/QH14', 2018, https://thuvienphapluat.vn/van-ban/cong-nghe-thong-tin/Luat-an-ninh-mang-2018-351416.aspx.

[318] Those entities must be collecting, exploiting, analyzing, and processing personal information data, data on the relationships of service users, or data generated by service users in Viet Nam.

[319] People's Republic of China, Cybersecurity Law, 2016, http://www.csrc.gov.cn/pub/newsite/flb/flfg/flxzsf/201805/t20180518_338285.html.

More broadly, Russia's Federal Law No. 242-FZ[320] provides that, as a general rule, operators must record, systematize, process, store, amend, update, and retrieve data on Russian citizens using databases located in the economy.

Box 4.6: Financial services and data storage requirements

An example of how requirements for data storage apply in practice is found in specific rules for the financial services sector. This is particularly burdensome for e-commerce as restrictions to digital financial services can lower the cost of doing online transactions, hindering the expansion and access to e-commerce markets. Examples of specific rules for financial services include the following:

Viet Nam's Cybersecurity Law considers online payments and payment intermediaries as Cyberspace Service Providers. Thus, these entities are requested to store data (both personal and related to the services) in Viet Nam.

Hong Kong, China's Circular to Licensed Corporations (Use of external electronic data storage),[321] which is applicable to firms licensed with Hong Kong, China's Securities and Futures Commission (SFC), enables such regulated entities to exclusively keep regulatory records at external electronic data storage providers (EDSPs), such as cloud service providers, whilst complying with their existing regulatory obligations and simultaneously preserving the SFC's effective access to those records under the SFC's existing regulatory powers. An SFC-licensed firm should keep regulatory records locally but is permitted to keep an identical set of records outside of Hong Kong. Alternatively, if an SFC-licensed firm chooses to exclusively keep regulatory records with an EDSP outside of Hong Kong, it should obtain an undertaking from the EDSP that the EDSP will provide all necessary assistance to the SFC in the performance of the SFC's functions and powers, including producing the SFC-licensed firm's data to the SFC pursuant to the exercise of the SFC's statutory power.

On the other side of the spectrum, there are efforts to facilitate the flow of financial data. This includes provisions in Free Trade Agreements (FTAs), one example being Article 8.45 of the EU-Viet Nam Free Trade Agreement, which provides that each Party shall permit financial service suppliers of the other Party to transfer information in electronic or other form. Besides FTAs, efforts to facilitate flow of financial data are also enshrined in specific forms of regulatory cooperation. This is the case of the United States - Singapore Joint Statement on Financial Services Data Connectivity, which aims at facilitating cross-border

[320] Russia, Federal Law No. 242-FZ, 'On the Introduction of Amendments to Certain Legislative Acts of the Russian Federation with regard to the Clarification of the Procedure for the Processing of Personal Data in Data Telecommunications Networks', https://pd.rkn.gov.ru/authority/p146/p191/.

[321] Hong Kong, China, https://www.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=19EC59

transfers of data, including personal information, if this activity is for the conduct of the business of a financial service supplier.

Sources:

- Pazarbasiogul, C et al, Digital Financial Services, World Bank, April 2020, p. 1, http://pubdocs.worldbank.org/en/230281588169110691/Digital-Financial-Services.pdf
- EU – Viet Nam Free Trade Agreement, 2019, https://trade.ec.europa.eu/doclib/press/index.cfm?id=1437
- United States - Singapore Joint Statement on Financial Services Data Connectivity, 2020, https://www.mas.gov.sg/news/media-releases/2020/united-states-singapore-joint-statement-on-financial-services-data-connectivity

PRO-COMPETITION RULES FOR THE DIGITAL ENVIRONMENT

Competition laws are being tested given new forms of collusion (e.g., via algorithms) and the use of data. Some examples of cases concerning digital platforms in the APEC region have already been collected by the Competition Policy and Law Group of the APEC Economic Committee (EC). They include cases of abuse of dominance, acquisition, exclusive dealing and mergers.[322] In light of the above, this sub-section provides an overview of competition rules among APEC economies and data portability obligations. While most APEC economies have competition laws in place, most of them do not have specific policies for competition issues associated with online platforms. Yet, in some cases, there are initiatives to adapt competition laws specifically to the digital environment. These are the cases of Canada; Chinese Taipei; Russia; Singapore; and Australia.

The Canadian Competition Bureau has taken specific steps towards the digital environment in 2020, when it unveiled its 2020-2024 vision. Furthermore, in 2019, the Bureau published a call-out for information to assist with its enforcement activities in the digital environment and appointed the first Chief Digital Enforcement Officer.

In the case of Chinese Taipei, the Fair Trade Commission established the "Digital Economy and Competition Policy Task Force" in April 2017. In addition, the Fair Trade Commission issued the Disposal Directions (Policy Statements) on the Cross-Sector Cooperation among Digital Convergence Related Enterprises,[323] which intend to help digital convergence related enterprises avoid violations and concurrently serve as a reference for handling future cases.

In 2018, Russia issued the Executive Order of the President of the Russian Federation "On State Competition Policy Guidelines" (Order of 21 December 2017 No. 618).[324] The

[322] See Table 3, APEC, 'Competition Policy for Regulating Online Platforms in the APEC Region', 2019, https://www.apec.org/Publications/2019/08/Competition-Policy-for-Regulating-Online-Platforms-in-the-APEC-Region.

[323] Fair Trade Commission Disposal Directions (Policy Statements) on the Cross-Sector Cooperation among Digital Convergence Related Enterprises, https://www.apeccp.org.tw/htdocs/doc/Taipei/Decision/2018-09-03.pdf.

[324] Russian Federation, 'Executive Order of the President of the Russian Federation On State Competition Policy Guidelines (Order of 21 December 2017 No. 618)', 2018, http://en.fas.gov.ru/documents/documentdetails.html?id=15342.

Guidelines include Article 3.t, which refers to the improvement of antimonopoly regulation in the context of the digital economy and its globalization.

With regards to Singapore, while the competition act applies horizontally to all economic sectors, the Competition and Consumer Commission of Singapore (CCCS) has a keen interest in competition issues relating to digital platforms, and has been actively considering the opportunities, challenges and policy implications of digital platforms for several years. The CCCS has described its current efforts as being directed towards deepening its understanding of technological and market developments, and reviewing whether its toolkit remains relevant and sufficient to meet the new business models that abound in the digital sector. The CCCS pledged to continue monitoring developments in specific areas such as algorithms and artificial intelligence as the sector evolves.

In other cases, provisions for the safeguarding of competitive markets are not found in competition laws themselves but in e-commerce laws. This is the case of the E-commerce Law of the People's Republic of China, where Article 22 provides that "where an e-commerce business operator has a dominant market position due to its technological advantage, number of users, and control of relevant industries, other business operators' reliance on it in trading, or any other factor, the e-commerce business operator shall not abuse its dominant market position to eliminate or restrict competition."[325]

Data portability is also an aspect that is considered to foster competition in digital markets.[326] It enables consumers to both migrate their data across devices and digital platforms and promotes competition in the market of online service providers. The evaluation of the data protection laws among APEC economies found that only the Philippines[327] and Thailand[328] have an explicit data portability right in place. In the case of China, while there is no right of data portability, the 2018 Personal Information Security Specifications provide the right of data access. According to Article 7(9) of the Specifications, data subjects also have the right to have personal data ported to a third party if technically feasible to do so.[329]

---

[325] People's Republic of China, 'E-commerce Law of the People's Republic of China', 2019, https://www.izvoznookno.si/Dokumenti/E-commerce%20Law%20of%20the%20People%E2%80%99s%20Republic%20of%20China.pdf.

[326] OECD, 'Consumer Data Rights and Competition - Background Note', DAF/COMP(2020)1, http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP(2020)1&docLanguage=En.

[327] The Philippines, 'Data Privacy Act (Republic Act 10173)', 2012, Section 18, https://www.privacy.gov.ph/data-privacy-act/#18; See also Blair Stewart, 'Case Studies: Data Portability in the Philippines Data Protection Act and in the New EU General Data Protection Regulation' (APEC Cross Border Privacy Rules System Meeting on Governance and Participation, Lima, Peru, 2016), http://mddb.apec.org/Documents/2016/ECSG/DPS-CBPR1/16_ecsg_dps_cbpr_003.pdf.

[328] KPMG, 'Thailand Personal Data Protection Act', Accessed January 12, 2020, https://home.kpmg/be/en/home/insights/2019/11/ta-thailand-personal-data-protection-act.html.

[329] People's Republic of China, 'Information Security Technology – Personal Information Security Specification (GB/T 35273-2017)', 2017, https://www.chinesestandard.net/PDF/English.aspx/GBT35273-2017.

Beyond the scope of data privacy laws, Australia adopted the Treasury Laws Amendment (Consumer Data Right) Act in 2019,[330] which incorporates the consumer data right, hence enabling individuals and businesses to access specific data related to them and held by businesses. This right largely resembles a data portability right. Similarly, Singapore has moved beyond discussion stage and proposed to include a Data Portability provision in the amended PDPA[331]. Other APEC economies where a possible right of data portability is being discussed include Korea, where a recent proposal for amendments of the Credit Information Use and Protection Act of 1995 include a data portability right, and Japan.[332]

PRINCIPLES ON ACCESS AND USE OF THE INTERNET FOR DIGITAL TRADE

APEC economies have taken different approaches toward network management practices (i.e. practices undertaken by internet services providers regarding the prioritization of certain traffic). Some have adopted the so called "network neutrality principle" in their regulations. According to this principle, internet traffic should be treated in a "non-discriminatory fashion, regardless of content, application, service, device, sources or recipients".[333] In particular, APEC members from Latin America have been enthusiastic about establishing specific network neutrality laws (such as the case of Chile) or incorporating network neutrality principles within telecommunication laws (Peru and Mexico). As an example, in the case of Peru, network neutrality provisions established in Law 29904 [334] prohibit arbitrary discrimination of content, and it is up to the regulator to define when an arbitrary behavior occurs.

There is also a number of APEC economies with no network neutrality rules. This is the case of Japan; the Philippines; Thailand; and the United States. For instance, in the case of Japan, although the government has been active in discussing approaches toward network neutrality, specific rules have not been adopted, leaving the regulation of internet traffic to the market.[335]

---

330 Australia, 'Treasury Laws Amendment (Consumer Data Right) Bill', 2019, https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6370_aspassed/toc_pdf/19126b01.pdf;fileType=application%2Fpdf.

331 See: Personal Data Protection Commission, 'Public Consultation on Personal Data Protection (Amendment) Bill', https://www.pdpc.gov.sg/guidelines-and-consultation/2020/05/public-consultation-on-personal-data-protection-(amendment)-bill.

332 METI, 'Establishment of Study Group for Data Portability', 2017, https://www.meti.go.jp/english/press/2017/1120_002.html.

333 Luca Belli and Primavera De Filipi, eds., 'Net Neutrality Compendium: Human Rights, Free Competition and the Future of the Internet (Switzerland: Springer, 2016)', 4.

334 Peru, Law for the Promotion of Broadband and the Construction of the National Optical Fiber Backbone, 'Law 29904', 2012. https://www.osiptel.gob.pe/articulo/ley-29904-promocion-banda-ancha-rdnfo. Article 6 of Law 29904 established that "Providers of internet access will respect network neutrality, according to which, they cannot arbitrarily block, interfere, discriminate or restrict internet user's rights to use applications or protocols independently of its origin, destiny, nature or ownership."

335 Jitsuzumi, Toshiya, 'Recent Development of Net Neutrality Conditions in Japan: Impact of Fiber Wholesale and Long-term Evolution (LTE), 26th European Regional ITS Conference, Madrid 2015 127152', (International Telecommunications Society, 2015), https://ideas.repec.org/p/zbw/itse15/127152.html.

In the case of the Philippines, the Public Telecommunications Policy Act[336] has avoided to establish network neutrally but has broad policy objectives such as keeping a healthy competitive environment.

All these differences reflect the ongoing debate about the advantages and disadvantages of network management practices and network neutrality itself, which can also be exemplified by the text agreed about it in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). According to Article 14.10 of the CPTPP, it is not against reasonable network management when internet access service suppliers offer its subscribers certain content on an exclusive basis.

INTERMEDIARY LIABILITY AND INTELLECTUAL PROPERTY RELATED REGULATIONS

During the development of the internet policy, Internet Service Providers -ISPs- (i.e., those providing users with internet access) were the main subject of regulation in the digital ecosystem. However, with the expansion of online activities, in addition to ISPs, a range of other actors including online platforms may be subject to legal liability for third-party use or content on their services. This has larger implications for e-commerce, which relies on platforms such as Alibaba and Mercado Libre, but also different payment and networking platforms. In this context, rules on ISP and other actors are often referred to as "internet intermediary liability rules" and aim to administrate the legal liability that these agents bear.

Previous policy studies have noted that appropriate limitations of liability for internet intermediaries "play an important role in promoting innovation and creativity, the free flow of information, and in providing the incentives for co-operation between stakeholders" [337] This is in contrast to a situation in which a strict liability regime could lead to the early or unnecessary blocking of content by the platform or to self-censorship by users given the heightened legal risk that they could be facing.[338] Yet this is a policy choice that depends on each economy, and as such internet intermediary liability regulation varies across APEC economies. The range of regulations spans from a liability protection zone; to conditional liability (often relying in safe harbors which exempt from liability if the intermediary adopts certain policy, for instance removing content upon request); to regulations posing greater liability. From a subject matter perspective, intermediary liability regulations could apply generally (i.e., to different kinds of content) or could be targeted to specific intellectual property (IP) rights (e.g., copyright). Finally, the very definition of what an intermediary is varies considerably across APEC

[336] The Philippines (Board of Investments), 'The Philippines Republic Act No. 7925', 2018, http://boi.gov.ph/sdm_downloads/ra-7925-public-telecommunications-policy-act-of-the-philippines/.

[337] OECD, 'OECD Council Recommendation Principles for Internet Policy Making', 2011, p.9, https://www.oecd.org/sti/ieconomy/49258588.pdf.

[338] OECD, 'The Role of Internet Intermediaries in Advancing Public Policy Objectives', 2011, p. 101-109, https://www.oecd.org/sti/ieconomy/theroleofinternetintermediariesinadvancingpublicpolicyobjectives.htm.

economies. In light of these considerations, a broad overview of relevant examples is provided below.

General safe harbors apply horizontally to any type of content and can be found in Japan; the United States; the Philippines; Brunei Darussalam; and Papua New Guinea. In the case of Japan, the Act on the Limitation of the Liability of Specific Telecommunications Service Providers (Act No. 137 of 2001) [339] covers all types of infringement. For the Philippines; Brunei Darussalam; and Papua New Guinea, ISP and intermediary rules are contained in Electronic Commerce Acts, [340] Electronic Transactions Acts, [341] and Cybercrime Policy [342] respectively. In the case of the United States, Section 230 of the Communications Decency Act insulates internet platforms from tort liability for user-generated content appearing on their platforms. Specifically, Section 230(c)(1) provides that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." Section 230(e)(2), however, contains a carve out for "any law pertaining to intellectual property."[343] At the same time, the United States also has specific safe harbors for copyright infringement as detailed below.

Intermediary liability regulations can also provide safe harbors for specific types of content, for instance copyright infringing content. As the internet amplifies the availability of copyrighted works, the online placement of such materials may be subjected to unrestricted reproduction and exchange. This can potentially harm copyright holders, which is the reason why several economies have had to rethink their IP domestic laws and adjust them to the digital environment. Beyond copyright, other IP rights can also be affected, for instance trademarks when counterfeit goods are offered in online platforms. That is why, intermediary liability rules should also aim at helping to enforce IP rights online while providing for scenarios where internet intermediaries can operate.

Different examples on how this balance could work are found among APEC economies. For instance, in the United States, the Digital Millennium Copyright Act provides safe harbors for

---

[339] Japan, 'Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders', 2001, http://www.japaneselawtranslation.go.jp/law/detail/?id=2088&vm=04&re=02.

[340] See: Section 30 of the Philippines' Electronic Commerce Act, exempts ISPs from any civil or criminal liability if it merely provides access with respect to the electronic data message or electronic document.

[341] See Chapter 196 of Brunei Darussalam Electronic Transactions Act 2001 which deals with access ISPs, providing that shall not be subject to any civil or criminal liability under any rule of law in respect of third-party material in the form of electronic records to which he merely provides access if such liability is founded on (a) the making, publication, dissemination or distribution of such materials or any statement made in such material; or (b) the infringement of any rights subsisting in or in relation to such material.

[342] See Cybercrime Policy of Papua New Guinea, which states that in cases where responsibility and or liability exists, legislation should limit the criminal responsibility and/or liability of ISPs and/or Access Providers on offences committed by users of their service, if the ICT provider (a) did not initiate the transmission, (b) - did not select the receiver; and (c) did not modify the information contained in the transmission. The criminal responsibility of Caching Providers should likewise be limited, if liability exists, for the automatic, intermediate and temporary storage of information.

[343] The United States, Communications Decency Act (CDA) of 1996, https://www.govinfo.gov/content/pkg/USCODE-2011-title47/html/USCODE-2011-title47-chap5-subchapII-partI-sec230.htm.

certain types of ISPs under specific circumstances.[344] In the case of Korea, its Copyright Act limits the liability of online service provider in cases where, once aware of the infringement, the provider "prevents or stops reproduction or transmission" of copyrights or other rights protected under the Act.[345] Other economies providing safe harbors for copyright infringement include Singapore;[346] Hong Kong, China;[347] Russia;[348] Canada;[349] Chinese Taipei;[350] Australia;[351] Malaysia;[352] and Chile.[353]

As observed, the limited liability and enjoyment of safe harbors is conditional to certain actions by the ISP. Some of those conditions include removing infringing content upon receiving notice. This is called 'notice and take down' (see Box 4.7). If these conditions are not met, the intermediary cannot rely on a safe harbor.

Box 4.7: Notice and take down regulations

ISP and internet intermediaries may be subject to notice and take-down regulations, which require the removal or disabling of copyright infringement material once they are alerted of a copyright infringement. However, notice and take down regulations can also be applied to other types of content.

While several APEC economies have notice and take down regulations (e.g., the United States; Japan; Thailand; Chile; Singapore; Korea; Malaysia; China; and Russia), there is a wide variation in the requirements for requesting them, as well as the process that follows. In some cases, a court order is required (e.g., Chile), while in others the process should not last longer than 24 hours (e.g., Viet Nam) or 48 hours (e.g., Malaysia).

In other cases, such as Canada, a "notice and notice" regime has been put in place. This means that if a copyright holder alerts the intermediary of infringement, the intermediary must forward the notice to the internet subscribers to alert them of the infringing activity.

Sources:

- The United States, Digital Millennium Copyright Act, 1998, https://www.copyright.gov/legislation/dmca.pdf
- Viet Nam, Circular No. 38/2016/TT-BTTTT providing detailed regulations on the cross-border provision of public information, 2013, Article 5, http://vbpl.vn/tw/Pages/vbpqen-toanvan.aspx?ItemID=11120; and, Decree No. 72/2013/ND-CP on the Management, provision and

[344] The United States, Digital Millennium Copyright Act, 1998, Title II, https://www.copyright.gov/legislation/dmca.pdf.
[345] Korea, Copyright Act, 2003, Article 102, https://www.wipo.int/edocs/lexdocs/laws/en/kr/kr058en.pdf.
[346] Singapore, Copyright Act (Chapter 63), https://sso.agc.gov.sg/Act/CA1987#pr193A-
[347] Hong Kong, China, Copyright ordinance, Article 205-4, https://www.elegislation.gov.hk/hk/cap528?tab=m&xpid=ID_1438403328788_001.
[348] Russia, Federal Law No. 364-FZ (Anti-Piracy Law), 2014, Section 4, https://rg.ru/2013/07/10/pravo-internet-dok.html.
[349] Canada, 'Copyright Act', 'R.S.C., 1985, c. C-42', 1985, https://laws-lois.justice.gc.ca/PDF/C-42.pdf.
[350] Chinese Taipei, 'Copyright Act', 2019, https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=J0070017.
[351] Australia, Copyright Act, 1968, latest amended in 2017, https://www.legislation.gov.au/Details/C2017C00094.
[352] Malaysia, Copyright Act, 1987, Article 43 (c) (1), http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20332%20-%20Copyright%20Act%201987%20Cetakan%20Semula%202013.pdf.
[353] Chile, Intellectual Property Law - Law 17.336, Article 85 Y, https://www.leychile.cl/Navegar?idNorma=28933.

use of internet services and online information, 2013, https://vnnic.vn/en/about/legaldocs/decree-no-72-2013-nd-cp-july-15-2013-management-provision-and-use-internet?lang=en

- Japan, Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders
- Thailand, Copyright Act (No. 2), Section 32/3, https://www.wipo.int/news/en/wipolex/2015/article_0006.html
- Chile, Intellectual Property Law (Law 17336), Articles 85 Q and R, https://www.leychile.cl/Navegar?idNorma=28933
- Singapore, Copyright Act, Section 193DDB, https://sso.agc.gov.sg/Act/CA1987#pr193A-
- Korea, Copyright Act Article 103, https://www.wipo.int/edocs/lexdocs/laws/en/kr/kr058en.pdf
- Malaysia, Copyright Act Article 43H, http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20332%20-%20Copyright%20Act%201987%20Cetakan%20Semula%202013.pdf
- People's Republic of China, Regulations on Protection of Communication through Information Network, 2006, https://wipolex.wipo.int/en/text/182147
- Russia, Federal Law No. 364-FZ (Anti-Piracy Law), 2014, Section 4, https://rg.ru/2013/07/10/pravo-internet-dok.html
- Canada, Notice and Notice Regime, https://ic.gc.ca/eic/site/oca-bc.nsf/eng/ca02920.html

Other models for liability

In China, the Administrative Measures on Internet Information Services requires internet intermediaries not to disseminate any illegal information (ranging from content that is against basic principles determined in the constitution, to content prohibited by laws or administrative regulations). The failure to sufficiently monitor this type of content, take it down or report violations, may carry fines, criminal liability, and revocation of business or media licenses.[354] On the other hand, Indonesia has a safe harbor policy applying only to e-commerce platforms, as stated in the Regulation No. 80 of 2019 on Trading through Electronic Systems.[355]

Lack of ISP liability rules

A final scenario is the lack of legislation pertaining to ISP liability. This is the case of New Zealand,[356] Mexico[357] and Peru. In the case of Peru, despite existing rules on ISP liability contained in the United States-Peru FTA,[358] the economy does not yet have any specific laws on this subject at the domestic level.

[354] People's Republic of China, Administrative Measures in Internet Information Services, http://www.china.org.cn/business/2010-01/20/content_19274704_4.htm.

[355] Indonesia, Regulation No. 80 of 2019 on Trading through Electronic Systems, https://jdih.setneg.go.id/viewpdfperaturan/P18728/PP%20Nomor%2080%20Tahun%202019.

[356] WIPO, Comparative Analysis Of The National Approaches To The Liability Of Internet Intermediaries, https://www.wipo.int/export/sites/www/copyright/en/doc/liability_of_internet_intermediaries.pdf.

[357] Garrote, Ignacio, Comparative Analysis on National Approaches to the Liability of Internet Intermediaries for Infringement of Copyright and Related Rights, p. 43, https://www.wipo.int/export/sites/www/copyright/en/doc/liability_of_internet_intermediaries_garrote.pdf.

[358] The United States-Peru Free Trade Agreement (2006), Article 16.11 (29) 'Limitations on Liability for Service Providers', https://ustr.gov/sites/default/files/uploads/Countries%20Regions/africa/agreements/pdfs/FTAs/peru/16%20IPR%20Legal.June%2007.pdf.

International commitments for the protection of copyright online

IP laws had also been adjusted at the international level to deal with the expansion of internet-enabled activities. For instance, the 2002 World Intellectual Property Organization (WIPO) Copyright Treaty (WCT) enacted greater restrictions on the use of technology to copy works in the economies that ratified it. The WCT provisions fill the gaps of earlier international laws in the subject, such as the World Trade Organization's Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) of 1995. At the same time, Article 7 of the WCT extends the applicability of the reproduction right and the exceptions and limitations thereunder to the digital environment. This alleviates the challenges faced by ISPs, which before the adoption of the Treaty faced liability for the interim copy of copyrighted works (which is necessary for the internet to work as reproduction of content is an intrinsic feature of transferring information online). Out of the 21 APEC economies, 17 of them have ratified the WCT.[359]

FTAs contain international rules on intermediary liability. For example, the United States-Mexico-Canada Agreement (USMCA) sets limits to intermediary liability. The USMCA requires parties to provide limitations in their laws that have the effect of precluding monetary relief against intermediaries for copyright infringements "that they do not control, initiate, or direct, and that take place through systems or networks controlled or operated by them or on their behalf". However, parties must provide certain requirements for intermediaries to meet in order to qualify for this limitation on liability, including requiring intermediaries to remove or disable access to copyright infringing content on their networks upon obtaining knowledge of its existence. The requirements and conditions under which intermediaries qualify for this limitation are set out in Article 20.88 of the USMCA.[360]

ONLINE CONTENT RELATED REGULATIONS

While the internet contains different types of lawful material, it also contains offensive and unlawful material. Internationally, there is divergence on the kind of material that is deemed unlawful, but materials such as extreme violence and child pornography are generally seen as not desirable. In this regard, various APEC economies have issued regulations to control specific kinds of offensive content. A broad clustering of the main issues deemed unlawful or requiring content moderation is described below.

[359] WIPO, Contracting Parties: WIPO Copyright Treaty, https://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=16.
[360] USMCA, Article 20.88.

Special regulations targeted at child pornography

There are cases where economies have introduced specific regulations to prevent the online distribution of child pornography, for instance Peru[361], the Philippines[362] and Chinese Taipei[363]. In the case of Korea, the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (Network Act)[364] is complemented by the Juvenile Protection Act, [365] which restricts content harmful to children. Indonesia has enacted Regulation No. 19 of 2014 on Controlling Internet Websites Containing Negative Content, which contains provisions that require "negative content" to be filtered. The filtering is done at the ISP level, against an approved blacklist. While the regulation does not provide the definition of "negative content", it has previously been reported that contents relating to privacy, child pornography, religious or ethnic violence, or that which could result in social unrest, would qualify as "negative content".

Special regulations targeted at domestic security, public order and/or the deterrence of offensive acts undertaken online

Other types of content that can render ISP liable concern the protection of domestic security, public order and/or the deterrence of offensive acts undertaken online. For example, Viet Nam's Decree No. 72/2013/ND-CP on the Management, Provision, Use of Internet Services and Information Content Online, prohibits the use of internet services for reasons defined in the law.[366] In the case of Russia, the Federal Law No. 149-FZ on Information, Information Technologies and Information Protection establishes certain grounds for the regulation of online content, including offenses to human dignity and public morality, the disrespect of the Russian Federation, and violation of Russian Law among others.[367] China has recently issued the Provisions on Ecological Governance of Network Information Content, [368] which safeguards various issues including domestic security and public interests.

---

[361] Peru, Regulation implementing Law 30254 on the Safe and Responsible Use of Information and Communication Technologies by Children and Teenagers, 'Supreme Decree 093-2019-PCM', 2019, https://busquedas.elperuano.pe/normaslegales/aprueban-el-reglamento-de-la-ley-n-30254-ley-de-promocion-decreto-supremo-n-093-2019-pcm-1768942-2/.

[362]; The Philippines, Act Defining the Crime of Child Pornography, Prescribing Penalties Therefor and for other Purposes, 'Republic Act Np- 9775', 2009, https://www.lawphil.net/statutes/repacts/ra2009/ra_9775_2009.html.

[363] Chinese Taipei, Child and Youth Sexual Exploitation Prevention Act (1995), https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=D0050023.

[364] Korea, Act on Promotion of Information and Communications Network Utilization and Information Protection, 2016, https://elaw.klri.re.kr/eng_service/lawView.do?hseq=38422&lang=ENG.

[365] Korea, Juvenile Protection Act, Act No. 14067, 2016, https://elaw.klri.re.kr/eng_service/lawView.do?hseq=38401&lang=ENG.

[366] Viet Nam, Decree No. 72/2013/ND-CP on the Management, Provision, Use of Internet Services and Information Content Online, 2013, Article 5, https://vnnic.vn/sites/default/files/vanban/Decree%20No72-2013-ND-CP.PDF.

[367] Russia, Federal Act No. 149-FZ "On Information, Information Technologies and Protection of Information", 2006, Article 15, http://www.consultant.ru/document/cons_doc_LAW_61798/.

[368] People's Republic of China, Provisions on Ecological Governance of Network Information Content, 2019, http://www.cac.gov.cn/2019-12/20/c_1578375159509309.htm.

Misinformation online

Several economies have regulations to combat online misinformation. This is the case for Singapore, where the Protection from Online Falsehood and Manipulation Act (POFMA)[369] aims to tackle online falsehoods that harms public interest. Under POFMA, internet intermediaries may be required to surface a correction to users who have seen a falsehood (Section 21) or take steps to stem the spread of misinformation (including if necessary its online removal) (Section 22). Thailand has also recently adopted its Computer Crimes Act,[370] which criminalizes the sharing and publication of false information. However, the Act does not have a mandate to impose punishments on ISPs if they cooperate in removing illicit content from their sites upon receiving a court order.

No online content regulation

Some APEC economies have no specific laws or regulations targeted at regulating online content. This is the case for Australia or Canada. However, this does not mean that illegal acts, when undertaken online, are not punishable. In fact, child pornography is illegal in Canada under Section 163.1(4.1) of the Criminal Code, whether it happens offline or online.[371]

OPEN GOVERNMENT DATA

Every APEC economy has either a wide policy, plan or law toward an open government data environment, or an available open data portal. This has been influenced by the membership of some economies to open data or open government international frameworks. For instance, some economies (e.g., Australia; Canada; Chile; Indonesia; Korea; Mexico; New Zealand; Peru; the Philippines; and the United States) are part of the Open Government Partnership,[372] which promotes among others, the implementation of Access to Information Laws and Open Data portals. In addition, seven economies are part of the Open Data Charter (i.e. Australia; Canada; Chile; Korea; Mexico; New Zealand; and the Philippines). The Charter advances six principles on how to publish data: 1) open by default; 2) timely and comprehensive; 3) accessible and usable; 4) comparable and interoperable; 5) for improved governance and citizen engagement; and 6) for inclusive development and innovation.

Among APEC economies, specific efforts to implement Open Data goals have taken different policy approaches. Some economies have passed specific Open Data laws. This is the case of

[369] Singapore, 'Protection from Online Falsehoods and Manipulation Act', 2009, https://sso.agc.gov.sg/Act/POFMA2019?ValidDate=20191002.
[370] Thailand, 'Computer Crimes Act (No. 2) B.E. 2560', 2017.
[371] Canada, 'Criminal Code', 'R.S.C., 1985, c. C-46', 1985, https://laws-lois.justice.gc.ca/eng/acts/c-46/page-1.html.
[372] Open Government Partnership, 'Digital Governance', Accessed February 6, 2020, https://www.opengovpartnership.org/policy-area/digital-governance/.

Chinese Taipei;[373] the United States;[374] Peru; [375] Korea;[376] Russia,[377] and the Philippines.[378] Some other economies have complemented legislation with open data action plans. This is the case of New Zealand, whose declaration on open and transparent government dates back to 2011. It also has an open data action plan, which took effect on 1 July, 2017, following public consultation, and sets out goals and initiatives to 30 June 2020.

Other economies have laws promoting access to information. This is the case for China's recent Open Government Information Regulation;[379] and Canada's Access to Information Act of 1982.[380] These laws do not tackle specifically the reuse of datasets, but apply broadly to government-held information stored online or offline.

Finally, in the case of economies that do not have a law or regulation regarding open data, the release of open datasets have occurred following the implementation of open data portals, as Table 4.2 shows.

Table 4.2: Open Data Portals of APEC economies

Economy	Open data portal
Australia	data.gov.au
Brunei Darussalam	data.gov.bn
Canada	open.canada.ca/en/opendata
Chile	datos.gob.cl
Hong Kong, China	data.gov.hk
Indonesia	data.go.id
Japan	data.go.jp
Korea	data.go.kr
Malaysia	data.gov.my
Mexico	datos.gob.mx
New Zealand	data.gov.nz
Peru	datosabiertos.gob.pe
The Philippines	data.gov.ph
Russia	data.gov.ru

[373] Chinese Taipei (National Development Council), 'Open Data Regulations', 2020, https://www.ndc.gov.tw/en/Content_List.aspx?n=5CA9F5695922B90B.

[374] The United States, 'Foundations for Evidence-Based Policymaking Act of 2017', Pub. L. No. H.R.4174, 2019, https://www.congress.gov/bill/115th-congress/house-bill/4174/text.

[375] Peru, 'Supreme Decree No- 16-2017-PCM, which approves the National Strategy of Open Government Data for 2017-2021 and the Open Government Data Model', 2017, https://www.datosabiertos.gob.pe/ds2017.pdf.

[376] Korea, 'Act on the Provision and Use of Public Data', Act No. 11956, 2013, https://elaw.klri.re.kr/eng_service/lawView.do?hseq=30365&lang=ENG.

[377] Russia, Federal Law149-FZ, https://www.wipo.int/edocs/lexdocs/laws/en/ru/ru126en.pdf.

[378] The Philippines, 'Open Data Joint Memorandum Circular 2015-01', 2015 https://www.dbm.gov.ph/wp-content/uploads/Issuances/2015/Joint%20Memorandum%20Circular/JMC%28OP-DBM-PCDSPO%29%20NO.%202015%20-%201%20DATED%20MAY%2018,%202015.pdf.

[379] People's Republic of China, 'Order No. 711 of the State Council of the People's Republic of China', 2019, http://www.gov.cn/zhengce/content/2019-04/15/content_5382991.htm.

[380] Canada, 'Access to Information Act (R.S., 1985, c. A-1)', 1985, https://laws-lois.justice.gc.ca/eng/acts/A-1/index.html.

Singapore	data.gov.sg
Chinese Taipei	data.gov.tw/en
Thailand	data.go.th/default.aspx
United States	data.gov
Viet Nam	itrithuc.vn

Source: Compilations by APEC PSU.

4.3 FOCUS AREA C: CONSUMER PROTECTION AND PRIVACY ISSUES

CONSUMER PROTECTION

All APEC economies have consumer protection laws and regulations. In some economies, these laws can also be found at the state/provincial level. For instance, while an overarching consumer protection law is enacted in the United States through the Federal Trade Commission Act, more in-depth consumer protection laws are available at the state (e.g. Florida[381]) and city levels (e.g. New York City[382]). In a similar vein, economies have also enacted sector-specific regulations. As an example, Article 15 of the Advertising Law of the People's Republic of China indicates specific advertising guidelines for the prescription drug industry.[383] An analysis of these consumer protection laws and regulations showed that there are variations in how the different aspects are covered.

Extent of E-commerce Coverage

While consumer protection laws among APEC members broadly cover e-commerce transactions, only some such as Malaysia[384] and Mexico[385] have made specific references to it. This is not surprising as many of these laws were first introduced before e-commerce became mainstream (e.g., early 1990s). At the same time, it should be noted that while consumer protection regulations in APEC economies generally do not make explicit reference to e-commerce, none of them exclude e-commerce, indicating that consumer protection laws are rather flexible and arguably can be applied to e-commerce as well.

Some economies have also taken additional steps to introduce specific regulation or modify statutes to address issues affecting e-commerce, such as online fraud and online advertisement. An example is Korea which has introduced the "Act on the Consumer Protection in Electronic

[381] Florida, 'Regulation of Trade, Commerce, Investments, and Solicitations', Chapter 501. http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Index&Title_Request=XXXIII#TitleXXXIII.

[382] New York City, 'Consumer Protection Law', last amended 2011. https://www1.nyc.gov/assets/dca/downloads/pdf/about/ConsumerProtectionLawPacket.pdf.

[383] China, 'Advertising Law of the People's Republic of China (2015)', Article 15. https://www.hfgip.com/sites/default/files/law/advertising_law_16.02.2016.pdf.

[384] Malaysia, 'Consumer Protection Act 1999', last amended 1 September 2016, Article 2. http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act 599 - 29.08.2016.pdf.

[385] Mexico, 'Federal Consumer Protection Law 2006'. Chapter 8. https://www.profeco.gob.mx/juridico/pdf/l_lfpc_06062006_ingles.pdf.

Commerce" to better protect the rights and interests of consumers who participate in e-commerce transactions. Specifically, Article 7 helps protect consumers against their own input errors.[386] The United States has enacted guidelines for social media influencers to better inform them on the laws surrounding deceptive advertising given their impact on e-commerce sales.[387]

Misleading, deceptive and/or fraudulent practices

An evaluation of what constitutes misleading, deceptive and/or fraudulent practices is important in the context of e-commerce. This is particularly so considering that consumers are primarily reliant on product information and on contract terms provided by suppliers when deciding to make their purchases. Clarifying the dos and don'ts provides clarity to online suppliers and ensures that consumers are protected.

Many APEC economies have made efforts to define such practices but the breadth of coverage differs across economies. While some regulations focus specifically on the transaction of goods and services, some have included other areas. For instance, the Australian Competition and Consumer Act includes pyramid schemes and pricing within its definition of unfair practices.[388] Similarly, Indonesia's Consumer Protection Law covers deceiving/misleading practices for the provision of goods and services as well as advertising, auctions and lotteries.[389] Although these areas are all important in the context of consumer protection, some are more closely related to e-commerce and are further elaborated on below.

Provision of goods and services

From the perspective of goods and services provision, two areas that economies have deemed as misleading, deceptive and/or fraudulent practices includes the provision of false/misleading information and the use of aggressive commercial practices. For the former, Australia's Competition and Consumer Act highlights that a seller should not misrepresent a product or a service to be new, of a particular standard, quality, value of grade among others.[390] Brunei Darussalam's Consumer Protection (Fair Trading) Order stipulates that unfair practices include situations where a supplier omits information, makes a false claim or takes advantage of a consumer.[391]

---

[386] Korea, 'Act on the Consumer Protection in Electronic Commerce', etc 29 March 2016, Article 7. https://elaw.klri.re.kr/eng_service/lawView.do?hseq=38513&lang=ENG.

[387] United States Federal Trade Commission. (2019). 'Disclosure 101 for Social Media Influencers'. Retrieved from https://www.ftc.gov/system/files/documents/plain-language/1001a-influencer-guide-508_1.pdf.

[388] Australia, 'Competition and Consumer Act 2010', Last amended 2019, https://www.legislation.gov.au/Details/C2020C00079/Html/Volume_3#_Toc32223193.

[389] Indonesia, 'Law of the Republic of Indonesia Number 8 Year 1999', https://aseanconsumer.org/file/pdf_file/04%20Law-No.-8-Concerning-Consumer-Protection.pdf.

[390] Australia, 'Competition and Consumer Act 2010', Last amended 2019, https://www.legislation.gov.au/Details/C2020C00079/Html/Volume_3#_Toc32223193.

[391] Brunei Darussalam, 'Consumer Protection (Fair Trading) Order 2011', Article 4, http://extwprlegs1.fao.org/docs/pdf/bru113413.pdf.

For the latter, Hong Kong, China's Trade Descriptions Ordinance indicates that a commercial practice can be considered aggressive if it impairs the average consumers' freedom of choice or conduct through the use of harassment, coercion or undue influence and causes the consumers to make a decision that they would not have made otherwise.[392] Article 15 of Indonesia's Consumer Protection Law prohibits businesses from offering goods and/or services by using force or any other methods, which can cause either physical or psychological annoyance to the consumers.[393]

Box 4.8: Consumer Protection and COVID-19

The panic buying caused by COVID-19 has resulted in a huge demand for medical products. While this has further fueled the adoption and growth of e-commerce, it has also led to an overwhelming increase in demand for these products and related unscrupulous practices such as false advertisements on the efficacy of certain products against COVID-19. There has also been a rise in cases where consumers did not receive the products that they have paid for and/or had their personal information stolen from them. The fact that consumers are unable to assess the products until delivery has further exacerbated this issue.

APEC economies have scrambled to stop these practices. For instance, Singapore has removed more than 1,700 listing of products that have been falsely advertised with COVID-19 related claims as of 6 May 2020. Ontario, Canada has issued an emergency order to tackle price gouging of essential items that could result in fines as high as CAD10 million if it involves a corporation, or imprisonment of up to one year if it involves an individual. In the United States, the Federal Trade Commission has released advice for how consumers can avoid COVID-19 scams, considering that more than 22,000 consumer complaints (which amounted to total losses of USD22 million) were received between January 2020 and mid-April 2020.

This crisis has re-affirmed the importance of consumer protection laws, in particular concerning e-commerce and the need for effective enforcement and penalties to be in place to deter such practices. In addition, the WTO has reiterated the importance of international cooperation in the development of e-commerce policies given how it has supported small businesses in times of crisis. Hong Kong, China has, in anticipation of an upsurge of disputes arising from or relating to COVID-19, launched a COVID-19 Online Dispute Resolution Scheme enabling affected persons to settle disputes at a very low cost.

Sources:

- The Straits Times. (2020, May 6). Coronavirus: 1,600 sellers warned by HSA for falsely claiming products protect against Covid-19. Retrieved from

[392] Hong Kong, China, 'Cap. 362 Trade Description Ordinance', Article 13F. https://www.elegislation.gov.hk/hk/cap362.

[393] Indonesia, 'Law of the Republic of Indonesia Number 8 Year 1999', Article 15. https://aseanconsumer.org/file/pdf_file/04%20Law-No.-8-Concerning-Consumer-Protection.pdf.

https://www.straitstimes.com/singapore/coronavirus-1600-sellers-warned-by-hsa-for-falsely-claiming-products-protect-against-covid
- Consumer Protection Ontario. (n.d.). Report price gouging related to coronavirus (COVID-19). Retrieved from https://www.ontario.ca/page/report-price-gouging-related-coronavirus-covid-19
- United States Federal Trade Commission. (n.d.). Coronavirus Advice for Consumers. Retrieved from https://www.ftc.gov/coronavirus/scams-consumer-advice
- https://www.ebram.org/covid_19_odr.html
- OECD (2020). Protecting online consumers during the COVID-19 crisis. Retrieved from https://read.oecd-ilibrary.org/view/?ref=130_130819-ay45n5rn74&title=Protecting-online-consumers-during-the-COVID-19-crisis
- WTO (2020). E-commerce, trade and the Covid-19 Pandemic. Retrieved from https://www.wto.org/english/tratop_e/covid19_e/ecommerce_report_e.pdf

Contract Terms

Beyond goods and services provision, misleading, deceptive and/or fraudulent practices can manifest within contracts. While the section on Focus Area A (electronic transactions framework) discusses the validity of e-contracts relative to their physical counterparts, this section looks into what constitutes as acceptable terms in contracts. As an illustration, Malaysia defines unfair contract terms as those that provide an unfair advantage to the supplier or consumer or if the circumstances within which a contract was signed is unfair.[394] In the same vein, Article 15 (2) of Ontario (Canada)'s Consumer Protection Act indicated that unconscionable practices include situations when *"the terms of the consumer transaction are so adverse to the consumer as to be inequitable."*[395]

Advertising

Given the role of advertising in potentially increasing sales, misleading, deceptive and/or fraudulent practices are observed within advertisements as well. In response, several economies have enacted regulations to help better identify and provide guidance on advertising practices that are not acceptable. One form of advertising which can be considered as such is bait advertising. Australia defines this as a practice where suppliers advertise goods and service at a price with no reasonable ground for which they are aware of. Assuming that a party manages to supply these goods and services at the advertised prices, they have to be sold within a reasonable period considering the nature of the market and the advertisement.[396] Another form of advertising that is considered misleading, deceptive and/or fraudulent is the misrepresentation of information. In response to this, The City of New York's (the United States) Consumer Protection Law provides specific information on the way goods and services can be represented, and how words such as "free" as well as its synonyms can be used. Beyond

[394] Malaysia, Consumer Protection Act 1999, Last amended 2016, Article 24c. http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act 599 - 29.08.2016.pdf.
[395] Canada (Ontario), Consumer Protection Act 2002, Article 15(2). https://www.ontario.ca/laws/statute/02c30.
[396] Australia, Competition and Consumer Act 2010, Last amended 2019, Article 35. https://www.legislation.gov.au/Details/C2020C00079/Html/Volume_3#_Toc32223193.

the use of specific words, the Law also extends to the usage of out-of-context quotes. Specifically, it does not allow quotes by individuals to be rearranged or abstracted such that it alters the intended message.[397]

Transparency

Information transparency is particularly relevant to products sold through e-commerce, as issues such as the inability to assess them physically means that some information asymmetry are embedded within such transactions. Article 20 of the Law of the People's Republic of China on the Protection of Consumer Rights and Interests stipulates that "Business operators shall provide consumers with true and complete information on the quality, performance, use, and useful life, among others, of commodities or services; and shall not conduct any false or misleading promotion."[398] Similar information is found within Indonesia's regulation, which stipulates that entrepreneurs should fulfill certain labelling requirements.[399]

Liability of Advertisers

The section on Focus Area B (openness and cross-border issues) covers the liability of platforms with regards to IP infringement. This section touches on the liability of advertisers, in particular if they publish information about goods and services that are false and/or misleading. Article 17 of Indonesia's Consumer Protection Law prohibits advertisers from deceiving, providing inaccurate or lack of information as well as violating the ethical and/or legal provisions of advertising.[400] Article 23 of Chinese Taipei's Consumer Protection Act indicates that advertisers should ascertain that their advertisements are true for situations whereby advertisers know or should have known claims made to be false.[401]

If these advertising requirements are not met, some economies have included provisions to hold advertisers liable unless proven innocent. For instance, Article 20 of Singapore's Consumer Protection (Trade Description and Safety Requirements) Act indicates that it is the onus of the individual to prove that he/she merely served as an advertising platform and had no reason to suspect that its publication would contravene a law.[402] Article 56 of the Law of the People's Republic of China on the Protection of Consumer Rights and Interests indicates that the

[397] New York City, Consumer Protection Law, Last amended 2011, Section 5-65. https://www1.nyc.gov/assets/dca/downloads/pdf/about/ConsumerProtectionLawPacket.pdf.
[398] China, Law of the People's Republic of China on the Protection of Consumer Rights and Interests, Last amended 2013, Article 20. http://www.lawinfochina.com/display.aspx?id=e0a656d399acddc2bdfb&lib=law.
[399] Indonesia, Law of the Republic of Indonesia Number 8 Year 1999, Article 8. https://aseanconsumer.org/file/pdf_file/04%20Law-No.-8-Concerning-Consumer-Protection.pdf.
[400] Indonesia, Law of the Republic of Indonesia Number 8 Year 1999, Article 17. https://aseanconsumer.org/file/pdf_file/04%20Law-No.-8-Concerning-Consumer-Protection.pdf.
[401] Chinese Taipei, Consumer Protection Act, Last amended 2015, Article 23. https://cpc.ey.gov.tw/en/FC9F20A6623A8B4C
[402] Singapore, Consumer Protection (Trade Descriptions and Safety Requirements) Act 1975, Last amended 2013, Article 20. https://sso.agc.gov.sg/Act/CPTDSRA1975.

advertiser is responsible for any damage caused to consumers as a result of false advertisements that aim to defraud or mislead them.[403]

On the other hand, some economies have stipulated that advertisers should not be held liable for the factual accuracy of the advertisements run. For instance, Ontario (Canada) has indicated that no liability is borne by the advertisers.[404] Article 124 of the Consumer Act of the Philippines has indicated that the liability of false advertisements does not lie on the publisher of advertisements, assuming that the publisher does not withhold information on the name and post office address of the supplier; however, this provision does not absolve suppliers and advertisers from legal liability for the false advertisements.[405]

Claim Period

APEC economies have included provisions to provide clarity on the time period where consumers ought to have made their claims, although these provisions tend to vary. This is particularly relevant for e-commerce where consumers are often unable to review the product until it is received. As an example, for goods that are defective, consumer protection laws in China require the consumer to take action within 6 months,[406] while in Australia, the period is significantly longer at approximately 3 to 10 years depending on the situation.[407]

Box 4.9: Scope of application of laws

Some APEC economies have extra-territorial provisions in their consumer protection laws. For instance, section 21A of Hong Kong, China's Trade Descriptions Ordinance, Cap. 362, indicates that the law is extra-territorial in nature. A trader is deemed to have committed an offence with respect to a commercial practice even if the practice is directed to consumers outside the territory of Hong Kong, China, provided that at the time of engaging in the practice, the trader is in Hong Kong, China or Hong Kong, China is the trader's usual place of business. Similarly, Russia's adoption of the Overview of the Court Practice related to Protection of Consumer Rights with regard to Sale of Goods and Services has allowed consumers in Russia to raise claims against a firm that sells or promotes the good in Russia but is domiciled outside the economy.

However, other APEC economies have indicated that their laws are only applicable within their territory. As an illustration, Article 2 of Viet Nam's Law on Protection of Consumer

[403] China, Law of the People's Republic of China on the Protection of Consumer Rights and Interests, Last amended 2013, Article 56. http://www.lawinfochina.com/display.aspx?id=e0a656d399acddc2bdfb&lib=law

[404] Canada (Ontario), Consumer Protection Act 2002, Article 17(3). https://www.ontario.ca/laws/statute/02c30

[405] The Philippines, The Consumer Act of the Philippines 1992, Article 124. https://www.lawphil.net/statutes/repacts/ra1992/ra_7394_1992.html

[406] China, 'Law of the People's Republic of China on the Protection of Consumer Rights and Interests', Last amended 2013, Article 23. http://www.lawinfochina.com/display.aspx?id=e0a656d399acddc2bdfb&lib=law

[407] Australia, 'Competition and Consumer Act 2010', Last amended 2019, Article 143. https://www.legislation.gov.au/Details/C2020C00079/Html/Volume_3#_Toc32223193

Rights states that "This Law applies to consumers; goods and service traders; agencies, organizations and individuals involved in the protection of consumer rights in the territory of Vietnam."

With the growing number of economies having laws with extra-territorial effects, international cooperation has become increasingly important. One such initiative participated by APEC economies is the International Consumer Protection Enforcement Network (ICPEN). It is a multilateral forum that brings together consumer protection law enforcement authorities across several economies (Table 4.3). Some key initiatives undertaken by the network includes its econsumer.gov initiative which allows consumers to report cross-border issues via a single platform which is participated in by 36 economies.

Table 4.3: International Consumer Protection Enforcement Network (ICPEN) Membership

Economy	ICPEN member?	Year Joined
Australia	Yes	1992
Brunei Darussalam	No	-
Canada	Yes	1992
Chile	Yes	2005
China	Yes	2006
Hong Kong, China	No	-
Indonesia	No	-
Japan	Yes	1992
Korea	Yes	1996
Malaysia	No	-
Mexico	Yes	1994
New Zealand	Yes	1992
Papua New Guinea	Yes	2012
Peru	Yes	2015
The Philippines	Yes	2014
Russia	No	-
Singapore	No	-
Chinese Taipei	No	-
Thailand	No	-
United States	Yes	1992
Viet Nam	Yes	2013

APEC economies have also engaged in other multilateral and bilateral consumer protection initiatives. For instance, Australia is a member of the London Action Plan on International Spam Enforcement Cooperation. It has also signed several memorandums of understanding on consumer protection issues with other economies such as China and New Zealand. Similarly, the Philippines has participated in the Global Privacy Enforcement Network and Chinese Taipei is part of the Unsolicited Communications Enforcement Network among others.

Sources:

- Viet Nam, Law on Protection of Consumer Rights. http://vietnamlawmagazine.vn/law-on-protection-of-consumer-rights-4688.html
- Hong Kong, China, Cap. 362 Trade Description Ordinance. https://www.elegislation.gov.hk/hk/cap362
- Russia, Overview of the Court Practice related to Protection of Consumer Rights with regard to Sale of Goods and Services 2018
- econsumer.gov. (n.d.). Retrieved April 2020 from https://www.econsumer.gov/en/FileAComplaint#crnt

UNSOLICITED COMMERCIAL ELECTRONIC MESSAGES/SPAM

In the context of e-commerce, unsolicited commercial electronic messages or SPAM are often sent to promote commercial products or services to individuals without their consent.[408] SPAM has also been used to deceive individuals and disrupt networks among others. Many APEC economies have enacted regulations pertaining to SPAM. Some common characteristics of these laws are highlighted below.

Interpretation and types of Consent

Defining consent

Consent is often a key element within SPAM regulations. The OECD highlights three main types of consent (Table 4.4).

Table 4.4: Definitions of Consent

Type of Consent	Description of Consent
Express Consent (opt-in)	A form of consent where an individual or organization has actively given their consent to a particular action or activity.
Implicit Consent	This is consent which generally can be inferred from the conduct and/or other business relationships of the recipient.
Assumed Consent (opt-out)	There is a presumption of consent until it is removed by the recipient, for example by unsubscribing or by placing their electronic address on a do-not contact-list

Source: Report of the OECD Task Force on SPAM: Anti-SPAM Toolkit of Recommended Policies and Measures (http://www.oecd.org/internet/consumer/36494147.pdf)

The express consent approach is often also referred to as the opt-in approach, which "prohibits the sending of unsolicited electronic messages unless a prior relationship exists with the recipient or if the recipient has given his/her consent."[409] An example of express consent can be seen in the United States' CAN-SPAM Act; it defined "affirmative consent" as: (1) when

[408] OECD. (2006). OECD Anti-Spam Toolkit of Recommended Policies and Measures. Retrieved from https://www.oecd-ilibrary.org/science-and-technology/oecd-anti-spam-toolkit-of-recommended-policies-and-measures_9789264027176-en.
[409] OECD. (2004). Background Paper for the OECD Workshop on Spam.

the individual provides express consent to receiving the message; and (2) if the information was received from a third party, the individual must have been given clear and conspicuous notice that their email will be transferred over to another party for the purpose of receiving commercial messages.[410] The Philippines stipulates that advertisers can only send messages to individuals who have provided prior consent or have opted in to receive the message without incurring additional costs.[411]

"Assumed consent" is often also referred to as the opt-out approach, where prior consent is not required. Instead, it gives the individuals an opportunity to remove themselves from the electronic message upon request.[412] An example of an economy employing this approach is Japan; Article 4 of its Act on Regulation of Transmission of Specified Electronic Mail notes that electronic mail should not be sent to individuals who have already indicated their request not to receive it.

Implicit consent is also covered in regulation where the conditions that ought to be met are outlined before consent can be assumed to be implied. For instance, Hong Kong, China's Unsolicited Electronic Messages Ordinance stipulates that consent can be provided either through express consent or through "consent that can reasonably be inferred from the conduct of the individual or organization concerned."[413] New Zealand's Unsolicited Messages Act 2007 allows consent to be inferred from the "the conduct and the business and other relationships of the persons concerned."[414] While some regulations provide room for consent to be implied, others take a stronger stance against it. For example, the Philippines' House Bill No. 3629 introduced in 2016 defines consent as when a written contract is signed between the subscriber and the content provider agreeing to receive advertisements.[415]

Scope of the law

Technology

Laws on SPAM can either be technology-specific (i.e., where the law refers explicitly to certain messaging technology) or technology-neutral. While specifying the technology in the regulations could give more clarity, being technology-neutral allows for the law to be more flexible in accommodating current technology and future ones without any amendments.[416]

---

[410] The United States, 'Public Law 108-187', 2003, Section 3. https://www.ftc.gov/sites/default/files/documents/cases/2007/11/canspam.pdf.

[411] The Philippines, 'House Bill No. 3629', 2016, Section 6. http://www.congress.gov.ph/legisdocs/basic_17/HB03629.pdf.

[412] OECD. (2004). Background Paper for the OECD Workshop on Spam.

[413] Hong Kong, China, Cap. 593 Unsolicited Electronic Messages Ordinance, Article 5. https://www.elegislation.gov.hk/hk/cap593.

[414] New Zealand, Unsolicited Electronic Messages Act 2007, Article 4. http://www.legislation.govt.nz/act/public/2007/0007/latest/whole.html#DLM405141.

[415] The Philippines, House Bill No. 3629, 2016, Section 6. http://www.congress.gov.ph/legisdocs/basic_17/HB03629.pdf.

[416] OECD. (2006). OECD Anti-Spam Toolkit of Recommended Policies and Measures. Retrieved from https://www.oecd-ilibrary.org/science-and-technology/oecd-anti-spam-toolkit-of-recommended-policies-and-measures_9789264027176-en.

Many APEC economies have implemented technology-neutral laws. For instance, Hong Kong, China defined electronic message as "message in any form sent over a public telecommunications service to an electronic address and includes, but is not limited to: (a) a text, voice, sound, image or video message; and (b) a message combining text, voice, sound, images or video".[417] Similarly, Australia indicates that an electronic message is one that uses an internet or listed carriage service and is sent to an electronic address in connection with an email, instant messaging, telephone or similar account.[418]

At the other end of the spectrum, some economies have excluded certain technologies through their SPAM regulations. For example, the Philippines stipulates that unsolicited messages cannot be sent using broadcast messages services, which refers to a "system which allows the sending of the same short messaging service (SMS) or multimedia messaging service (MMS) message to a large number of mobile phones."[419]

Determination of bulk messages

Among APEC economies, Singapore and Hong Kong, China have defined what should be regarded as bulk messages. Singapore's SPAM Control Act 2008 considers the following to be bulk message: (a) more than 100 electronic messages containing the same or similar subject-matter during a 24-hour period; (b) more than 1,000 electronic messages containing the same or similar subject-matter during a 30-day period; or (c) more than 10,000 electronic messages containing the same or similar subject-matter during a one-year period.[420] Part 3 (Rules about Address-harvesting and Related Activities) and Part 4 (Fraud and Other Illicit Activities Related to Transmission of Commercial Electronic Messages) of Hong Kong, China's Unsolicited Electronic Messages Ordinance views the following as the transmission of multiple commercial electronic messages: (a) more than 100 commercial electronic messages during a 24-hour period; or (b) more than 1,000 commercial electronic messages during a 30-day period.

Content of SPAM messages

Laws on unsolicited messages have gone beyond just regulating the transmission of electronic messages but also their content. Generally, many economies with SPAM-related regulations have included stipulations that cover the content of the messages. While the language used may differ across regulations, they generally mandate electronic messages to contain at least three of the following components: 1) identity of the individual or organization that authorized sending the message; 2) accurate information on how the sender can be contacted; and 3) an option to unsubscribe. The different means by which they have been included within a regulation is illustrated in the following examples. Canada indicates that all electronic

[417] Hong Kong, China, Cap. 593 Unsolicited Electronic Messages Ordinance, Article 2. https://www.elegislation.gov.hk/hk/cap593.
[418] Australia, 'Spam Act 2003', Article 5. https://www.legislation.gov.au/Details/C2016C00614.
[419] The Philippines, 'House Bill No. 3629', 2016 Section 3. http://www.congress.gov.ph/legisdocs/basic_17/HB03629.pdf
[420] Singapore, 'Spam Control Act', Last amended 2020, Article 6. https://sso.agc.gov.sg/Act/SCA2007.

messages should comply with the following requirements: a) set out prescribed information that identifies the person who sent the message and the person — if different — on whose behalf it is sent; b) set out information enabling the person to whom the message is sent to readily contact one of the persons referred to in paragraph a); and c) set out a mechanism to unsubscribe.[421] The Advertising Law of the People's Republic of China states that electronic advertisements are to clearly indicate the identity and contact information of the seller as well as provide the recipient with a method to unsubscribe.[422]

It is worthwhile to note that while the option to unsubscribe may not be indicated within the provisions which specify the content requirements of messages, it may be included in other provisions. This is the case of the Philippines, where Section 7 of House Bill No. 3629 outlines the need for an opt-out mechanism to be provided to subscribers at no cost.[423]

Beyond the content of the message, some economies have stipulated that the information in the message have to be valid for at least 30 days. These provisions have been found in the laws and regulations of Australia;[424] Hong Kong, China;[425] and New Zealand.[426]

Cross-Border Jurisdiction

Similar to consumer protection laws, an important consideration for SPAM laws is whether the regulation extends beyond the economy. In most cases, regulations only apply within an economy's territory. For instance, Article 2 of the Advertising Law of the People's Republic of China (2015) stipulates that its law only applies to commercial advertising activities within its territory[427]. However, others have indicated that the laws are applicable outside the economy so long as companies or individuals are based within its territory. One example is Article 14 of Australia's Spam Act 2003, which stipulates "Unless the contrary intention appears, this Act extends to acts, omissions, matters and things outside Australia."[428] Similarly, New Zealand's Unsolicited Electronic Messages Act 2007 indicates that this law extends extra-territorial application to individuals and companies based in the economy.[429]

[421] Canada, 'S.C. 2010', c. 23., Article 6(2) https://laws-lois.justice.gc.ca/eng/acts/E-1.6/page-1.html#h-176975.
[422] China, 'Advertising Law of the People's Republic of China (2015)', Article 8. https://www.hfgip.com/sites/default/files/law/advertising_law_16.02.2016.pdf.
[423] The Philippines, 'House Bill No. 3629', 2016, Section 6. http://www.congress.gov.ph/legisdocs/basic_17/HB03629.pdf
[424] Australia, 'Spam Act 2003', Article 17. https://www.legislation.gov.au/Details/C2016C00614.
[425] Hong Kong, China, 'Cap. 593 Unsolicited Electronic Messages Ordinance', Article 8. https://www.elegislation.gov.hk/hk/cap593.
[426] New Zealand, 'Unsolicited Electronic Messages Act 2007', Article 10. http://www.legislation.govt.nz/act/public/2007/0007/latest/DLM405134.html.
[427] China, 'Advertising Law of the People's Republic of China (2015)', Article 2. https://www.hfgip.com/sites/default/files/law/advertising_law_16.02.2016.pdf.
[428] Australia, Spam Act 2003, Article 14. https://www.legislation.gov.au/Details/C2016C00614.
[429] New Zealand, 'Unsolicited Electronic Messages Act 2007', Article 8. http://www.legislation.govt.nz/act/public/2007/0007/latest/DLM405134.html.

DATA PROTECTION AND PRIVACY

Data protection and privacy are particularly important issues in the context of e-commerce given how various information can be shared between platforms and service providers. Examples of information that are often shared range from an individual's age to more sensitive information such as home address or even payment details. Considering the volume and type of information shared today, there is a need for firms to be legally obliged to better protect such information so that they are not misused and therefore, increase the individuals' confidence to participate in e-commerce.

In response to this growing need, APEC economies with the exception of Papua New Guinea, have introduced laws relating to data privacy and protection. While some have stand-alone data privacy laws, others have nested data privacy regulations within regulations on cybersecurity. Apart from Brunei Darussalam whose data policy refers specifically to government agencies, many have included laws whose scope cover both the public and private sector. Despite the different structures of these laws, there are several similar aspects. These include definitions on personal information and the use of privacy principles.

Personal Information

A key part of data protection regulation usually indicates the types of information to be protected. This is often determined by how personal information is defined in the laws and regulations. In terms of the type of information categorized as 'personal information', some economies have focused strictly on identifiable information while others have included non-identifiable information. As an illustration, Canada defines personal information as "information about an identifiable person."[430] Similarly, Japan defines it as "information about a living person that identifies that (sic) person by name, date of birth, or other description, including information that will allow easy reference to other information and will thereby enable the identification of the person."[431] On the other hand, economies like Chile[432] and Mexico[433] consider both identifiable and non-identifiable individuals explicitly. Beyond the definition of personal information, some economies have also defined what identifiable means. For instance, economies such as the Philippines have denoted that identifiable information refers to those that directly provide information on an individual, as well as those that can be assembled with other information to identify an individual.[434]

---

[430] Canada, 'Personal Information Protection and Electronic Documents Act', S.C. 2000, c. 5. https://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html.

[431] Japan, 'Act on the Protection of Personal Information Act No. 57 of 2003', Article 2 https://www.jetro.go.jp/ext_images/usa/APPI.pdf.

[432] Chile, Personal Data Protection, Article 2. https://www.leychile.cl/Navegar?idNorma=141599.

[433] Mexico, 'Federal Law on Protection of Personal Data', Article 3. https://www.duanemorris.com/site/static/Mexico_Federal_Protection_Law_Personal_Data.pdf.

[434] The Philippines, 'Republic Act No. 10173', Section 2. https://www.officialgazette.gov.ph/downloads/2012/08aug/20120815-RA-10173-BSA.pdf.

Another aspect in which some economies have differed in their interpretation of personal information is in terms of its storage format. Some economies have indicated that the material form of the information does not matter. For instance, Australia notes that personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not."[435] Similarly, the Philippines' Republic Act No. 10173 indicates that personal information refers to any type of information which allows the identity of an individual to be directly or indirectly inferred regardless of whether it is in material form or not.[436] Hong Kong, China is more specific in its law, which stipulates that "personal data means any data…in a form in which access to or processing of the data is practicable."[437]

Some regulations have identified certain personal information which are deemed more sensitive, hence requiring more protection. Several APEC economies have created this category within their personal data protection regulations. For example, Article 9 of Mexico's Federal law on protection of personal data held by private parties indicates that the data controller is expected to obtain express written consent for the processing of such data. In addition, it prohibits the creation of databases that makes use of these sensitive personal information if they are not justified, legitimate, concrete or consistent with the objectives initially agreed to.[438] Similarly, Article 10 of Chile's personal data protection law indicates that sensitive information is prohibited from being processed unless the law allows for it, consent has been provided by the owner, or it is necessary for the health of the owners.[439] Japan's Act on the Protection of Personal Information (Act No.57 of 2003) had not initially included provisions for sensitive information, but this is now included with the amendments made in 2017[440].

What is considered to be sensitive information may differ between economies. In general, economies have opted to list down information that should be regarded as sensitive information. As an example, Malaysia's Personal Data Protection Act 2010, defines it to be "any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence or any other personal data as the

[435] Australia, 'Privacy Act 1988', Article 6, last amended 2013. https://www.legislation.gov.au/Details/C2014C00076.

[436] The Philippines, 'Republic Act No. 10173', Section 2. https://www.officialgazette.gov.ph/downloads/2012/08aug/20120815-RA-10173-BSA.pdf.

[437] Hong Kong, China, 'Cap. 486 Personal Data (Privacy) Ordinance', Article 2. https://www.elegislation.gov.hk/hk/cap486?tab=m.

[438] Mexico, 'Federal Law on Protection of Personal Data', Article 9. https://www.duanemorris.com/site/static/Mexico_Federal_Protection_Law_Personal_Data.pdf.

[439] Chile, 'Protecccion De Datos De Caracter Personal', Article 10. https://www.leychile.cl/Navegar?idNorma=141599.

[440] Japan, 'Act on the Protection of Personal Information (APPI) (Act No. 57 of 2003)', Last amended 2017, https://www.ppc.go.jp/files/pdf/280222_outline_v2.pdf.

Minister may determine by order published in the Gazette."[441] Apart from stating the types of information that are considered sensitive, China also includes within its definition, any form of information that can cause harm (e.g. reputational, physical, and mental) to an individual.[442]

Data Protection Authorities

Many APEC economies have data protection authorities, although their number and hence scope of responsibility vary. For instance, some economies have a centralized authority that are responsible for all things data related while others share the responsibility with several different agencies. For the former, Peru's Directorate for the Protection of Personal Data is one such example.[443] The same can be said for the Personal Information Protection Commission in Japan, which was established through the amended Act on the Protection of Personal Information in 2017.[444] For the latter, while the Cyberspace Administration of China (CAC) generally serves as the primary data protection authority, there are other data protection regulators as well including sector specific ones (e.g. China Banking and Insurance Regulatory Commission).[445] In the same vein, Viet Nam does not have a dedicated authority for personal data protection. Instead, it has several authorities involved with data protection which includes the Ministry of Information and Communication, the Ministry of Public Security and the Viet Nam Cybersecurity Emergency Response Teams.[446]

Privacy Principles

Privacy laws in several APEC economies usually identify a set of principles that anyone handling personal data have to adhere to. For example, Australia has an entire schedule to explain and detail these principles, which include: 1) open and transparent management of personal information; 2) anonymity and pseudonymity; 3) collection of solicited personal information; 4) dealing with unsolicited personal information; 5) notification of the collection of personal information; 6) use or disclosure of personal information; 7) direct marketing; 8) cross-border disclosure of personal information; 9) adoption, use or disclosure of government related identifiers; 10) quality of personal information; 11) security of personal information; 12) access to personal information; and 13) correction of personal information. It operationalizes these principles through associated Articles in the same law. As an illustration, it promotes 'open and transparent management of personal information' through Article 1.3 of

---

441 Malaysia, 'Personal Data Protection Act 2010', Article 4. http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20709%2014%206%202016.pdf.

442 China, China Personal Information Security Specification, 2018.

443 Peru, 'Decreto Supremo Nº 003-2013-JUS, Article 115'. https://hiperderecho.org/wp-content/uploads/2019/04/Reglamento_Ley_PDP.pdf.

444 Japan, 'Act on the Protection of Personal Information (APPI) (Act No. 57 of 2003)', Last amended 2017, https://www.ppc.go.jp/files/pdf/280222_outline_v2.pdf.

445 DLA Piper, 'National Data Protection Authority', Last accessed 18 June 2020. https://www.dlapiperdataprotection.com/index.html?t=authority&c=CN&c2=.

446 DLA Piper, 'National Data Protection Authority', Last accessed 18 June 2020. https://www.dlapiperdataprotection.com/index.html?t=authority&c=VN.

Schedule 1, which stipulates that "An APP entity must have a clearly expressed and up-to-date policy (the APP privacy policy) about the management of personal information by the entity'.[447]

Korea has also listed principles for protecting personal information in Article 3 of its Personal Information Protection Act. Some examples include: 1) the personal information controller shall specify and explicit the purposes for which personal information is processed; and shall collect personal information lawfully and fairly to the minimum extent necessary for such purposes; 2) the personal information controller shall make public its privacy policy and other matters related to personal information processing; and shall guarantee the data subject rights, such as the right to access their personal information; and 3) the personal information controller shall process personal information in a manner to minimize the possibility to infringe on the privacy of a data subject.[448]

Data Breach Notification

Data breaches can potentially bring significant harm to individuals as the nature of the transaction itself requires large amounts of personal information to be transferred and kept digitally. In response, several economies have enacted breach notification requirements, which necessitates data controllers to inform individuals and/or authorities when a security breach has occurred. One example of breach notification obligations is found in Article 10 of Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), which stipulates that an organization will have to both report to the Commissioner as well as provide notification to the individual whose information has been breached if there is real risk of significant harm to the individual.[449] China's Personal Information Security Specification provides detailed information on the requirements for personal information controllers both pre- (Article 9.1a) and post-incident (Article 9.1c). Some measures to be taken post-incident include assessing possible impacts and reporting in a timely manner amongst others[450]. In the case of Korea, its regulations mandate the following information to be made available to the affected individuals: 1) type of personal information breached; 2) when and how personal information have been breached; 3) information on how the data subjects can minimize the risk of damage from the breach; 4) countermeasures and remedial measures undertaken by the personal information controller; and 5) help desk and contact points for the data subjects to report damage.[451]

[447] Australia, Privacy Act 1988, Last amended 2013, Schedule 1. https://www.legislation.gov.au/Details/C2014C00076.

[448] Korea, Personal Information Protection Act, Last amended 2016, Article 3 (5). http://www.pipc.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000500301&fileSn=2.

[449] Canada, Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, Article 10. https://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html.

[450] China, China Personal Information Security Specification, 2018.

[451] Korea, 'Personal Information Protection Act', Last amended March 2016, Article 34. http://www.pipc.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000500301&fileSn=2.

Appointment of Data Protection Officers

As the management of information becomes increasingly important, economies are seeing the need to appoint individuals focused on ensuring that information are collected, processed and used in accordance to regulations in place. Brunei Darussalam is one example; all government agencies responsible for data are to appoint a designated Information Security Officer, who will be tasked with carrying out both scheduled and unscheduled compliance checks to ensure the agency adheres to the policy.[452] Article 30 of Mexico's Federal Law on Protection of Personal Data held by Private Parties indicated that data controllers must both designate a personal data person or department as well as promote the protection of personal information within their organization.[453] While some economies mandate the need for data protection officers across firms, others have only mandated it for specific type of firms. For instance, Thailand requires data controller and data processor to designate a data protection officer only if the organization is a public authority, if the organization has personal information which require regular monitoring, and/or if collecting, use or disclosure of personal information is the core business of the firm.[454]

Regulations are more diverse in economies with federal systems in place, as is the case of the United States. While there is no overarching regulation requiring the appointment of data officers, some states require the appointment of one or more employees to the role. For instance, New York City has required financial service companies to designate a Chief Information Officer to oversee and implement the entity's cybersecurity policy.[455]

4.4 FOCUS AREA D: CYBERSECURITY/ NETWORK SECURITY

As mentioned in Section 3.4, a number of WTO submissions noted the need to strengthen capabilities to prevent and respond to cybersecurity incidents[456] and some economies have suggested the adoption of risk-based frameworks.[457] The increased interest to tackle cybersecurity issues is also motivated by rising levels of cybercrime (see Box 4.10 for examples of common cyber threats),[458] which highlights the necessity of ensuring the security of data, transactions and networks. Those aspects are key for both consumers and companies alike and to some extent have been included in the work areas of APEC Internet Digital Economy

[452] Brunei Darussalam, 'Data Protection Policy', Section 16, Last accessed June 23, 2020, http://www.information.gov.bn/PublishingImages/SitePages/New%20Media%20and%20IT%20Unit/Data%20Protection%20Policy%20V.2.2.pdf.

[453] Mexico, 'Federal Law on Protection of Personal Data', Article 30, Last accessed June 23, 2020, https://www.duanemorris.com/site/static/Mexico_Federal_Protection_Law_Personal_Data.pdf.

[454] Thailand, 'Personal Data Protection Act', 2019, Section 41, Last accessed June 23, 2020, https://www.etda.or.th/app/webroot/content_files/13/files/The%20Personal%20Data%20Protection%20Act.pdf.

[455] The United States (New York City), 'Cybersecurity requirements for financial services companies', Section 500.04, Last accessed June 23, 2020, https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf.

[456] INF/ECOM/6, INF/ECOM/14, INF/ECOM/17, INF/ECOM/19, INF/ECOM/27/Rev.1

[457] INF/ECOM/5

[458] INF/ECOM/14

Roadmap (Enhancing trust and security in the use of ICTs)[459] and the APEC Framework for Securing the Digital Economy of 2019.[460] In light of this, this section provides a broad overview of the state of cybersecurity laws, as well as cybercrime legislation, among APEC economies.

Box 4.10: Most common cyber threats in brief

E-commerce can be particularly affected by cyber threats which target businesses and users, and hence undermine trust in online transactions. For instance, a recent survey by PwC revealed that 47 percent of interviewed companies experience a fraud recently and that the average number of frauds per company is six. Some recurrent examples of cyber threats are:

Internet fraud
Phishing: using a fake e-mail to send and require users to click on a URL. Once the user clicks, he/she is directed to a fraudulent log-in page to enter personal information, putting them at risk of identity theft.

Illegal access to IT systems
Hacking: accessing a computer device or a computer system without the user's knowledge and authorization.

Malware (or malicious software): using malicious software to infiltrate a computing device or system without the user's knowledge. It can then execute specific destructive tasks, putting at risk information system and data. Malware includes various computer viruses such as worms, trojan horses, spyware, adware and other types of intrusive software.

System interference
Distributed Denial-of-Service (DoS): blocking access to computer system by legitimate users. They usually target businesses rather than consumers. It works by attacking computer system with more requests than it can handle, thus preventing users to have access to the computer system.

Cyber extortion
Ransomware: using malicious software for extortion. It works by locking access to or threatening to publish a victim's data unless a ransom is paid.

[459] APEC, 'APEC Internet and Digital Economy Roadmap' (2017/CSOM/006, Singapore: APEC, 2017), Last accessed June 23, 2020, https://www.apec.org/-/media/Files/Groups/ECSG/17_csom_006.pdf. See also section 1.2 of this report.

[460] The APEC Framework for Securing the Digital Economy of 2019 provides non-binding principles and strategic recommendation to inform member economies as they develop policy and regulatory frameworks for securing their digital infrastructure, software, communications, and data. Those non-binding principles, which should be interpreted holistically, include awareness, responsibility, cooperation, and privacy. See: APEC; 'APEC Framework for Securing the Digital Economy', (APEC#219-TC-03.1, Singapore: APEC, 2019), https://www.apec.org/Publications/2019/11/APEC-Framework-for-Securing-the-Digital-Economy.

Sources:

- Adapted from: U.S. Department of Commerce - National Institute of Standards and Technology, *Glossary*, Last accessed June 23, 2020, https://www.nist.gov/
- Kaspersky Resource Center, What is cybersecurity?, Last accessed June 23, 2020, https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security
- PwC, PwC's Global Economic Crime and Fraud Survey 2020, Last updated 2020, Last accessed June 23, 2020, https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html
- ITU, Understanding Cybercrime: Phenomena, Challenges and Legal Response, Last updated 2012, Last accessed June 23, 2020, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

LAWS AND REGULATIONS ON CYBERCRIME AND CYBERSECURITY

Technically, cybercrime and cybersecurity are two different concepts. On the one hand, cybercrime refers to "a range of offences including traditional computer crimes, as well as network crimes".[461] The Budapest Convention on Cybercrime (see Box 4.11) offers examples of the types of offenses punished by cybercrime legislations,[462] however recent domestic laws may include additional ones.

Box 4.11: The Budapest Convention on Cybercrime

The Council of Europe Convention on Cybercrime or Budapest Convention is an international treaty seeking to harmonize and promote international cooperation on cybercrime. The convention covers mainly three issues:

(i) *Substantive computer crimes*, including illegal access (Article 2), illegal interception (Article 3), data interference (Article 4), system interference (Article 5), misuse of device (Article 6), computer-related forgery (Article 7), computer-related fraud (Article 8), offences related to child pornography (Article 9), and offences related to the infringement of copyright and related rights (Article 10);

(ii) *Procedural aspects for electronic evidence gathering*, including provisions on expedited preservation of stored computer data;

(iii) *International cooperation and mutual assi*stance, including extradition and mutual assistance.

To date, the Budapest Convention is the only international instrument to address the issue of cybercrime. Despite Japan and the United States not being members of the Council of Europe, both economies participated in the negotiation of the Convention as observers, and later ratified it. Other APEC members that have ratified the Convention include Canada; Chile; and Peru. Globally, it has been ratified by 64 economies. The Convention is also used

[461] ITU, Understanding Cybercrime: Phenomena, Challenges and Legal Response, 2014, p. 12, Last accessed June 23, 2020, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/cybercrime2014.pdf.

[462] Council of Europe, Convention on Cybercrime, ETS 185, Open for signature Budapest, 23 November 2001, Titles 1 and 2.

by other economies (that are not parties to it) as a source of inspiration for the adoption of domestic laws covering substantive and procedural matters of cybersecurity.

At the moment, a second additional protocol to the Budapest Convention is under negotiation. The protocol could facilitate the sharing of certain cross-border electronic evidence in criminal investigations in a much more efficient way by ensuring greater international cooperation.

Sources:

- Council of Europe, Convention on Cybercrime, ETS 185, Open for signature Budapest, 23 November 2001
- European Commission, Questions and Answers: Mandate for the Second Additional Protocol to the Budapest Convention, 2019, Last accessed June 23, 2020, https://ec.europa.eu/commission/presscorner/detail/en/MEMO_19_865

On the other hand, cybersecurity regulations, often found in independent statute, deal with a larger set of issues. According to ITU, cybersecurity is "the collection of policies and actions that are used to protect connected networks (including, computers, devices, hardware, stored information and information in transit) from unauthorized access, modification, theft, disruption, interruption or other threats."[463] This places emphasis in concepts such as data security and critical infrastructures, which go beyond the traditional scope of cybercrime legislations. Yet, both concepts reinforce each other and cybersecurity strategies often contain provisions on cybercrime.[464] In fact, ITU's Global Cybersecurity Index includes the existence of cybercrime legislations as one of the components of a cybersecurity legal framework.[465]

Analysis of the database reflects that all APEC economies have at least a cybercrime legislation (often found in criminal codes). Several also have a cybersecurity legal framework (composed of one or various laws and regulations). In other cases, privacy regulations may include additional requirements for data security (e.g., Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)[466]). Specific laws in some sectors holding sensitive data also contain an additional layer of duties for data security (e.g., the case of financial services[467]

[463] ITU, 'Overview of Cybersecurity', X.1205, 2008, p.6. Last accessed June 23, 2020, https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-X.1205-200804-I!!PDF-E&type=items.

[464] ITU, 'Understanding Cybercrime: Phenomena, Challenges and Legal Response', 2012, p. 2, Last accessed June 23, 2020, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf.

[465] ITU, 'Global Cybersecurity Index', 2018, Last accessed June 23, 2020, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

[466] Canada, 'Personal Information Protection and Electronic Documents Act (PIPEDA)', 'S.C. 2000, C.5', 2000, Clause 4.7 of Schedule 1, Last accessed June 23, 2020, https://www.parl.ca/DocumentViewer/en/36-2/bill/C-6/royal-assent/page-19#1.

[467] Under the Gramm-Leach-Bliley Act, the FTC is responsible for establishing standards for data security that will reduce the likelihood of data breaches and protect consumer privacy. See: United States, Gramm-Leach-Bliley Act, Public Law 106-102, 1999, Last accessed June 23, 2020, https://www.govinfo.gov/app/details/PLAW-106publ102.

and healthcare services [468] in the United States). These obligations could include the requirement to report data breaches, which is dealt with in Section 4.3 of this report.

Despite the variation between the laws and regulations, it can be argued that all APEC economies have implemented cybercrime or cybersecurity legislation at the domestic level. In some cases, the laws and regulations are relatively recent, especially among Asian economies. Table 4.5 illustrates the adoption of cybercrime and cybersecurity legislations among APEC economies.

Table 4.5: Cybercrime and Cybersecurity legislation in APEC Economies

Economy	Cybercrime Laws	Cybersecurity laws	Cybersecurity strategy
Australia	O		O
Brunei Darussalam	O		O
Canada	O		O
Chile	O		O
China	O	O	O
Hong Kong, China	O		
Indonesia	O	O	O
Japan	O		O
Korea	O	O	O
Malaysia	O		O
Mexico	O		O
New Zealand	O		O
Papua New Guinea	O		
Peru	O		O
The Philippines	O		O
Russia	O		O
Singapore	O	O	O
Chinese Taipei	O	O	O
Thailand	O	O	O
United States	O	O	O
Viet Nam	O	O	

Sources: APEC Electronic Commerce Steering Group, Regulations, Policies and Initiatives on E-Commerce and Digital Economy for APEC MSMEs' Participation in the Region, March 2020; ITU, Global Cybersecurity Index & Cyberwellness Profiles, 2015, http://www.combattingcybercrime.org/files/virtual-library/national-laws/global-cyber-security-index-and-cyberwellness-profiles.pdf; ITU, National Cybersecurity Strategies Repository, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx.

[468] The HIPAA breach notification rule requires covered entities and their business associates to provide notification following a breach of unsecured protected health information. See: United States, Health Insurance Portability and Accountability Act (HIPAA), 'Pub. L. 104-191', 1996, 45 CFR §§ 164.400-414, Last accessed June 23, 2020, https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf.

A broad overview of the content of some of these laws and regulations is provided within the following paragraphs:

CYBERCRIME LAWS

Different APEC economies have cybercrime legal frameworks embedded in their criminal laws. These usually penalize crimes committed using a computer, computer network or other form of ICT. For instance, Mexico's Federal Criminal Code prohibits conducts such as illegal access to computer systems, modification or destruction of information contained in computer systems and databases; misuse, interference or destruction of public telecommunications networks.[469] Other economies which regulate cybercrime within their criminal laws include Canada;[470] New Zealand;[471] Russia;[472] and Peru.[473]

In addition to this, some economies have laws and regulations that are specific to cybercrime and therefore, can complement the criminal acts. For instance, Peru's Law 30096 (Law on Cybercrime) [474] contains substantive criminal law largely in line with the Budapest Convention.[475] The same can be said for Australia's Cybercrime Act of 2001.[476] Other cybercrime laws include crimes beyond the scope of the Budapest Convention. This is the case of Papua New Guinea's Cybercrime Code Act, which dates back to 2016. According to the information reported by the economy, "the Act criminalizes offences relating to the integrity of data and electronic systems or devices, computer related offences, content related offences and other offences such as online copyright infringement, trademark infringement, patent and industrialize infringement, unlawful advertising and other offences."[477] There are some cybercrime laws, such as Chile's Law 19233, that are expected to undergo changes and typify new cybercrimes in order to comply with the Budapest Convention, to which Chile acceded in 2017.[478]

---

[469] Mexico, 'Federal Criminal Code', Article 211, Last accessed June 23, 2020, http://www.diputados.gob.mx/LeyesBiblio/pdf/9_140714.pdf

[470] Canada, 'Criminal Code', 1995; Section 4, Last accessed June 23, 2020, https://laws-lois.justice.gc.ca/eng/acts/c-46/

[471] New Zealand, 'Crimes Act of 1961', Last accessed June 23, 2020, http://www.legislation.govt.nz/act/public/1961/0043/latest/whole.html#DLM327382

[472] Russia, 'Criminal Code, 1996', Chapter 28, Last accessed June 23, 2020, https://www.legislationline.org/download/id/4247/file/RF_CC_1996_am03.2012_en.pdf

[473] Peru, 'Penal Code, Law 27309', Article 154-A, Last accessed June 23, 2020, http://spij.minjus.gob.pe/content/publicaciones_oficiales/img/CODIGOPENAL.pdf

[474] Peru, 'Law 30096 on Cybercrime (Delitos Informáticos)', Last updated 2013, Last accessed June 23, 2020, https://busquedas.elperuano.pe/normaslegales/ley-de-delitos-informaticos-ley-n-30096-1003117-1/

[475] Organization of American States, Inter-American Development Bank, 'Cybersecurity: Are we ready in Latin American and the Caribbean? 2016 Cybersecurity Report', 2016, p. 22, Last accessed June 23, 2020, http://www.combattingcybercrime.org/files/virtual-library/phenomena-challenges-cybercrime/cybersecurity-%e2%80%93are-we-ready-in-latin-america-and-the-caribbean.pdf

[476] Davidson, Alan, 'Social Media and Electronic Commerce Law', Cambridge University Press, 2018, p.352

[477] Survey on E-Commerce Regulations in APEC, p. 36.

[478] See: Ministerio de Hacienda, 'Proyecto de ley que deroga la ley 19233, establece normas sobre delitos informáticos y modifica otros cuerpos legales con el objeto de adecuar su regulación al convenio de Budapest', 2018, Last accessed June 23, 2020, http://www.dipres.gob.cl/597/articles-182132_doc_pdf.pdf.

CYBERSECURITY LAWS

Apart from cybercrime legislation, a number of economies have cybersecurity laws. The scope of some of those laws include the protection of Critical National Information Infrastructure.[479] For example, in the case of China, its Cybersecurity Law provides for "specific security obligations of products and service providers and network operators, personal information protection rules, and critical information infrastructure protection requirements."[480] Thailand's Cybersecurity Act[481] also lists a set of sectors considered as Critical Information Infrastructure Organizations. Similarly, Singapore's Cybersecurity Act 2018 also includes Critical Information infrastructure identified from 11 critical sectors, to which statutory obligations apply. In other cases, upcoming cybersecurity laws do not make any reference to Critical National Information Infrastructure.[482]

Some existing cybersecurity laws contain requirements for monitoring, preventing and handling cyber risks and threats. For example, Article 25 of China's Cybersecurity Law contains specific obligations for network operators. Preventive obligations include the formulation of an emergency response plans for cybersecurity incidents and promptly addressing system vulnerabilities, computer viruses, cyberattacks, network intrusions, and other cybersecurity risks. In the case of the occurrence of a cybersecurity incident, network operators should immediately initiate an emergency response plan, adopt corresponding remedial measures, and report to the relevant competent departments in accordance with relevant provisions.[483] Thailand's Cybersecurity Act contains provisions for government agencies to prepare codes of practice and standard frameworks for managing cybersecurity at a preventive stage as well as coping with ongoing cyber threats.[484] In the case of Chinese Taipei, the Cyber Security Management Act and Related Regulations contain measures that a government agency should follow in case of cybersecurity incidents. These include notification to competent authority upon one hour of its occurrence.[485] Finally, in some cases, cybersecurity laws target cyber risks that occur not only within the territory of an economy but also beyond its territory.[486]

[479] APEC, 'Structural Reform and Digital Infrastructure – Report Commissioned by the APEC Business Advisory Council', 2018, p. 28.
[480] Survey on E-Commerce Regulations in APEC, p. 9.
[481] Thailand, Cybersecurity Act, B.E. 2562, 2019.
[482] Peru, 'Proposed Law on Cybersecurity', 2018, Last accessed June 23, 2020, http://www.leyes.congreso.gob.pe/Documentos/2016_2021/Proyectos_de_Ley_y_de_Resoluciones_Legislativas/PL04352201905 17.pdf.
[483] People's Republic of China, 'Cybersecurity Law', 2017, Article 25, Last accessed June 23, 2020, http://www.csrc.gov.cn/pub/newsite/flb/flfg/flxzsf/201805/t20180518_338285.html.
[484] Thailand, 'Cybersecurity Act, B.E. 2562', 2019, Section 44.
[485] Chinese Taipei, 'Cyber Security Management Act & Related Regulations', 2019, Article 4, Last accessed June 23, 2020, https://nicst.ey.gov.tw/en/3FF2617AC997EFB7/dbcd2508-b1c7-4b42-8b42-43839243b882.
[486] People's Republic of China, 'Cybersecurity Law', 2017, Article 5, Last accessed June 23, 2020, http://www.csrc.gov.cn/pub/newsite/flb/flfg/flxzsf/201805/t20180518_338285.html.

Box 4.12: Contingency measures against attacks/ or preventive measures

In most cases, cybersecurity laws and strategies have measures or plans regarding cyberattacks (e.g., Chinese Taipei and the United States). Additionally, it is worth highlighting that every APEC economy has economy-level bodies that deal with cyber incidents (often referred as Computer Incident Response Teams – CIRT-). Furthermore, 13 economies (Australia; Brunei Darussalam; China; Hong Kong, China; Indonesia; Japan; Korea; Malaysia; New Zealand; Singapore; Chinese Taipei; Thailand and Viet Nam) are members of the Asia-Pacific Computer Emergency Response Team (APCERT).

In addition, APEC's Telecommunications and Information Working Group has developed the APEC Framework for Securing the Digital Economy in 2019, which provides non-binding principles and strategic recommendations to inform member economies as they develop policy and regulatory frameworks to secure their digital economies and their digital futures.

Sources:

- United States National Cyber Incident Response Plan (NCIRP), Last accessed June 23, 2020, https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan
- Chinese Taipei, Cyber Security Management Act & Related Regulations, Last accessed June 23, 2020, https://nicst.ey.gov.tw/en/3FF2617AC997EFB7/dbcd2508-b1c7-4b42-8b42-43839243b882
- ITU, National CIRT, Last accessed June 23, 2020, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx
- APCERT, Member Teams, Last accessed June 23, 2020, https://www.apcert.org/about/structure/members.html
- Telecommunications and Information Working Group, APEC Framework for Securing the Digital Economy, APEC#219-TC-03.1, 2019, Last accessed June 23, 2020, https://www.apec.org/Publications/2019/11/APEC-Framework-for-Securing-the-Digital-Economy

CYBERSECURITY STRATEGIES

A large majority of APEC economies have developed strategies to protect themselves against cyber threats. These economies are Australia;[487] Brunei Darussalam;[488] Canada;[489] Chile;[490]

[487] Australia, '2020 Cybersecurity Strategy', Last accessed June 23, 2020, https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/cyber-security-strategy-2020.

[488] Brunei Darussalam, 'E-Government Strategic Plan 2009-2014', Last accessed June 23, 2020, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Brunei.pdf.

[489] Canada, 'National Cyber Security Strategy', Last accessed June 23, 2020, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf.

[490] Chile, 'Política Nacional de Ciberseguridad', Last accessed June 23, 2020, https://www.ciberseguridad.gob.cl/media/2017/04/PNCS-ES.pdf.

China;[491] Indonesia;[492] Japan;[493] Korea;[494] Malaysia;[495] Mexico;[496] New Zealand;[497] Peru;[498] Philippines;[499] Russia;[500] Singapore;[501] Chinese Taipei;[502] Thailand;[503] and the United States.[504]

In contrast to cybercrime and cybersecurity laws which are granular in identifying, penalizing and setting legal procedures to combat illicit acts, the content of cybersecurity strategies is overarching. Some common themes include the setting of goals for a determined period of time, basic principles, the identification of key stakeholders including government ministries and agencies, the allocation of responsibilities (e.g., pertaining to incident management response). Among APEC economies, the aspects of focus vary, which are reflective of the maturity levels of cyber frameworks. For instance, in the case of the current Australia's Cybersecurity Strategy (which succeeds the former strategy of 2016), there are five themes of action: a national cyber partnership, strong cyber defenses, global responsibility and influence, growth and innovation and a cyber-smart economy.[505] In the case of Mexico, the National Cybersecurity Strategy has 5 strategic objectives: society and rights, economy and innovation, public institutions, public safety, and national security.[506] This cybersecurity strategy is also part of Industry 4.0 MX Platform.

4.5 FOCUS AREA E: INFRASTRUCTURE RELATED ASPECTS

[491] People's Republic of China, 'National Cyberspace Security Strategy', Last accessed June 23, 2020, http://politics.people.com.cn/n1/2016/1227/c1001-28980829.html.

[492] Indonesia, 'Cybersecurity Strategy', Last accessed June 23, 2020, https://bssn.go.id/strategi-keamanan-siber-nasional/.

[493] Japan, 'The Cybersecurity Policy for Critical Infrastructure Protection', Last accessed June 23, 2020, https://www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4.pdf.

[494] Korea, 'National Cybersecurity Masterplan', Last accessed June 23, 2020, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Korea_RepublicOf_2011_KOR_NCSS_2011.pdf.

[495] Malaysia, 'National Cybersecurity', Last accessed June 23, 2020, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Malaysia_2006_NCSP-Policy2.pdf.

[496] Mexico, 'Estrategia Nacional de Ciberseguridad', Last accessed June 23, 2020, https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf.

[497] New Zealand, 'Cybersecurity Strategy 2019', Last accessed June 23, 2020, https://dpmc.govt.nz/sites/default/files/2019-07/Cyber%20Security%20Strategy.pdf.

[498] Peru, 'Política Nacional de Cyberseguridad', Last accessed June 23, 2020, http://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/A36311FB344A1DC7052583160057706D/$FILE/Pol%C3%ADtica_Nacional_de_Ciberseguridad_peru.pdf.

[499] The Philippines, 'National Cybersecurity Plan 2022', Last accessed June 23, 2020, https://dict.gov.ph/national-cybersecurity-plan-2022/.

[500] Russia, 'Cybersecurity Strategy (2015)', Last accessed June 23, 2020, http://static.kremlin.ru/media/events/files/ru/l8iXkR8XLAtxeilX7JK3XXy6Y0AsHD5v.pdf.

[501] Singapore, 'Cybersecurity Strategy', Last accessed June 23, 2020, https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy/~/media/0ecd8f671af2447890ec046409a62bc7.ashx.

[502] Chinese Taipei, 'National Cyber Security Program (2017 to 2020)', Last amended 2017, Last accessed June 23, 2020, https://www.twncert.org.tw/policy_strategy.

[503] Thailand, 'National Cybersecurity Strategy 2017-2021', Last accessed June 23, 2020, http://www.nsc.go.th/.

[504] The United States, 'National Cyber Strategy of the United States of America', Last updated 2018, Last accessed June 23, 2020, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

[505] Australia, 'Cyber Security Strategy', Last accessed June 23, 2020, https://cybersecuritystrategy.homeaffairs.gov.au/.

[506] Survey on E-Commerce Regulations in APEC, p. 31.

The greater use of digital technology and in turn participation in e-commerce has been ongoing for some time. However, in light of the current pandemic, the reliance of many business sectors on telecommunications infrastructure has taken the spotlight. In fact, since economies began implementing measures to contain COVID-19, the demand for internet and mobile data services has increased, and the network capacity and spectrum has had to be adapted by both operators and governments.[507] According to analysts, some operators have opened public Wi-Fi hotspots in order to facilitate access to the internet for all their customers, and some of the main disruptions in the telecommunications ecosystem are faced by Over the Top (OTT) services, as video calls and forms of online entertainment went from being a niche segment to becoming mainstream.[508] In light of this, the need to bridge the digital divide has also become evident and many ICT-related government initiatives have prioritized the expansion of access to telecommunication services.[509] Given that telecommunications infrastructure plays the role of an enabler for e-commerce, this section describes the commitments of APEC economies with regards to telecommunications liberalization at the WTO level, with particular focus on the WTO Telecommunications Reference Paper.

INTERNATIONAL AGREEMENTS

GATS Commitments on Telecommunication Services

The rules governing telecommunication services in the context of the WTO are established in the General Agreement of Trade in Services (GATS), the GATS Annex on Telecommunications, applicable to public telecommunications transport network and services (See Box 4.13),[510] and the Telecommunications Reference Paper (for economies that scheduled the Reference Paper in their schedules of commitments).

Telecommunications commitments are mainly (but not exclusively) based on Services Sectoral Classification List (W/120 List).[511] The W/120 List contains, for almost all services sectors, correspondence with categories of the United Nations Provisional Central Product Classification (CPC).[512] In the W/120 List, telecommunication services are a sub-category of communication services. They include: voice telephone services (CPC 7521), packet-switched

[507] WTO, 'E-commerce, Trade and the Covid-19 Pandemic', 2020, p. 5, Last accessed June 23, 2020, https://www.wto.org/english/tratop_e/covid19_e/ecommerce_report_e.pdf.

[508] Sinibaldi, G, 'COVID-19 is revolutionizing digital communications and testing providers' reliability and ability to innovate (Analysis Mason, April 2020)', Last accessed June 23, 2020, https://www.analysysmason.com/Research/Content/Comments/covid19-ott-comms-rdmv0/.

[509] GSMA, 'How temporary access to spectrum can ease congestion during the COVID-19 crisis', Last updated April 2020, Last accessed June 23, 2020, https://www.gsma.com/gsmaeurope/news/how-temporary-access-to-spectrum-can-ease-congestion-during-the-covid-19-crisis/.

[510] WTO, 'GATS Annex on Telecommunications', Last accessed June 23, 2020, https://www.wto.org/english/tratop_e/serv_e/12-tel_e.htm.

[511] WTO, 'Services Classification Sectoral List', MTN/GNS/W/120, 10 July 1991.

[512] Tuthill, Lee, and Martin Roy, 'GATS Classification Issues for Information and Communication Technology Services.' In Trade Governance in the Digital Age: World Trade Forum, edited by Mira Burri and Thomas Cottier, p. 161 (Cambridge: Cambridge University Press, 2012).

data transmission services (CPC 7523), circuit-switched data transmission services (CPC 7523), telex services (CPC 7523), telegraph services (CPC 7522), facsimile services (CPC 7521 + CPC 7529), private leased circuit services (CPC 7522 + CPC 7523), electronic mail (CPC 7523), voice mail (CPC 7523), on-line information and data base retrieval (CPC 7523), electronic data interchange (CPC 7523), enhanced/value-added facsimile services, including store and forward, store and retrieve (CPC 7523), code and protocol conversion (n. a.), on-line information and/or data processing , including transaction processing (CPC 843), among other services.

One aspect to note is that some telecommunication services in the W/120 List are less relevant to the digital economy than others. This is the case of value-added facsimile services and telex and telegraph services. On the contrary, other services are difficult to classify and may overlap with computer and related services. For example, on-line information and data base retrieval (CPC 7523) is closely related to data processing services (CPC 843), a sub-sector found under the sector Business Services (see Box 4.13).

Box 4.13: Types of Telecommunication Services

The negotiation of Telecommunication Services at the WTO has followed mainly a dual classification system, namely: (i) basic telecommunications, and (ii) value-added telecommunication services.

Basic telecommunication services encompass "public telecommunications transport networks and services." The term "public" does not refer to the ownership structure, instead it refers to whether there is a universal service obligation (USO) attached to the telecommunication service at issue or a public service requirement. Basic telecommunication services "typically involve real-time transmission of customer supplied information between two or more points without any end-to-end change in its form or its context". Some examples include: voice telephone services, packet-switched data transmission services, circuit-switched data transmission services.

Telecommunication services not falling within this definition are generally referred to as "*value-added*". They require the infrastructure that basic telecommunication service offer. Examples include: electronic mail, online information and data base retrieval, electronic data interchange, online information and/or data processing.

While this dual classification is still relevant for the purpose of applying the Reference Paper, it faces challenges given the contemporary nature of digital business models, which consists of a bundle of services comprising of different telecommunications as well as other services. For instance, many e-commerce platforms run over basic telecommunication services but also rely in other value added services, such as email, online data processing, database storage and retrieval, among others, which at the same time allow a myriad of other services, for instance online payments. Hence, the necessity to reevaluate GATS commitments.

Sources:

- WTO, Services Classification Sectoral List, MTN/GNS/W/120, 10 July 1991 and Draft Model Schedule of Commitments on Basic Telecommunications, Informal note by the secretariat, JOB 1311/WTO/April 1995
- GATS Annex on Telecommunications, Last accessed June 23, 2020, https://www.wto.org/english/tratop_e/serv_e/12-tel_e.htm
- WTO, Telecommunication Services: Background Note by the Secretariat, S/C/W/299, 2009, Last accessed June 23, 2020, https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=98995,99355,81611,67501,60381,53378,47135,56028,51535,60690&CurrentCatalogueIdIndex=2&FullTextHash=&HasEnglishRecord=True&HasFrenchRecord=True&HasSpanishRecord=True
- Wolfrum, Rüdiger, Stoll, Peter-Tobias, and Feinäugle, Clemens, eds., 'WTO: Trade in Services', p. 692 (Leiden: BRILL, 2008)
- Tuthill, L. 'The GATS and New Rules for Regulators', Telecommunications Policy, 1997, 21(9/10): p. 792.
- The WTO Telecommunications Reference Paper applies only to basic telecommunications. WTO, 'Telecommunication Services: Background Note by the Secretariat, S/C/W/299', 10 June 1999, https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=98995,99355,81611,67501,60381,53378,47135,56028,51535,60690&CurrentCatalogueIdIndex=2&FullTextHash=&HasEnglishRecord=True&HasFrenchRecord=True&HasSpanishRecord=True
- WTO, 'Coverage of basic telecommunications and value-added services', https://www.wto.org/english/tratop_e/serv_e/telecom_e/telecom_coverage_e.htm

As previous PSU studies have shown, most APEC economies have adopted full market entry liberalization for telecommunication services. By 2009, all APEC economies had liberalized their mobile telecommunication sectors.[513] In addition, there are many more commitments made at the level of FTAs. However, there still exist a number of limitations. Based on the World Bank – WTO Applied Services Trade Policy database,[514] differences can be observed in many aspects, for instance in caps to foreign ownership for fixed-line and mobile telecommunication services (mode 3). Examples include Canada; China; and Indonesia;, where there are different caps for greenfield investments, while in other cases such as Australia; Japan; Mexico; and Peru, this aspect is fully liberalized. Limitations on foreign entry affect open and competitive telecommunications markets, which are strongly associated with higher broadband penetration rates and lower prices.[515] Restrictions for competitively priced telecommunications services can harm e-commerce as access may be out of reach for a significant share of the population. In light of this, WTO proposals[516] have stressed the need to have competitive telecommunication markets, which is a prerequisite to close the digital divide. One important instrument to achieve this is the adoption of the commitments contained in the WTO Telecommunications Reference Paper, which different APEC economies adhere to in different extents.

[513] Findlay, C. (ed), 'The Impacts and Benefits of Structural Reforms in the Transport, Energy and Telecommunications Sectors in APEC Economies, Report prepared for the APEC Policy Support Unit', p. xii (PSU, 2011), Last accessed June 23, 2020, https://www.apec.org/Publications/2011/01/The-Impacts-and-Benefits-of-Structural-Reforms-in-Transport-Energy-and-Telecommunications-Sectors.

[514] See: WTO, 'I-TIP Services', Last accessed 6 October 2020, https://i-tip.wto.org/services/default.aspx.

[515] OECD, 'STRI Sector Brief: Telecommunications', 2019, Last accessed June 23, 2020, http://www.oecd.org/trade/topics/services-trade/documents/oecd-stri-sector-note-telecommunications.pdf.

[516] INF/ECOM/5, EU INF/ECOM/13, EU INF/ECOM/43

WTO Telecommunications Reference Paper

The WTO Telecommunications Services Reference Paper addresses pro-competitive regulation in basic telecommunications services. Specifically, it addresses six regulatory aspects: 1) competitive safeguards against cross-subsidization, the withholding technical information about essential facilities, among others; 2) interconnection, which should be provided in non-discriminatory and transparent terms as well as at cost-oriented rates; 3) universal service; 4) public availability of licensing criteria, including terms and conditions and reasons for denial; 5) independence of the regulator, that should be separate, and not accountable to any supplier of basic telecommunications; and 6) allocation and use of scarce resources (such as frequencies and numbers) which should be carried out in an objective, timely, transparent and non-discriminatory manner. These principles apply for those WTO members that voluntarily adopted the Reference Paper and incorporated it in their GATS schedules. It should be noted that adoption of the Reference Paper is optional, as well as the way WTO members enunciate the commitments in their GATS schedules.[517] Additionally, the principles contained in the Reference Paper do not establish ready-made regulations, but economies are free to implement their specific legal and regulatory frameworks to comply with those regulatory principles.[518]

During the current e-commerce talks at the WTO, some economies have shown support in favor of all parties to the WTO e-commerce negotiations committing to fully implementing the Reference Paper. According to these economies, the principles contained in the Reference Paper works as a baseline and the precondition necessary to further foster competition in other telecommunication services. To date, based on the GATS schedules, the differences in the adoption of the Reference Paper by APEC economies are summarized in Table 4.6.

Table 4.6: Adoption of the WTO Telecommunication Reference Paper among APEC Economies

Economy	Reference Paper	Limitations on Reference paper	Additional Commitments to Reference Paper
Australia	O		
Brunei Darussalam	O		
Canada	O		
Chile	O		
China	O		
Hong Kong, China	O		
Indonesia	O		
Japan	O		
Korea	O		

[517] Tuthill, L. 'The GATS and New Rules for Regulators, Telecommunications Policy', 1997, 21(9/10): 783–98.
[518] Wolfrum, Rüdiger, Stoll, Peter-Tobias, and Feinäugle, Clemens, eds., 'WTO: Trade in Services', p. 721 (Leiden: BRILL, 2008).

Malaysia	O	O[519]	O[520]
Mexico	O		
New Zealand	O		
Papua New Guinea	O		
Peru	O		
The Philippines	O	O[521]	O[522]
Russia	O		
Singapore	O		
Chinese Taipei	O		
Thailand	O		
United States	O		
Viet Nam	O		

Source: WTO, Schedules of specific commitments and lists of Article II exemptions, https://www.wto.org/english/tratop_e/serv_e/serv_commitments_e.htm.

As observed, APEC economies have adopted the Reference Paper to various degrees. In majority of the cases, the Reference Paper has been annexed in its entirety. In other cases, further commitments have been adopted (Malaysia and the Philippines). These same economies have also adopted a modified and reduced version of the competitive safeguard provision in their GATS schedules.

LIBERALIZATION OF TELECOMMUNICATION SERVICES IN FTAS

Since WTO members committed to different levels of liberalization in telecommunication services in their GATS schedules (mostly during the 1990's), the telecommunication sector has evolved rapidly (with the increased importance of ensuring broadband penetration, managing convergence of value added services, among other). As some FTAs are relatively more recent compared to the GATS schedules, they may contain provisions that could better address the

[519] Modified and reduced language regarding competitive safeguards. See: Malaysia, Schedule of Specific Commitments - Supplement 2, GATS/SC/52/Suppl.2, https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S006.aspx?Query=(@Symbol=%20gats/sc/*)%20and%20((%20@Title=%20malaysia%20)%20or%20(@CountryConcerned=%20malaysia))&Language=ENGLISH&Context=FomerScriptedSearch&languageUIChanged=true#.

[520] Additional language regarding universal service, which add that network operators should contribute to the Universal Service obligation, particularly the extension of services into rural and other underserved areas as stipulated in the licenses. See: Malaysia, Schedule of Specific Commitments - Supplement 2, GATS/SC/52/Suppl.2, https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S006.aspx?Query=(@Symbol=%20gats/sc/*)%20and%20((%20@Title=%20malaysia%20)%20or%20(@CountryConcerned=%20malaysia))&Language=ENGLISH&Context=FomerScriptedSearch&languageUIChanged=true#.

[521] Modified and reduced language regarding competitive safeguards. See: The Philippines, Schedule of Specific Commitments - Supplement 2, GATS/SC/52/Suppl.2, https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S006.aspx?Query=(@Symbol=%20gats/sc/*)%20and%20((%20@Title=%20philippines%20)%20or%20(@CountryConcerned=%20philippines))&Language=ENGLISH&Context=FomerScriptedSearch&languageUIChanged=true#.

[522] Additional language regarding universal service, which requires authorized international gateway and mobile cellular telephone service providers are required to install a set number of local exchange lines in designated areas. See: The Philippines, Schedule of Specific Commitments - Supplement 2, GATS/SC/52/Suppl.2, https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S006.aspx?Query=(@Symbol=%20gats/sc/*)%20and%20((%20@Title=%20philippines%20)%20or%20(@CountryConcerned=%20philippines))&Language=ENGLISH&Context=FomerScriptedSearch&languageUIChanged=true#.

current telecommunications market. In fact, most FTAs signed in the past decade contain specific chapters dedicated to telecommunication services, containing provisions relevant for the current digital economy and e-commerce.

For instance, while the CPTPP telecommunications chapter contain different provisions that reflect the GATS Annex on Telecommunications and the principles contained in the Reference Paper, there are other provisions that expand and build on those previous commitments.[523] Some examples include Article 13.5.4 regarding the obligation of suppliers of public telecommunications services to ensure number portability, Article 13.6 regarding international mobile roaming, Article 13.9 regarding resale of public telecommunication services, Article 13.10 regarding unbundling of network elements by major suppliers,[524] Article 13.11 regarding interconnection with major suppliers, Article 13.12 on provisioning and pricing of leased circuit services by major suppliers, Article 13.13 on co-location by major suppliers, Article 13.14 regarding international submarine cable systems, Article 13.21 regarding the resolution of telecommunication disputes, among others. Just to illustrate the differences on the level of regulatory detail between CPTPP commitments vis-à-vis similar GATS provisions, one could take Article 13.12 of the CPTPP "regarding pricing of leased circuits by major suppliers", which should be offered to services suppliers of another party at "capacity based and cost oriented prices." This is a higher level pro-competitive regulation than the one found in Article 5 of the GATS Annex on Telecommunication Services (Access and Use of Public Telecommunications Transport Networks and Services), which does not contain a similar reference.

4.6 FOCUS AREA F: MARKET ACCESS

ACCESS TO IT-RELATED GOODS

Relating to telecommunications equipment, a pre-requisite to participating in e-commerce is having access to devices such as mobile phones and computers as well as their underlying parts and components. Restrictions on access to key technologies, parts and components can be detrimental to the development of the digital economy including e-commerce, particularly if the affected economies and businesses are unable to find alternative suppliers. One way to improve access to these products is through a tariff elimination agreement, as exemplified by the WTO Information Technology Agreement (ITA) (See **Error! Reference source not found.** f or more details). The original and expanded ITA, agreed during the WTO Ministerial Conference in Singapore (December 1996) and in Nairobi (December 2015) respectively, arguably effected one of the most meaningful trade liberalization processes by eliminating

[523] Another aspect worth highlighting is that CPTPP, unlike GATS, takes a negative list approach towards scheduling commitments, which means that all subsectors and modes of supply are liberalized, except those where an exception was made.
[524] Before the CPTPP, local loop unbundling has also been regulated in Article IV.2.b of Annex IVb of the Japan-Singapore PTA, https://www.enterprisesg.gov.sg/-/media/esg/files/non-financial-assistance/for-companies/free-trade-agreements/Japan-Singapore-EPA/Legal-text/Chapter-7/Annex-IVB-Telecommunications-Services; as well as Article 14.4.4 of the Chapter 14 if the Peru-United States FTA, https://ustr.gov/sites/default/files/uploads/agreements/fta/peru/asset_upload_file942_9515.pdf

customs duties for IT devices on a most favored nation (MFN) basis. It led to increased trade in products covered by the agreement, and hence improved access to them, many of which are critical to ensure growth of sectors such as e-commerce. Sixteen (16) APEC members are ITA participants, namely Australia; Canada; China; Hong Kong, China; Indonesia; Japan; Korea; New Zealand; Peru; the Philippines; Russia; Singapore; Chinese Taipei; Thailand; the United States; and Viet Nam.[525]

Box 4.14: WTO Information Technology Agreement

The WTO Information Technology Agreement (ITA) is arguably one of the most significant international agreements with positive implications on e-commerce. The original ITA was agreed and signed during the WTO Ministerial Conference in Singapore (1996). Unlike plurilateral agreements which restrict benefits to its signatories, the ITA is an open agreement extended to all members of the WTO, including non-signatories on the principle of most-favoured nation (MFN). It covered a wide range of products including computers, telecommunication equipment, semiconductors and most of the related parts and components. In addition to improving access as well as promoting innovation and development in various sectors, the fact that it covered parts and components of many end-products facilitated the participation of more developing economies in global supply chains.

Despite the benefits of the original ITA, the rapid technological change challenged the coverage of the original agreement as it became outdated relatively fast. For example, technological progress changed certain product characteristics, such as the case of set-top boxes with built-in recording capabilities or network access; PC flat-panel displays that carry standardised ports (i.e. DVI ports) and therefore, could be used as video monitors; and multi-functional printers that can also serve as copiers and fax machines. After several attempts at reviewing and expanding the original agreement, in 2015, almost all participants to the review agreed to eliminate tariffs on an additional list of 201 products, essentially including them within the expanded ITA. Among the products covered are new generation semi-conductors, optical lenses and GPS navigation equipment. Furthermore, the agreement has a commitment to overcome non-tariff barriers in the IT sector and to keep the list of products covered under review, in case further expansion to reflect future technological developments is needed.

Currently, 82 WTO members which collectively contributed about 97 percent of the global trade in IT products are parties to ITA. The Agreement requires each participant to eliminate and bind customs duties at zero for all products specified, and include them in the participants' WTO schedules of concessions. This implementation on MFN basis allows economies which are not parties to ITA to also benefit from the opportunities generated by the tariff elimination.

[525] WTO. 'Map of ITA Participants'. https://www.wto.org/english/tratop_e/inftec_e/ita_map_e.htm.

Sources:

- Lee-Makiyama, H, 'Future-Proofing World Trade in Technology: Turning the WTO IT Agreement (ITA) into the International Digital Economy Agreement (IDEA)' 2011, https://ecipe.org/wp-content/uploads/2014/12/WP201104.pdf
- WTO, 'International Technology Agreement', 2020, https://www.wto.org/english/tratop_e/inftec_e/inftec_e.htm

ENCRYPTION AND E-COMMERCE

As an increasing share of transactions are conducted online including via e-commerce, so too are crimes. Indeed, a study conducted by the Center for Strategic and International Studies (CSIS) and McAfee (2018) noted that close to USD600 billion is lost to cybercrime annually, up from about USD445 billion in 2014.[526] With more people and devices being connected to the Internet - Cisco (2018) estimated that the number of networked devices will increase by about 10.5 billion between 2017 and 2022, while the number of networked devices from 2.4 to 3.6 over the same period – more information will be available online.[527] One way to secure information from unauthorized access or use is through encryption, a process of changing information from plaintext (which can be read) into cipher text (which cannot be read).[528] Along with other cryptographic tools, encryption can enhance the use of authentication procedures and verify the validity of instructions.[529] In the context of e-commerce, strong encryption enables businesses and consumers to engage in secure transactions. The increased level of trust would also lead to more transactions, thus enabling e-commerce to grow further.

Recognizing its value, more economies have pointed to encryption as one of the mechanisms to secure information. For example, Article 24(3) of Korea's Personal Information Protection Act requires information managers to take necessary measures, including encryption, to prevent loss, theft, leakage, alteration or damage of personal information.[530] Several economies have put in place regulations such as those requiring the use of specific encryption standards, the licensing of encryption products and/or their exports, which are further elaborated in the sections below. Some of the regulations may have an inadvertent impact on market access.

[526] Lewis, J, 'Economic Impact of Cybercrime – No Slowing Down', Center for Strategic and International Studies (CSIS) and McAfee, 2018, https://www.mcafee.com/enterprise/enus/assets/reports/restricted/rp-economic-impactcybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70EMAIL_CAMPAIGN_2018_02_21&utm_medium=email.

[527] Cisco. 'Cisco Virtual Networking Index: Forecast and Trends', 2018, https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networkingindex-vni/white-paper-c11-741490.pdf.

[528] APEC PSU, 'Fostering an Enabling Policy and Regulatory Environment in APEC for Data-Utilizing Businesses', 2019, https://www.apec.org/Publications/2019/07/Fostering-an-Enabling-Policy-and-Regulatory-Environment-in-APEC-for-Data-Utilizing-Businesses.

[529] Digital Europe and The Information Technology Industry Council 'ICT Recommendations for Regulatory Cooperation in the Transatlantic Trade and Investment Partnership', 2015, https://www.bitkom.org/sites/default/files/file/import/ICT-Industry-position-on-TTIP-Regulatory-Cooperation.pdf.

[530] Korea, 'Personal Information Protection Act – Law No. 10465', 2011, latest amended in 2020, Article 23(4), https://www.privacy.go.kr/eng/laws_view.do?nttId=8186&imgNo=1.

Use of specific encryption standards

The Philippines' National Privacy Commission indicates that any approved technology used to store, transport or access sensitive personal information for purposes of off-site access have to be secured by recognized encryption standard and pointed to Advanced Encryption Standard with a key size of 256 bits (AES-256) as the most appropriate encryption standard.[531]

Article 22 of China's Cryptography Law, which will come into force in 2020, notes that the government would establish and improve a system of standards for commercial cryptography.[532] Article 24 of the Law further notes that commercial cryptography work units launching commercial cryptography activities shall comply with the technical requirements of relevant laws, administrative regulations, compulsory state standards on commercial cryptography, as well as the unit's public standards.

Licensing of encryption products

Analysis of relevant laws/regulations showed that one way for economies to ensure adherence of encryption and encryption-related products in their market to certain encryption standards is to require licensing/approval from relevant authorities. Economies may do so at different levels such as manufacturers, traders and users. At the level of manufacturers, for instance, China's State Council Order No. 273 on "Regulation of Commercial Encryption Codes" (State Council Order No. 273) requires manufacturers to seek approval from the National Commission on Encryption Code Regulations/State Cryptography Administration regarding the type and model of their encryption products to be sold in the economy.[533]

At the level of traders, Article 31 of Viet Nam's Law on Network Information Security obligates businesses that buy and sell civil encryption products to get a license from the Government Cipher Committee.[534] In assessing the license application, various criteria are used including business plans, product supply and staff skills. Article 12 of Russia's Federal Law No. 128-FZ On Licensing Specific Types of Activity indicated that a license is required to develop, manufacture, distribute and maintain encryption products as well as provide encryption services.[535] Article 26 of China's Cryptography Law states that commercial cryptography products that involve domestic security, domestic welfare and the people's livelihood, or the societal public interest, shall be lawfully entered into the catalogs of critical network equipment and specialized cybersecurity products, and must pass testing and certification by qualified bodies before being sold or provided. Moreover, testing and

[531] National Privacy Commission of the Philippines. https://www.privacy.gov.ph/implementing-privacy-and-data-protection-measures/data-security/#7.
[532] China, 'Cryptography Law of the People's Republic of China', 2019, https://www.chinalawtranslate.com/en/cryptography-law/.
[533] China, 'Regulation of Commercial Encryption Codes', 2000, http://www.asianlii.org/cn/legis/cen/laws/rocec383/.
[534] Viet Nam, 'Law on Network Information Security', 2015, https://english.mic.gov.vn/Upload/VanBan/Law-on-Network-Information-Security-16-05-30.pdf.
[535] Russia, 'Federal Law No. 128-FZ "On Licensing Specific Types of Activity"', http://pravo.gov.ru/proxy/ips/?docbody=&prevDoc=102072404&backlink=1&&nd=102147413.

certification of commercial cryptography products is to apply the relevant provisions in the Cybersecurity Law to avoid repetitive testing.

At the level of users, Article 36 of Viet Nam's Law on Network Information Security requires organizations and individuals that use civil encryption products sold by a non-licensed traders to declare them with the Government Cipher Committee. However, exceptions are provided to the diplomatic community including international organizations. China's State Council Order No. 273 indicates that only encryption products approved by the National Commission on Encryption Code Regulations can be used in the economy. If users want to use encryption products that are self-developed and/or manufactured overseas, approval from the Commission is needed. Similarly, exceptions apply to the diplomatic community.

Export of encryption products

Besides regulations affecting the use of encryption products in the domestic market, some economies also have export regulations that affect the sale/use of those products in foreign markets. For example, Canada's Export Control List, which is established under the Export and Import Permits Act and requires export permit to be sought for exports of items in the list, which includes certain cryptographic products.[536] However, exceptions apply if the products are marketed to the general public or to be exported to the United States. The United States' International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR) put export controls on some forms of encryption.[537] China's State Council Order No. 273 requires an export license to be sought from the National Commission on Encryption Code Regulations/State Cryptography Administration for encryption products. Viet Nam's Article 34 on the Law on Network Information Security also mentions about the need for a license if a company wants to export cryptographic products.

REGULATIONS BEYOND ENCRYPTION AND ENCRYPTION-RELATED PRODUCTS

Analysis of relevant laws/regulations also showed that several economies require electronic and/or IT products other than those related to encryption to be regulated in one way or another (e.g., licensing, pre-installed with specific software). For example, Article 32(1) of Indonesia's Law No. 36 of 1999 Regarding Telecommunications states that the telecommunications equipment traded, manufactured, assembled, imported and/or used within the economy shall comply with the technical requirements and be based on a license pursuant to prevailing statutory regulations.[538] Article 32(2) further states that provisions concerning the technical

[536] Canada, 'Export and Import Permits Act', 1985, https://laws-lois.justice.gc.ca/eng/acts/E-19/.

[537] The United States, 'International Traffic in Arms Regulations', https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=%2024d528fddbfc930044f9ff621f961987, and 'Export Administration Regulations', https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear.

[538] Indonesia, 'Law of the Republic of Indonesia No. 36 of 1999 Regarding Telecommunications', Last updated 1999, Last accessed June 23, 2020, https://www.postel.go.id/content/EN/regulasi/telecommunication/uu/law36-1999.pdf.

requirements of the telecommunications equipment referred to in paragraph (1) is subject to Government Regulation. Russia's Federal Law No.425-FZ On Introducing Amendments into Article 4 of the Law on Protection of Consumer Rights indicated that from 1 July 2020, certain types of electronic goods could only be sold in the economy if pre-installed with specific software. The list of specific products, the type of software affected and the installation procedure have yet to be determined.[539]

ACCESS TO PROPRIETARY INFORMATION

Many economies do not tie the condition of market access to the provision of proprietary information of products (e.g., source codes, algorithms). Indeed, some trade agreements explicitly require parties to eliminate such conditions. For example, Article 14.17 in the e-commerce chapter of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) requires the elimination of any government condition obliging firms to transfer or grant access to the source code as a pre-requisite for the import, distribution, sale or use of software or products containing such software. The provision is targeted at mass-market software.[540]

However, some economies condition market access with the provision of proprietary information. For example, albeit restricted to public agencies, Article 8(1) of Indonesia's Regulation No. 82 of 2012 Concerning Electronic System and Transaction Operation indicates that providers who develop software created specifically for an agency must submit the source code and documentation of the software to the agency concerned.[541] Where this cannot be implemented, Article 8(2) indicated that the source code and documentation of the software can be submitted to a trusted third party for storage, essentially creating an escrow arrangement.

It is worthwhile to mention that although some of the laws/regulations requiring licensing and software pre-installation discussed above do not explicitly require access to proprietary information, they also do not explicitly prohibit authorities from requesting for such access.

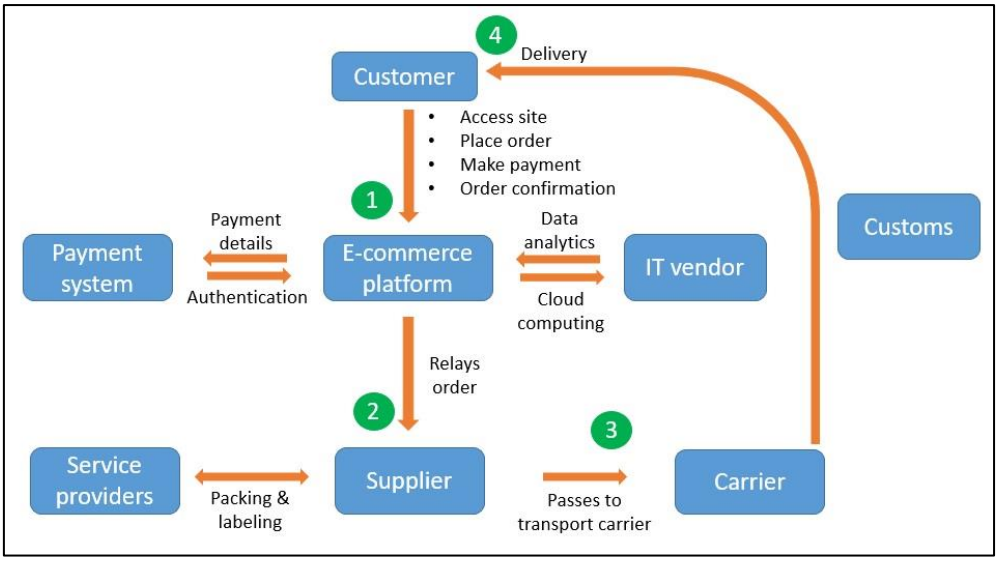
RESTRICTIONS ON ACCESS TO AND PROVISION OF SERVICES

Besides being an end product that can in essence be traded electronically (e.g., streaming services, telehealth services), services (in particular supporting and enabling services) can potentially contribute to smooth functioning of the e-commerce value chain (see Figure 4.1 for some examples). As an illustration, besides acting as intermediary between banks, merchants and customers, payment services widen the options available to merchants and customers.

[539] Baker McKenzie, 'Russia Mandates Pre-Installation of Russian Software on Electronic Devices', Last accessed June 23, 2020, https://globalcompliancenews.com/russia-mandates-pre-installation-of-russian-software-on-electronic-devices/.
[540] 'Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) Text', Last accessed June 23, 2020, https://www.enterprisesg.gov.sg/-/media/ESG/Files/Non-Financial-Assistance/For-Companies/Free-Trade-Agreements/CPTPP/Chapters/14ElectronicCommerce.pdf.
[541] Indonesia, 'Regulation No. 82 of 2012 Concerning Electronic System and Transaction Operation', Last updated 2012, Last accessed June 23, 2020, http://www.flevin.com/id/lgso/translations/JICA%20Mirror/english/4902_PP_82_2012_e.html.

Limited payment options may limit sellers' ability to sell if customers' preferred options are not available. Transport/logistics services are critical because a compelling appeal of e-commerce is indeed the convenience of having products delivered to the location of choice. Targeted advertising services, which in turn depends on data analytics, can potentially help raise shopping conversion rates (i.e., the percentage of website visitors who actually buy). Data analytics services can also be used to detect anomaly, combat fraud and provide enterprise solutions among others. Hence, e-commerce can benefit from wider market access for supporting and enabling services, as well as the end-to-end provision of digital products. While an extensive review of policies and regulations affecting services trade is beyond the scope of this study, the objective of this section is to show that there are variations in how economies regulate the trade of services sub-sectors such as transport/logistics, computer-related services, legal and accounting. The services covered are non-exhaustive. In addition, the section will not cover those services which have been discussed in earlier sections (e.g., financial services in Focus Area A, telecommunications services in Focus Area E).

Figure 4.1: Example of supporting/enabling services in the e-commerce value chain



Source: Adapted from Drew and Napier. 'E-commerce and Personal Data II – Navigating Cross-border Data Transfers'. Presentation on 24 November 2017.

Transport/logistics services

All APEC economies have made GATS schedules of commitments in the transport/logistics sector.[542] Some economies have also made additional commitments in their preferential trade agreements (PTAs).[543] Despite the progress, analysis of the OECD STRI database showed that the extent of liberalization at MFN level continues to vary between economies. In the maritime transport sector for example, analysis for APEC economies covered in the database showed that the score ranges between 0.18 and 0.56, with 0 being the least restrictive and 1 being the most restrictive. Breaking down the overall score into the different category of restrictions

[542] WTO, 'WTO iTIP Services', Last accessed June 23, 2020, https://i-tip.wto.org/services/.
[543] WTO, 'WTO iTIP Services', Last accessed June 23, 2020, https://i-tip.wto.org/services/.

showed that the main contributing restrictions are regulations affecting foreign entry, followed by those affecting movement of people. On those affecting foreign entry, for example, Indonesia restricts foreign ownership to no more than a share of 49 percent, although investors from ASEAN economies can hold ownership up to 70 percent in international maritime transport service providers. Thailand requires local presence for cross-border supply of maritime transport services. On those affecting movement of people, New Zealand requires labour market tests for intra-corporate transferees, contractual service suppliers and independent service suppliers.[544]

In the storage and warehouse subsector of logistics, analysis showed that the score ranges between 0.11 and 1. Breaking down the overall score into the different category of restrictions revealed that for some economies, the main contributing restrictions are regulatory transparency, while for others, they are regulations affecting foreign entry. On regulatory transparency, for example, while laws and regulation enters into force 10 days after the official publication in Russia, it was indicated in the database that they may differ in practice. In Chile, regulations enter into force the moment they are published in the official journal if a precise date is not specified.

Computer-related services

Eighteen (18) APEC economies have made commitments in their GATS schedules regarding computer-related services. Economies have also made additional commitments in their PTAs.[545] However, there continue to be variation in the extent of liberalization at MFN level, as shown by the analysis of the OECD STRI database. The OECD STRI score for APEC economies covered by the database range from 0.12 to 0.38. Depending on individual economies, the main contributing restrictions are either restrictions on foreign entry, restrictions to movement of people, other discriminatory measures or regulatory transparency. One example of a restriction on foreign entry is the limitation on proportion of foreign equity to 50 percent for a large extent of computer services in China, with online data processing services being an exception as it has been fully liberalized in June 2015. An example of restriction to movement of people is the limitation on duration of stay for contractual and independent services suppliers in Mexico. An example of other discriminatory measures is the less favorable treatment of foreign suppliers in terms of taxes in Canada.

Professional services

Certain professional services, such as legal services and accountancy, auditing and book-keeping services can be relevant for e-commerce businesses. Among others, legal services are required to provide legal advice on various matters pertaining to business operations and

[544] OECD, 'Services Trade Restrictiveness Index Simulator', Last accessed June 23, 2020, https://sim.oecd.org/.
[545] WTO, 'WTO iTIP Services', Last accessed June 23, 2020, https://i-tip.wto.org/services/.

disputes arising from e-commerce transactions. Accountancy and auditing services ensure that accounting rules have been adhered to for different reasons including taxation. Nineteen (19) APEC economies have indicated these two professional services in their GATS schedules of commitments. Similar to the above sectors, economies have also made additional commitments in their PTAs.[546] At the same time, however, analysis of the OECD STRI database showed variation in the extent of liberalization at MFN level between economies. Regarding legal services, the OECD STRI scores for APEC economies covered by the database range from 0.14 to 0.89, while in the accounting services, the scores range from 0.10 to 1.

For legal services, the main restrictions for most economies are either restrictions on foreign entry or restrictions on movement of people. For example, Japan's Attorney Act indicates that the member of a legal professional corporation shall be locally-licensed lawyers, and only locally-licensed lawyers can have equities. In Malaysia, citizenship or permanent residency is required to practice both domestic and international law. Similarly, for accounting services, the main restrictions for most economies are either restrictions on foreign entry or restrictions on movement of people. For example, Korea's Certified Public Accountant Act indicates that the maximum foreign equity share is under 50 percent, and that one foreign accountant can only have less than 10 percent of equity share. Related to this, only professionals are allowed to hold shares and Korea requires accountants who wants to be a certified public accountant (CPA) in the economy to pass the Korean CPA examination.

[546] WTO, 'WTO iTIP Services', Last accessed June 23, 2020, https://i-tip.wto.org/services/.

5 CASE STUDIES

This section comprises of a series of case studies covering different focus areas. Since each focus area comprises of various elements, each begins with an overview of the elements of the focus area which are covered in the case studies.

5.1 FOCUS AREA A: ELECTRONIC TRANSACTION FRAMEWORK

OVERVIEW

Supportive laws and regulations for e-commerce and electronic signatures

Electronic transactions frameworks covered in this report, including electronic authentication, electronic payment, electronic invoicing, as well as issues relating to trade facilitation, taxation and customs duties, are key to facilitating e-commerce. Noticing that current laws and regulations affecting these areas were adopted before e-commerce went mainstream, it is critical for them to recognize features of e-commerce which are now commonplace. For instance, e-contracts and e-signatures need to be recognized as legally binding in order to be used as evidence in the event of disagreement between parties to an e-commerce transaction. The absence of those basic rules may discourage electronic transactions to occur in the first place. Two case studies covering these areas are offered as examples of legal adaptation. The case study on China's E-Commerce Law provides insights on how China sets out to establish a framework for electronic transactions regarding legal rights and obligations of online businesses vis-à-vis their offline counterparts and the recognition of e-contracts. In the case of Chinese Taipei's Electronic Signatures Law, the case study showcases the value of giving legal recognition to electronic records and signatures, as well as the main challenges regarding their implementation.

E-payment

E-payments are one of the critical aspects which facilitate e-commerce. They can encompass a variety of methods, including wire transfers, electronic funds transfer (EFT) credits, credit cards, automated clearing house (ACH) credits, mobile banking, and prepaid cards.[547] While e-payment transactions have been increasing year-on-year, the current COVID-19 pandemic is likely to further accelerate growth as consumers shift more of their purchases online. To help encourage continued growth of e-commerce, it is important for e-payment methods to evolve to become faster, more convenient, and more secure. In recent years a number of economies have launched real-time bank to bank payment systems (RTP) to enable consumers to easily make instantaneous payments from their bank accounts to those of vendors. Essentially, RTP can make it easier for people who are unable to obtain credit cards and in some cases, the unbanked population to access e-commerce. The use of RTP also benefits merchants including

[547] Better Than Cash Alliance, 'How to define digital payments?', Last accessed 1 August 2020, https://www.betterthancash.org/tools-research/toolkits/payments-measurement/focusing-your-measurement/introduction.

MSMEs, as it allows them to avoid expensive credit card processing fees, and instantaneously receive customer payments. The case study on Australia's New Payments Platform (NPP) and Thailand's PromptPay are further elaborated below.

CASE STUDIES

China

China is the largest e-commerce market in the world. It is estimated that more than half of global online transactions occurred within the economy.[548] The 'Singles Day' shopping festival, which usually falls on 11 November annually, has continued to break records year after year. In 2019, it generated sales of RMB268 billion (USD38 billion) in just 24 hours, which was 25 percent higher than that in 2018.[549,550] Despite the economic impact of the pandemic, the e-marketer forecasted that China will become the largest overall retail market in the world for the first time in 2020.[551] Specifically on retail e-commerce, it was estimated that the Chinese consumers would spend a total of RMB14 trillion (USD2.1 trillion) this year. Although this figure is lower than the forecast made prior to the pandemic, it still is higher than the spending in 2019.

E-commerce and supporting factors

China recognizes the critical role of various factors such as strong infrastructure as well as supportive laws, regulations and initiatives in promoting e-commerce. As such, the economy has continued to enhance efforts in these areas. In the area of infrastructure, for example, data from the International Telecommunication Union (ITU) showed that more than 54 percent of China's population have access to the internet in 2018, while mobile cellular subscriptions stood at 115.53 per 100 people in the same year.

China's 13th Five-year Development Plan for E-commerce (2016-2020) identifies several projects which would have implications on e-commerce both directly and indirectly. Examples include: 1) the National Broadband Agenda which aims to establish a high-speed, high-capacity optical telecommunications system and extend connectivity to rural villages and improve basic network infrastructure in small and medium cities in the central and western region; 2) the development of comprehensive experimental zones for cross-border e-commerce; 3) the establishment of a unified open platform for big data; and 4) the development of infrastructure and service platforms to facilitate adoption of the Internet of Things. As part of its response to

[548] Cornell, 'The impact of e-commerce: China versus the United States', Last updated 18 February 2020, https://business.cornell.edu/hub/2020/02/18/impact-e-commerce-china-united-states/.
[549] China Daily, 'Double 11 record sales signal strength of Chinese consumption', Last updated 12 November 2019, https://www.chinadaily.com.cn/a/201911/12/WS5dca40a8a310cf3e35576d7f.html.
[550] CNBC, 'Alibaba breaks Singles Day record with more than $38 billion in sales ', Last updated 11 November 2019, https://www.cnbc.com/2019/11/11/alibaba-singles-day-2019-record-sales-on-biggest-shopping-day.html.
[551] eMarketer, 'China Ecommerce 2020', Last updated 10 June 2020, https://www.emarketer.com/content/china-ecommerce-2020.

tackling the COVID-19 pandemic, the government has coordinated with Alibaba to introduce a number of emergency support services directly targeting MSMEs, which include B2C e-commerce solutions.[552] Considering the rapid growth of e-commerce, it is also critical for China to regulate e-commerce conducts. This case study addresses specifically this point, focusing on China's E-Commerce Law.[553]

E-Commerce Law[554]

A. Pre-reform situation

There were several impetus which called for the development of China's E-Commerce Law. From the perspective of businesses, the absence of a law which specifically caters to online businesses made it challenging to understand their legal rights and obligations vis-à-vis their offline counterparts. Furthermore, it was indicated that the lack of clarity in the existing laws/regulations at that time could potentially led to the adoption of ad-hoc discriminatory policies or measures, with consequent negative implications on online businesses. In some cases where existing laws/regulations could provide clarity, the relevant articles were scattered across different laws/regulations, hence making it difficult for businesses to determine if they had adhered to them in entirety. From the perspective of consumers, the absence of a law which determines the dos and don'ts in the online marketplace meant that they might be subjected to questionable practices by businesses. For the more risk-averse participants, such uncertainty might lead to them deciding not to participate in the online market. Put simply, considering the rapid growth of e-commerce both domestically and internationally, China needed a law, which among others, would set the framework for electronic transactions and hence provide legal certainty to different participants.

B. Process and challenges of enacting the law

The process of enacting China's E-Commerce Law began back in 2013 and was spearheaded by the National People's Congress Standing Committee (NPCSC), which delegated it to its Economic and Finance Committee. While the process of enacting a law is usually led by a specific ministry, the cross-cutting nature of the E-Commerce Law necessitates that its development be taken at the higher level. Indeed, the development of the law involves 13 ministries in total and supported by expert groups as well as public consultations. Towards the end of 2016, the Economic and Finance Committee submitted the first draft of the law to the NPCSC for review. Three more reviews were conducted between 2017 and 2018, followed by

[552] Alibaba Business School, 'Digital Action for Entrepreneurs in the age of COVID-19', Last accessed 15 October 2020, https://files.alicdn.com/tpsservice/4851ee417ad1a379aa93e23ab5d73048.pdf; Tech Circle, 'Alibaba offers cloud services worth $30 mn to MSMEs', Last updated 23 April 2020, https://www.techcircle.in/2020/04/23/alibaba-cloud-offers-cloud-services-worth-30-bn-to-msmes.

[553] China, 'E-commerce Law of the People's Republic of China', Last updated 31 August 2018, https://www.izvoznookno.si/Dokumenti/E-commerce%20Law%20of%20the%20People%E2%80%99s%20Republic%20of%20China.pdf.

[554] Information in this section are mostly obtained from an interview conducted on 12 August 2020 with Prof. Xue Hong, Senior Expert from Legislation Consultation Group, Beijing Normal University.

public consultations. Additionally, two events were held to involve the international community in the development of the law; the first was participated by UNCITRAL and UNESCAP, while the second was participated by representatives from 20 economies.

Fulfilling the primary objective

As with the process of enacting laws in general, getting the E-Commerce Law from inception to its promulgation in 2018 and eventual entry into force in 2019 was not an easy journey. For one, policymakers had to ensure that the law fulfills the primary objective that it is meant to address, some of which have been discussed in the earlier section. In this regard, Article 4 of the E-Commerce Law made clear that the economy would treat both online and offline business activities on an equal footing and promote the integrated development of online and offline businesses. Furthermore, it is mentioned that governments and authorities at all levels shall not adopt discriminatory policies/measures or abuse administrative power to eliminate/restrict market competition.

- **Obligations of online platforms and businesses**

Specifically on obligations of online businesses, Article 5 indicates that e-commerce business operators should adhere to several principles in their conduct, including fairness and honesty. Section 1 of the Law, which comprises of Articles 9 to 26 provides more detailed information which e-commerce business operators have to abide by. They range from the need to disclose information concerning the goods or services in a truthful, accurate and timely manner, to deliver goods or services to consumers in the manner and time provided in their commitments or as agreed upon with consumers.

Noting that many online businesses sell goods and services through platforms instead of stand-alone websites, Section 2 of the Law includes Articles which are intended to empower e-commerce platform operators with legal rights and obligations with regards to online businesses registered with their platforms. For example, Article 27 indicated that platform operators shall request online businesses applying to sell via the platforms to submit information pertaining to her/his identity, address, contact information and administrative license among others. In a way, empowering platform operators co-opts them into helping to regulate the online businesses and to ensure that they do so, there are Articles in the Law which assign joint liability to platform operators and online businesses registered with them. As an illustration, Article 38 indicated that where platform operators know or should know that goods or services sold or provided by online businesses registered with them do not comply with certain requirements and yet, do not take necessary measures, they shall be jointly liable with the concerned online businesses. The Law also includes Articles to ensure that platform operators do not abuse their legal rights and obligations over online businesses registered with them. For instance, Article 32 requires platform operators to formulate platform services agreements and trading rules clearly.

- **Contract formation**

Since contract formation would likely be conducted electronically in the context of e-commerce, it is critical to give clarity to this specific element of the electronic transactions framework. In this regard, Chapter III of the Law focuses on the formation and performance of e-commerce contracts. Examples relevant to contract formation includes: 1) Article 47 which indicates that the provisions of existing laws such as the Contract Law and Electronic Signatures Law would apply to e-commerce contracts as well; and 2) Article 49 which specify clearly that a contract would be deemed to have been formed where information of goods or services published by online businesses meets the requirements of an offer, and when buyers select these goods or services and successfully submit their orders. An example relevant to contract performance would be Article 51 which indicates that where a contract is for delivery of goods and it is made by courier service, the time of delivery shall be the time when the recipient signs for receipt.

- **E-payment**

E-payment is yet another element of the electronic transactions framework that the E-Commerce Law aims to give clarity on, as elaborated by Articles 53 to 57. For example, Article 53 mentioned that parties to e-commerce contracts can agree on payment through electronic means and in providing e-payment services, providers shall comply with relevant regulations which cover issues such as risks and fees. Providers also need to ensure that payment orders are complete, coherent, traceable, verifiable and unalterable. Articles 54 and 55 assign liabilities to different parties under various events such as errors in payment order.

Balancing the interests of different stakeholders

Another aspect which policymakers have had to consider in the process of developing the law is to balance the interests of different stakeholders. Many articles in the law are indeed reflective of this balancing act. For instance, noting the usefulness of data analytics to online businesses in enhancing consumers' online shopping experience and at the same of time, the need to respect consumers' preference, Article 18 mentioned that although online businesses can provide a consumer with search results of goods or services based on her/his hobby, consumption habit or other traits, it shall also provide consumer with the option not to target her or his personal traits. Recognizing that platform operators can offer similar goods and services as online businesses registered with them and yet, the need to ensure that platform operators do not exploit this to the detriment of other online businesses (i.e., platform/vendor competition), Article 37 indicated that platform operators who do so shall label their own online businesses clearly to ensure that consumers are not misled. Specifically on e-payment, noting that unauthorized payment can be caused by different parties, Article 57 mentioned that while payment service providers shall usually be liable for such losses, they do not bear liabilities if they can prove that the unauthorized payment is caused by user's fault. On the contrary, if a user notifies payment service provider that a particular payment order is not authorized and yet,

the payment service provider does not promptly take measures, hence causing more losses, they shall bear liabilities for the additional losses.

Overcoming conflict of laws

The development of laws also need to take into account the potential for overlap between different laws and clarify which law would take precedent in such instances. Where different laws regulate different aspects of the same subject matter, this should be made clear as well. For the E-Commerce Law, Article 2 indicated that where any other law or administrative regulation provides rules for the sale of goods or provision of services, such other law or administrative regulation shall apply (meaning that they are *lex specialis*). It also indicated that the law shall not apply to financial products and services, as well as news information, audio and video programs, publications, cultural products, and other content services provided via information networks. In practice and using some examples as an illustration, while financial products and services would be covered by e-payments law instead, aspects pertaining to its use in e-commerce are covered by the E-Commerce Law, as elaborated earlier. Likewise, while the content aspect of news information is subject to other relevant laws, the commerce aspect is covered by the E-Commerce Law.

Last but not least, despite the possibility to amend existing laws, it is important to ensure that laws can stand the test of time. This is particularly so for laws such as the E-Commerce Law where the underlying ecosystem it regulates evolves rapidly along with technological progress. In this regard, the Law attempts to introduce a relatively new approach to regulation (i.e., self-regulation) in China, as exemplified in Article 8, which indicated that e-commerce industry associations shall in accordance with their own bylaws conduct industry self-discipline, as well as establish and improve industry standards among others.

C. Post-reform situation

The entry into force of the E-Commerce Law in January 2019 is a significant milestone in China's quest to regulate e-commerce conducts. The law has tried to address legal gaps, replace old norms, as well as consolidate and clarify legal rights and obligations of participants in the e-commerce ecosystem. While it is challenging to directly attribute the exponential growth of e-commerce in the economy since January 2019 to the E-Commerce Law, it is also not accurate to say that the law has had no impact on e-commerce. China continues to break records across various indicators (e.g., total spending in Singles' Day).

The introduction of newer approach to regulation in the law has led to some elements being incorporated into other laws. For example, the notice and take down aspect of the law (Articles 42 and 43) has been adopted in the Civil Code.

Despite the progress made, there remain issues to be improved upon. For example, while Article 2 mentioned that that the law shall apply to all e-commerce activities in China,

enforcement of the law on foreign-based platform operators which sell to Chinese consumers would be challenging as they are not physically present in the economy.

D. Way forward

Although it has been in force for almost two years now, the E-Commerce Law is relatively a young law. While it has led to better regulation of e-commerce conducts, implementation and operationalization of certain aspects of the law may not always be smooth sailing. Indeed, in some cases, it is only through implementation and operationalization that policymakers are able to identify room for improvements. In this regard, China continues to monitor the impact of the law and plans to introduce supporting regulations to clarify aspects of the law where relevant.

China indicated that as a regional forum, APEC can be an information hub where economies share experience with one another. APEC also stands in good stead to provide capacity building activities on various aspects of e-commerce.

Conclusion

E-commerce provides an additional channel for businesses and consumers alike to sell and access goods and services. However, it needs to be regulated to enhance the trust of different participants and hence promote its adoption. China's E-Commerce Law provides an illustration of an economy's efforts to achieve this. To ensure that the law fulfills its primary objective, it covers many relevant aspects such as those pertaining to the rights and obligations of online platforms and businesses as well as contract formation. Noting that the interests of different stakeholders may vary, the law has articles which aim to balance these interests (e.g., between businesses vis-à-vis consumers, platform vis-à-vis vendor). Recognizing that there could be potential overlap between laws, it clarifies which law would take precedent in such instances.

Chinese Taipei

Chinese Taipei is among the more mature e-commerce markets globally. In a poll conducted by Market Intelligence & Consulting Institute, 4.5 out of 10 purchases made in Chinese Taipei were online.[555] The U.S. Department of Commerce put the e-commerce market size in Chinese Taipei at USD42.7 billion in 2017 and noted that growth rate over the last five years hovered between 10 and 20 percent.[556] It further added that the economy had the highest proportion of e-commerce shoppers in Asia (67 percent) that are sophisticated and are familiar with global trends. In fact, the highest average revenue per e-commerce user (about USD3,000) in 2018. A wide range of items are purchased online by consumers in Chinese Taipei. Examples include media products, apparel and footwear, consumer electronics, and basic household necessities.

[555] Societe-Generale, 'Taiwan: The Market', Last accessed 5 October 2020, https://import-export.societegenerale.fr/en/country/taiwan/ecommerce.
[556] Export.gov, 'Taiwan E-commerce', August 2019, https://www.export.gov/apex/article2?id=Taiwan-ecommerce.

E-commerce has seen further growth under the ongoing global COVID-19 pandemic. Despite Chinese Taipei's strong response to contain the pandemic, the global economic downturn has nevertheless impacted commercial activities negatively in the economy. Retail sales in stores have seen a slight decline (3 percent) in the first quarter, of which the clothing industry, the food industry, and restaurants have suffered the most (7-12 percent decline). On the other hand, e-commerce retail sales have grown by nearly 20 percent in the same period as the public avoided public spaces for fear of contracting the virus. The food delivery service in particular saw a whopping growth of nearly 40 percent. This trend is expected to continue as commercial 5G networks became available in July 2020, with penetration projected to be 10 percent in the first year. New technologies which are facilitative of e-commerce such as Virtual Reality, Augmented Reality, Internet of Things, and Internet of Vehicles are likely to be further enhanced by the 5G networks.

E-commerce and supporting factors

In light of the ongoing shift towards the digital economy globally, these trends are unsurprising and seem to accurately reflect the current state of affairs. However, it is important to note that the digitalization of an economy is not a predetermined path. Maximizing the benefits while overcoming the challenges of digitalization require economies to undertake conscious choice.

In the context of Chinese Taipei, numerous factors have contributed to its current level of e-commerce growth. One factor is its strong infrastructure which has been reflected in a large internet user base. Data from the International Telecommunication Union (ITU) indicated that more than 86 percent of Chinese Taipei's population in 2018 have access to the internet.[557] According to Akamai, its average connection speed of 16.9 Mbps as of 1Q 2017 is among the top 5 in the Asia-Pacific region.[558]

Supportive laws, regulations and initiatives also play a critical role in promoting e-commerce growth. For example, Chinese Taipei had unveiled the Digital Nation & Innovative Economic Development Program 2017 – 2025 (DIGI+), a 9-year program to promote the development of broadband infrastructure and supporting regulations so as to establish a sound digital ecosystem. [559] In 2018, the Financial Technology Development and Innovative Experimentation Act was enacted to create a safe environment for fintech experimentation.[560] Its Consumer Protection Act extends to transactions conducted electronically.[561] In addition, the law details the type of information that must be provided clearly and conspicuously (e.g. the name of the traders, the contents, the period and procedure for consumer to exercise the

[557] ITU, 'Statistics', Last accessed 2020, https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[558] Akamai, 'akamai's [state of the internet]', 2017, https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q1-2017-state-of-the-internet-connectivity-report.pdf.
[559] Digital Innovation & Governance Initiative Committee, 'Introduction', Last updated 22 January 2018, https://digi.ey.gov.tw/en/5329AD162CD5F88A.
[560]Chinese Taipei, 'Financial Technology Development and Innovative Experimentation Act', Last updated 31 January 2018, https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=G0380254.
[561] Chinese Taipei, 'Consumer Protection Act', Last amended 2015, https://cpc.ey.gov.tw/File/99162D02EC293DE0?A=C.

right). To help businesses diversify and improve their presence in e-commerce in light of the COVID-19 pandemic, the Ministry of Economic Affairs has provided subsidies to small and medium-sized enterprises (SMEs) for launching online stores. As of July 2020, the Ministry of Economic Affairs has helped 25 businesses to launch online stores. The fact that e-commerce transactions are conducted electronically also necessitates the development of robust electronic transactions framework which among others, should provide legal recognition to electronic records and signatures. This case study addresses specifically this point, focusing on Chinese Taipei's Electronic Signatures Law.[562]

Electronic Signatures Law[563]

A. Pre-reform situation

The idea to formulate Chinese Taipei's Electronic Signatures Law was first brought up in 1999 by both the private and public sector. From the perspective of the private sector, the lack of a legal framework to recognize electronic records and signatures was becoming an impediment for electronic transactions, which at the time were gaining traction. This was because if disagreements were to arise between the parties to a transaction, the courts would have to resolve the dispute by referring to the provisions found in the Civil Code.[564] However, at that time, the Civil Code provided no formal indication that electronic records could be accepted as evidence. From the perspective of the public sector, the rise of online services and digitization of records required a legal norm allowing them to accept the electronic version of various documents as evidence and correspondingly, of having a supportive law.

B. Process and challenges of enacting the law

Recognizing this, the government set about the process of introducing a law whose primary objective was to provide legal recognition to electronic records and electronic signatures. In developing the draft law, Chinese Taipei used as reference laws/regulations existing in other economies such as Australia's Electronic Transactions Act 1999[565] and the United States' Electronic Signatures in Global and National Commerce Act (ESIGN)[566]. It also referred to model laws released by international organizations such as UNCITRAL Model Law on Electronic Commerce (1996)[567]. At the same time, Chinese Taipei noted the need to ensure that

[562] Chinese Taipei, 'Electronic Signatures Act', Last updated 14 November 2001, https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=J0080037.

[563] Information in this section and the next section on 'way forward' are mostly obtained from an interview conducted on 16 July 2020 with officials from Chinese Taipei's Bureau of Foreign Trade, Institute for Information Industry and Ministry of Economic Affairs.

[564] Chinese Taipei, 'Civil Code', Last amended 19 June 2019, https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=B0000001.

[565] Australia, 'Electronic Transactions Act 1999', Last amended 2011, https://www.legislation.gov.au/Details/C2011C00445

[566] The United States, 'Electronic Signatures in Global and National Commerce Act', 2000, https://www.govinfo.gov/content/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf.

[567] UNCITRAL, 'Model law on Electronic Commerce with Guide to Enactment 1996', https://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf.

the draft law be adapted to the local conditions and indicated that the inclusion of regulations affecting certification service providers in the law as an example where it has done so.

The process of enacting the law was not an easy endeavor. As the concept of electronic records was relatively new then, many stakeholders including public servants did not understand the underlying technology and how electronic records could be treated as equivalent to paper records. One primary concern referred to is the risk that electronic records could be relatively easy to manipulate (vis-à-vis paper records) and if so, their value as evidence could be put into question. There were also concerns beyond ensuring the authenticity of electronic records. For example, in situations where the recipients require certain electronic records to be received within a particular time, the act of sending these records before the stipulated time may not necessarily meant that the recipients did in fact received them before the stipulated time due to time lag and possibility of server issues among others. In another example, where the recipients require certain electronic records to be sent to a particular email address, the act of sending these records could not be assumed as a confirmation that the recipients received the electronic records, particularly if they were sent to a different email address other than the one indicated. As such, it was important to address all these scenarios and have a law sufficient to address the authenticity of electronic records and signatures (Articles 4 to 6, 9 and 10) and mechanisms to resolve potential disputes arising from their use (Articles 7 and 8).

Furthermore, while the law could indicate certain requirements to overcome these issues, it would also need to ensure that these requirements balance the interest of different stakeholders and do not put certain groups at a disadvantage. For example, noting the relatively higher cost of using digital signature, the law has opted to recognize two tiers of signatures which can be used for verification purposes, namely electronic and digital signature. Technically, electronic signature is any data attached to and associated with the electronic record, which can be used to identify/verify the identity or qualification of the signatory and hence the authenticity of the record, so long as all parties agree to its use. While digital signature is defined as an electronic signature generated by the use of mathematic algorithm (or other means) to create a certain length of digital data encrypted by the signatory's private key, and capable of being verified by the public key.[568] Such tiering enables smaller businesses and the general population to enter into most transactions electronically at minimal cost and without worry that these electronic records could not be used as evidence should there be disputes. Exceptions include transactions with parties in the financial sector (e.g., banks) where digital signature as a means of authenticating electronic records is a requirement, not an option.

Another example of balancing different stakeholder interests can be observed in how the law acknowledges that despite setting the legal framework to recognize electronic records, they may not be suitable in all instances, or even if suitable, particular technology or procedure may

[568] Chinese Taipei, 'Electronic Signatures Act', Article 2, Last updated 14 November 2001, https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=J0080037.

be required to complement it, as observed in some Articles (e.g., Article 4).[569] At the same time, the law requires that the stipulation or prescription of the specific technology or procedure be fair, reasonable and should not provide preferential treatment without proper justifications. Practical examples of how to operationalize this include:

- Government agencies are required to issue guidelines to indicate the kinds of activities where electronic records and signatures are (or are not) accepted. Where electronic records and signatures need to be complemented with additional steps, these have to be indicated in the guidelines as well.
- Similarly, the private sector is required to clarify instances where electronic records and signatures can (or cannot be) used, and if they need to be complemented with additional steps. For instance, while electronic records and signatures can be used to purchase an insurance plan, insurance firms would require the individual to undertake additional steps through physical interaction with insurance agents to complete the process. The same can be said for most financial services, such as opening of bank account.

As a digital signature is a relatively more secure instrument than electronic signature, it has to be generated by the use of a mathematic algorithm (or other means) and encrypted. Chinese Taipei requires the use of digital signature to be accompanied by a certificate that link the signature-verification data to a person so as to confirm his/her identity and attribute (Article 10). These certificates are issued by certification service providers, which are obligated to file a certification practice statement (CPS) that has to be published for public reference upon approval (Article 11). This ensures the transparency of operational processes of such providers especially with regards to their certification services.

Additionally, the law indicates that the certification service providers shall be liable for any damage caused by its operation or other certification-related process (Article 14). At the same time, to balance the interests of the service providers, the law allows them to prove that they have not acted negligently and to specify clearly the limitation in the use of certificates, beyond which they shall not be held liable. Two domestic service providers are currently operating in Chinese Taipei.

Noting that certificates can be issued by service provider established or regulated by foreign law, Chinese Taipei indicates that such certificates can be treated as equivalent to the one issued by a domestic service provider under the principles of reciprocity and equivalent requirements (Article 15).

[569] Chinese Taipei, 'Electronic Signatures Act', Article 4, Last updated 14 November 2001, https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=J0080037. It states that "….By stipulation of a law or regulation or prescription of a government agency, the application of the two preceding paragraphs may be exempted, or otherwise require that particular technology or procedure be followed. In the event that particular technology or procedure is required, the stipulation or prescription shall be fair and reasonable, and shall not provide preferential treatment without proper justifications."

As have been alluded above, Chinese Taipei engaged various stakeholders during the entire process of enacting the law by conducting public hearings to solicit feedback. Indeed, according to Article 2 of the Notes of Central Administrative Agencies legislative procedures, in the process of drafting legislations, the administrative agency should consult the opinion of experts and scholars, or held public hearings when necessary.[570] Specifically for the Electronic Signatures Law, when the draft was completed in July 1998, the Ministry of Economic Affairs held many public hearings, reported and explained the purpose of the Act, as well as seek the oral opinions of stakeholders, interest groups, and other interested parties.

C. Post-reform situation

The enactment (and entry into force) of the Electronic Signatures Law in November 2001 has given legal recognition to electronic records and signatures. Consequently, this has led to increased confidence among parties to conduct transactions electronically. While the role of other laws and regulations in promoting the growth of e-commerce should not be downplayed, the Electronic Signatures Law has certainly contributed to its growth as well.

Fundamentally, it has also led to wider acceptance of electronic records as a legal document and hence its use for a broad range of activities, for instance evidence. During the interviews with Chinese Taipei government officials, it was indicated that fewer government agencies still require paper records now. This is in contrast to the situation when the law had just been introduced - at that time, many agencies released guidelines listing activities where paper records were required, such as in the areas of real estate law, family law, succession law, and notary law. Many guidelines requiring paper records have since been abolished.

Despite these improvements, there remain issues to be resolved. One example is that while the law has given legal recognition of electronic records and signatures, there is still uncertainty as regards what constitutes a valid electronic record, particularly those that are not authenticated using digital signatures. The absence of clear guidance in the law means that often, the court has to decide on whether a specific electronic record is valid or not. The fact that other specific aspects can be better clarified (e.g., the time of dispatch and receipt of electronic records) also means that they are still open to interpretation.

Last but not least, although the law provides for recognition of a certificate issued by a foreign service provider, no foreign-issued certificate has been recognized so far.

D. Way forward

Moving forward, Chinese Taipei noted that the Electronic Signatures Law can be improved. One area would be to provide clarity on what can be deemed as valid electronic records and by extension, valid electronic signatures (in cases where the method of authentication is not a

[570] Chinese Taipei, 'Notes of Central Administrative Agencies', https://www.ey.gov.tw/File/32E887FC93867403?A=C (in Chinese).

digital signature). Another aspect would be to require the use of technology and procedures which do away with the need for interpretation (e.g., incorporation of time stamp in electronic records when they are dispatched and received). Through its public policy network participation platform (join.gov.tw), Chinese Taipei is also open to public feedback on how existing laws/regulations can be further enhanced.

On the role of APEC, Chinese Taipei indicated that the regional forum provides a good avenue for experience sharing among economies. Specifically on the Electronic Signatures Law, Chinese Taipei stands ready to share its practical experience with other member economies considering that the law has been in place for close to two decades. APEC is also in a good position to encourage discussions on cross-border issues, specifically on reciprocity.

Conclusion

Facilitating e-commerce requires an economy to have supportive electronic transactions framework. Chinese Taipei's Electronic Signatures Law aims to provide legal recognition to electronic records and electronic signatures, as well as mechanisms to resolve potential disputes arising from their use. Key insights from the case study include: 1) the benefits of referencing existing laws/regulations, while at the same time ensuring that the law be adapted to the local conditions; 2) the value of involving multiple stakeholders and balancing their interests in the development process of the law; as well as 3) the importance of having mechanisms to monitor how the law can be further improved over time.

Australia

Australia is one of the most mature e-payments markets in APEC, but is fragmented between multiple domestic bank transfer systems with overlapping purposes. The total value of cross-border e-commerce purchases made by Australian consumers is high and steadily increasing. The experience of Australia with the launch of its RTP system in the last few years and its focus on developing overlay services for the system to support additional features is informative for developed economies seeking to modernize e-payment systems.

Cross-border E-commerce growth trends

Australia has one of the strongest e-commerce sectors in APEC due to a high per-capita GDP and widespread internet technology penetration. In a population of 24 million, just under 20 million have internet access, and just under 15 million users are online shoppers.[571] Additionally, 63 percent of those shoppers are willing to purchase from overseas firms. This cross-border market has grown by 16 percent annually since 2013.[572] This trend can be

[571] 'SingPost eCommerce, eCommerce in Australia: 10 Key Insights', 2015, Last Accessed 1 August 2020, http://www.specommerce.com.s3.amazonaws.com/dl/fs/150416_fs_australia.pdf.
[572] The Paypers, 'Mobile commerce and online shopper behaviour in Australia', Last accessed 1 August 2020, https://thepaypers.com/ecommerce-facts-and-figures/australia/15.

partially attributed to the Australian Border Force's allowance that cross-border purchases under AUD1,000 (USD 700) are exempt from duties.[573]

In total, the Australian e-commerce market is forecast to approach AUD 35.2 billion (USD 25 billion) by 2021.[574] Cross-border e-commerce is expected to account for about 20 percent of that total, which would be equivalent to AUD 6.9 billion (USD 5 billion).[575]

The importance of access to mobile devices cannot be overstated. 68 percent of Australians own a smartphone, which is of particular importance considering the fact that USD 6 billion or more than a quarter of online sales are completed on mobile devices and the share is rising.[576]

Box 5.1: Real-time payment systems

Real-time Payments (RTP) address inefficiencies of current banking processes by providing low- or no-cost funds transfer with immediate funds availability, settlement finality, instant confirmation, and integrated information flows. Once uncommon, RTP have rapidly spread around the world over the last decade, and as of 2019 more than 50 economies had some form of domestic RTP system in operation, albeit at various levels of maturity.

Growth in RTP payments has been especially robust in the Asia Pacific region, which accounts for two-thirds of global RTP spending. This surge has been led by efforts in economies such as China, India, and Thailand to integrate RTP systems with quick response (QR) codes and reading apps to initiate payments. This ability enables physical and online retailers, including small and medium enterprises (SMEs) to realize the convenience of cashless payments. In e-commerce this is especially helpful for SMEs conducting business through social media, which represents a very large portion of e-commerce sales in economies such as Thailand.

Consumers also benefit from the various open Application Programming Interfaces (API) overlay services that economies and/or the private sector are building on top of RTP platforms to incorporate additional convenience features. Consumers can use simple proxy IDs when sending or requesting payments so that they do not need to enter long and complex account numbers to pay, or to log into online banking apps to make payments. Australia's New Payments Platform (NPP) for example allows the use of aliases, and plans to provide open API-based transactional services.

[573] Australian Border Force, 'Buying online', 17 March 2020, Last accessed 1 August 2020, https://www.abf.gov.au/buying-online/buying-online.

[574] WebAlive, 'The State of Australia's Ecommerce in 2019', 24 June 2019, Last accessed 1 August 2020, https://www.webalive.com.au/ecommerce-statistics-australia/.

[575] Wisconsin Economic Development Corporation, 'Opportunities in Australia's e-commerce sector', June 2018, Last accessed 1 August 2020, https://wedc.org/export/market-intelligence/posts/opportunities-in-australias-ecommerce-sector/.

[576] J.P. Morgan, 'E-commerce Payments Trends: Australia', 2019, Last accessed 1 August 2020, https://www.jpmorgan.com/europe/merchant-services/insights/reports/australia.

Sources:

- J.P. Morgan, 'The Real Value of Real-Time Payments', 2017, Last accessed 1 August 2020, https://www.jpmorgan.com/global/cib/treasury-services/real-value-real-time-payments
- FIS, 'Flavors of Fast Report 2019', 2019, Last accessed 1 August 2020, https://empower1.fisglobal.com/rs/650-KGE-239/images/Report_Flavors_of_Fast_2019.pdf

Australian customers are increasingly willing to buy from online retailers in other economies. There are many advantages: polls have shown that consumers appreciate the higher quality, variety of products, availability, and prices that foreign sites provide. In particular, Australians appreciate the discounts on fashion and related sectors. On the other hand, there are challenges which may be slowing the growth ofcross-border commerce such as the need for foreign currency exchange, difficulty of returns, and lack of trust for foreign sites and customer service.[577]

E-payments motivation and adoption status

In Australia, card payments and bank transfers have displaced checks and cash as the dominant forms of payment over the last two decades. Check and cash payments decreased from 70 percent to under 40 percent of transactions from 2007 to 2016.[578] Direct payments between bank accounts have gained momentum through the innovations of internet banking and mobile banking apps, now used by over 54 percent and 46 percent of the population, respectively.[579]

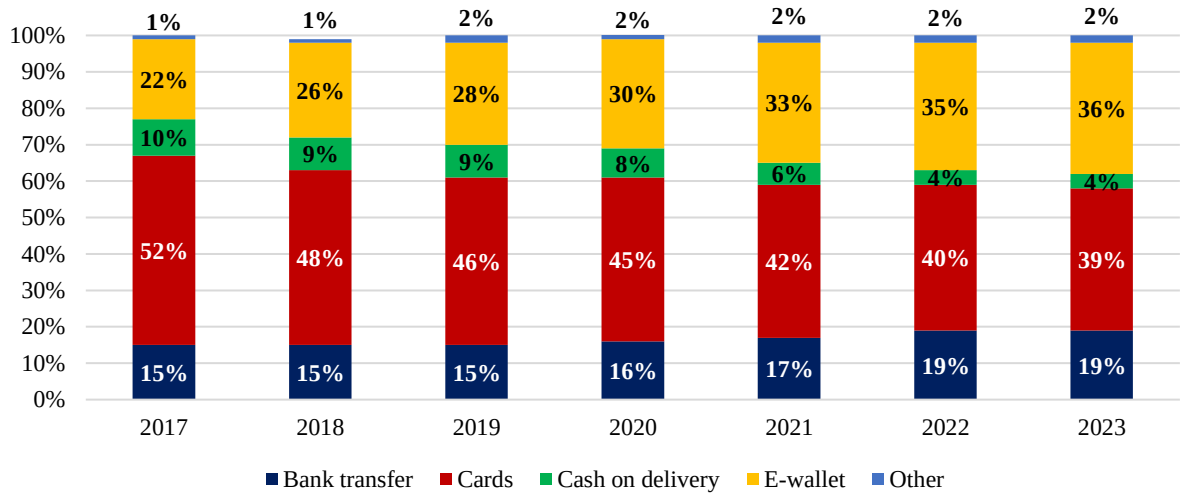
Concerning preferred payment types for e-commerce, credit and debit cards continued to dominate in 2019, representing a combined 46 percent of the total value of e-commerce sales. However, as Figure 5.1 below shows, the share of cards is forecast to gradually decline to 39 percent by 2023, while bank transfers (notably RTP payments) increase from 15 percent to 19 percent, and e-wallet transactions increase from 28 percent to 36 percent.

[577] Willemsen, Roald and Abraham, Jorij, et al. 'Australia B2C E-commerce Report 2016'. 2016, Last accessed 3 August 2020, https://www.ecommerce-europe.eu/wp-content/uploads/2016/09/Australia-B2C-E-commerce-Light-Country-Report.pdf.

[578] Doyle, Mary-Alice and Fisher, Chay et al. 'How Australians Pay: Evidence from the 2016 Consumer Payments Survey', Reserve Bank of Australia, April 2017, Last accessed 3 August 2020, https://www.rba.gov.au/publications/rdp/2017/pdf/rdp2017-04.pdf.

[579] Roy Morgan, 'The Way Australians Bank', 4 May 2018, Last accessed 3 August 2020, https://www.roymorgan.com/findings/7577-the-way-australians-bank-201805040431.

Figure 5.1: Shares of total e-commerce sales value by payment type in Australia



Note: Forecast adjusted for expected impact of COVID-19.
Source: eCommerce-Australia, Statista, (August 2020), [Online] Available at https://www.statista.com/outlook/243/107/ecommerce/australia#market-arpu [accessed: 10 August 2020].

While e-payment use has been high in Australia for some time, payment processing systems were relatively slow, and limited to processing during banking hours. Consumers and vendors would have to wait up to three days for transactions to complete over a weekend. The Australian system which runs the transfer of funds between cards is called the Electronic Funds Transfer at Point of Sale (EFTPOS), which is only run in Australia and is incompatible with other economies' systems. In terms of cross-border commerce, e-payments were typically handled by third parties such as PayPal with high transaction fees.[580]

As such, the Australian government saw a need to modernize the underlying payments system, and launched the New Payments Platform (NPP) in February 2018 to provide RTP payments 24/7 with the potential for cross-border interoperability.

New Payments Platform (NPP)

A. Background and development

In 2012, the Reserve Bank of Australia (RBA) established strategic goals for payment infrastructure improvements based on a review of current functionality and needs in the payments system. The RBA identified the following areas for improvement:

- Enabling users to make RTP payments;
- Sending more complete remittance information with payments;
- Addressing payments in a relatively simple way; and
- Making and receiving payments outside normal business hours.

[580] imrg, 'Payments Methods in Australia', Last accessed 3 August 2020, https://www.imrg.org/australia-payments/.

RBA developed "core criteria" to provide the financial industry with clear requirements for achieving these goals. In 2014 the RBA approved a proposal by an industry committee for them (i.e., the industry) to lead development and operation of the NPP. Twelve financial institutions committed to funding this effort and became the founding members of NPP Australia Limited (NPPA), which is a company established to run the NPP.

NPPA contracted professional services firm KPMG to manage the project with the member financial institutions acting as shareholders of NPPA, operating the NPP as mutually-owned utility infrastructure. Secure financial messaging services provider SWIFT was contracted by NPPA to build the NPP's basic infrastructure and Australian payment service BPAY Osko was selected to build the platform's first overlay payment service for consumers.[581]

RBA built the Fast Settlement Service (i.e., the settlement component of the NPP), which allows the transactions to be settled individually in nearly real time on a 24/7 basis. RBA's Banking Department is also a customer of the NPP infrastructure.[582]

B. Capabilities

Third parties can introduce overlay services on top of NPP's core capabilities to provide new features and convenience to customers. One example of such an overlay service is Osko, a retail-focused fast payment service which banks can offer their customers via their mobile and internet banking platforms. It is mostly focused on supporting person to person transfers. Other potential overlay services include "payment with a document" and "request to pay", which would allow vendors to request payment from a customer who can then respond and pay in real time.

To simplify the payment process and avoid repeated entry of long account numbers, NPP established a new form of identification called "PayID." This allows customers to use a phone number or email address for ID, which is linked to the account number. About 50 banks, credit unions and building societies began offering their customers the opportunity to set up PayIDs in 2018.

Another advantage to NPP is richer transaction descriptions than were possible with existing payment systems. Whereas other systems limited this field to 18-30 characters, NPP allows consumers to use up to 280 characters to describe their transfers, making it much easier to clearly communicate the purposes of complex transactions to recipients.[583]

---

[581] Reserve Bank of Australia, 'The Development and Initial Operations of the NPP', June 2019, Last accessed 3 August 2020, https://www.rba.gov.au/payments-and-infrastructure/new-payments-platform/functionality-and-access-report/the-development-and-initial-operations-of-the-npp.html.

[582] Reserve Bank of Australia, 'The New Payments Platform', Last accessed 3 August 2020, https://www.rba.gov.au/payments-and-infrastructure/new-payments-platform/.

[583] Watson, Tom, 'Banking in a flash: A guide to the New Payments Platform (NPP)' Mozo, 15 February 2018, Last accessed 3 August 2020, https://mozo.com.au/bank-accounts/guides/banking-in-a-flash-a-guide-to-the-new-payments-platform-npp.

In some ways NPP's capabilities are progressing faster than industry adoption. NPP can already receive an instruction from an overseas entity to transfer funds for a payment in real-time. However, according to the Emerging Payments Association Asia, Australian banks will not enable that feature yet because they do not have the necessary security checks in place yet, and moreover do not see a clear benefit to their operations from facilitating transactions for foreign institutions.[584]

C. Stakeholder engagement

From 2010 to 2012, RBA consulted with the payments industry and other key stakeholders to compare Australia's progress on payment system innovation with other economies. RBA concluded that the financial industry's ad hoc collaborative approach to innovation in payments system infrastructure and services has resulted in slow progress in Australia, typically moving at the pace of the slowest institutions.[585]

In the conclusions to its 2012 review of payment systems, RBA identified four specific gaps in the existing payments system that could become increasingly problematic if not resolved.[586] Specifically, they highlighted the following needs:

1. Real-time processing for payments

The capacity for real-time retail payments could help individual consumers to make personal payments to other individuals or businesses, help businesses to make more efficient use of cash balances since there is no waiting time to receive payments, and help government agencies to make emergency assistance payments quickly.

2. 24/7 payment processing

24/7 processing would eliminate lengthy payment delays over weekends and holidays. The systems used for the exchange of non-card payment instructions between institutions did not operate on weekends at the time of the review, delaying interbank settlement and posting payments to accounts until the following week. Therefore a bank transfer started on a Friday might not be received until the following Tuesday.

3. Transmission of data with payments

The RBA found that providing the capacity to carry additional remittance information with payments could result in a significant improvement to business efficiency. At the time bank transfer messages could carry a maximum of only 18 characters of additional remittance information with the payment message, which prevents for example businesses from incorporating detailed information about the goods/services being paid for, complicating

[584] Washington Core interview with John Ryan, Emerging Payments Asia (19 July 2020).

[585] Richards, Tony, 'An Update on Australia's New Payments Platform', Reserve Bank of Australia, 3 October 2018, Last accessed 3 August 2020, https://www.rba.gov.au/speeches/2018/sp-so-2018-10-03.html.

[586] 'Strategic Review of Innovation in the Payments System: Conclusions'. Reserve Bank of Australia, June 2012, 6-12, Last accessed 3 August 2020, https://www.rba.gov.au/payments-and-infrastructure/payments-system-regulation/past-regulatory-reviews/strategic-review-of-innovation-in-the-payments-system/conclusions/pdf/conclusions-062012.pdf.

bookkeeping. The ISO 20022 message standard solves this issue by enabling the inclusion of a large amount of data.

4. Addressing payments

According to RBA, the method by which the payer has to provide the payee's account details fundamentally affects the ease of use of a payment system, and it is preferable to make it as simple as possible. In Australia, the payee's bank branch number and account number had to be provided to conduct a bank transfer, resulting in problems such as the payer not remembering the payee's account info, or the payee not wanting to share his/her account info due to fraud concerns, or data entry errors due to the long 15-digit account numbers. These challenges are believed to make some people reluctant to make e-payments, and also cause significant costs when payments end up being made mistakenly to the wrong account.[587]

The Australian Payments Network, the payments industry association, coordinated the industry's response to the RBA's review, establishing a Real-Time Payments Committee to prepare the proposal for the NPP. Following approval, the industry established a Steering Committee to guide the project and invited RBA to contribute two representatives, one from its policy area and one from its settlements infrastructure area. RBA also helped NPP participants to maintain sufficient liquidity to enable the smooth operation of the NPP.[588]

D. Implementation challenges and adoption status

The NPP was launched with an initial group of 61 financial institutions participating, later increasing to 80. This number also includes 68 smaller financial institutions and one non-bank payment provider that access the NPP indirectly through the services of an aggregator or another sponsoring participant, which means they do not need to operate their own payment gateways to directly connect to the NPP.

Financial institutions have generally opted for a staged approach to rolling-out their end-user NPP services (i.e., gradually offering various functionality, channels and customer segments). For example, some major banks prioritized retail vis-à-vis business customers, or mobile banking over internet banking access. Some banks have offered services with restricted functionality (e.g., ability to only make payments to registered PayIDs with relatively lower payment limits).

The RBA has expressed disappointment with the gradual pace of this roll-out, noting that while some banks may legitimately need additional time to refine their systems and processes as they go along, others appear to have made insufficient efforts to prepare. Some of the major banks

[587] Ibid.

[588] '2. The Development and Initial Operations of the NPP', Reserve Bank of Australia, June 2019, Last accessed 3 August 2020, https://www.rba.gov.au/payments-and-infrastructure/new-payments-platform/functionality-and-access-report/the-development-and-initial-operations-of-the-npp.html.

could have underestimated the complexity of integrating the NPP with their own legacy systems and therefore, the related investment required for upgrades. For example, the RBA's Assistant Governor for Financial System, Michele Bullock said that while the four largest banks have connected their back-end systems with the NPP, they still need to work on enabling communications between their customer-facing front end systems and the NPP.[589] In November 2018, RBA Governor Philip Lowe further noted that smaller financial institutions had been quicker to provide NPP functionality to customers than the large institutions.[590]

This gradual roll-out has contributed to delays in the development of planned overlay services for the NPP including the ability to send a document with a payment and the ability to make and receive payment requests. For example, while extensions to BPAY's Osko service were initially expected to be operational shortly after the NPP's launch, they are now not expected to become available before late 2020 at the earliest.

Another obstacle to rapid adoption is the existence of a variety of other payment options for Australian consumers and businesses, and many have not come to appreciate the value of NPP enough to want to move away from their current payment methods. More public outreach and education is needed to effectively communicate the benefits of NPP and drive interest. Once the merchants understand that maybe they could use NPP for free and get useful additional information on their transactions, adoption could increase. Enabling QR codes is also very important for adoption by retailers.[591]

Although the roll-out has been slower than expected, the number of end-users with access to RTP payments, as well as the number and value of transactions through the NPP platform have been growing steadily. While the total value of transactions remains relatively low compared with other retail payment systems in Australia, RBA points out that the speed of adoption of the NPP has been roughly similar to RTP systems in the UK and Sweden.[592]

There is a big discussion now in Australia about a possible consolidation of NPP with the other two major Australian payment networks – EFTPOS and BPAY[593] - but this is complicated by

[589] Bajkowski, Julian. 'Big four legacy systems cop another spanking from RBA over slow NPP progress', itnews, 25 February 2019, Last accessed 3 August 2020, https://www.itnews.com.au/news/big-four-legacy-systems-cop-another-spanking-from-rba-over-slow-npp-progress-519791.

[590] Lowe, Philip. 'A Journey Towards a Near Cashless Payments System', Reserve Bank of Australia, 26 November 2018, Last accessed 3 August 2020, https://www.rba.gov.au/speeches/2018/sp-gov-2018-11-26.html.

[591] Washington Core interview with John Ryan, Emerging Payments Asia (19 July 2020).

[592] Fitzgerald, Emilie and Rush, Alexandra. 'Two Years of Fast Payments in Australia', Reserve Bank of Australia, 19 March 2020, Last accessed 3 August 2020, https://www.rba.gov.au/publications/bulletin/2020/mar/two-years-of-fast-payments-in-australia.html.

[593] EFTPOS and BPAY operate as mutually-owned low-cost payments infrastructure providers for banks and big merchants. Overseen by the RBA and industry self-regulatory body AusPayNet, this 'direct entry' system of bilateral bank-to-bank connections enables Australians to transfer money directly from their bank accounts to another person or merchant. Source: Bajkowski, Julian, 'Big four legacy systems cop another spanking from RBA over slow NPP progress, itnews, 25 February 2019, Last accessed 3 August 2020, https://www.itnews.com.au/news/big-four-legacy-systems-cop-another-spanking-from-rba-over-slow-npp-progress-519791.

the fact that there are so many existing clients on each network. It may take a few years to transition everyone to NPP.[594] This discussion was begun by a Review of Retail Payments Regulation paper released by the RBA in November 2019 to solicit industry feedback. Submissions from the Commonwealth Bank of Australia (CBA) and the ANZ Banking Group, two of Australia's top four banks, suggested that it would be more efficient to move Australia toward a single industry-wide payments platform to replace the fragmented approach that includes payment methods such as EFTPOS, BPAY, and personal checks.

E. Interoperability with other economies

Recognizing the move towards international standards and the potential cross-border interoperability benefits, the NPP was built using the ISO 20022 messaging standard, as described in Box 5.2. The NPP platform was enabled to support in-bound cross-border payment (international funds transfer instruction (IFTI) Payments) in late 2019,[595] although banks have not yet offered this functionality to customers.

Migrating to ISO 20022 is not an easy step for payment providers, requiring changes to back-office systems; treasury and liquidity management systems; fraud, Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) monitoring and sanctions screening systems; and downstream client systems.[596]

Box 5.2: ISO 20022 standard

The ISO 20022 messaging format has become the leading international standard for electronic data interchange between financial institutions. ISO 20022 can carry much richer payment descriptions than previous messaging formats, providing more than 1,400 data fields in the payment clearing message, and additional data can be provided via linked documents. The structured data capabilities of ISO 20022 enable the development of a common data lexicon for particular payment types to ensure consistent use by all participants involved in the processing of a payment. Using these common and consistent data elements in existing business processes and systems will enable greater automation of payment processing, increasing efficiency by reducing error rates and exceptions and therefore reducing the amount of manual reconciliation effort required.

SWIFT, the worldwide messaging network used by banks and other financial institutions which acts as the registration authority for ISO 20022, is working aggressively to promote

[594] Washington Core interview with John Ryan, Emerging Payments Asia (19 July 2020).
[595] NPP Australia Limited. 'ISO 20022 Migration for the Australian Payments System – Issues Paper – Response Template'. Reserve Bank of Australia, April 2019, Last accessed 3 August 2020, https://www.rba.gov.au/payments-and-infrastructure/submissions/migration-for-the-australian-payments-system/pdf/nppa.pdf.
[596] 'ISO 20022 Migration for the Australian Payments System – Issues Paper'. Reserve Bank of Australia, April 2019, Last accessed 3 August 2020, https://www.rba.gov.au/publications/consultations/201904-iso-20022-migration-for-the-australian-payments-system/pdf/issues-paper.pdf.

worldwide adoption of the standard, and will migrate all SWIFT-based cross-border payment messages and reporting to ISO 20022 by November 2022.

In November 2019, SWIFT released a first set of guidelines for using ISO 20022 in cross-border payments. SWIFT expects that adoption of ISO 20022 by the financial industry will lead to the standard supporting over 80% of high-value payments worldwide by the end of 2025, at which point SWIFT will decommission corresponding legacy messaging and reporting on its platform.

Sources:

- ISO, 'ISO 20022', Last accessed 1 August 2020, https://www.iso20022.org/
- NPP Australia Limited, 'New Payments Platform Roadmap 2019', 28 October 2019, Last accessed 1 August 2020, https://nppa.com.au/wp-content/uploads/2019/10/NPP-Roadmap-2019_28-Oct-2019-final.pdf
- The Banker, 'Getting ready for Europe's new payments architecture', 25 November 2019, Last accessed 1 August 2020, https://www.thebanker.com/Transactions-Technology/Getting-ready-for-Europe-s-new-payments-architecture
- Lakhwani, Nanda. 'SWIFT defers ISO 20022 cross-border payment migration', FST Media, 18 March 2020, Last accessed 1 August 2020, https://fst.net.au/financial-services-news/swift-defers-iso-20022-cross-border-payment-migration/.
- Swift, '[UPDATED] ISO 20022 usage guidelines for cross-border payments released', 2019, Last accessed 1 August 2020, https://www.swift.com/news-events/news/news-overview/updated-iso-20022-usage-guidelines-cross-border-payments-released

In comments to the RBA in 2019, the NPPA suggested that the RBA work with industry to promote awareness of the benefits of ISO 20022 amongst payment systems, financial services and other industries that use the payment system. Feedback should be sought from industry stakeholders about how to manage the transition from legacy to ISO 20022 compliant systems, and a phased migration approach should be laid out with clear and reasonable deadlines. NPPA also suggested that Australia learn from best practices established by other large scale migration programs such as the U.S. Federal Reserve Bank's ISO 20022 Migration Plan and Canada's Modernisation Program.[597] In its comments to the RBA, the CBA also suggested that the timing of banks' migration to ISO 20022 will be influenced by how quickly other major markets such as the U.S. and Europe adopt ISO 20022 for cross border payments.[598]

[597] NPP Australia Limited. 'ISO 20022 Migration for the Australian Payments System – Issues Paper – Response Template', April 2019, Last accessed 3 August 2020, https://www.rba.gov.au/payments-and-infrastructure/submissions/migration-for-the-australian-payments-system/pdf/nppa.pdf.

[598] Commonwealth Bank. 'ISO 20022 Migration for the Australian Payments System – Issues Paper – Response Template'. September 2019, Last accessed 3 August 2020, https://www.rba.gov.au/payments-and-infrastructure/submissions/iso-20022-migration-for-the-australian-payment-system/pdf/commonwealth-bank-of-australia.pdf.

F. Expected impact on cross-border E-commerce

The recent introduction of the NPP and so far gradual adoption rate make it difficult to assess the potential impact on e-commerce growth. According to a March 2019 RBA survey, only 20 percent of consumers had heard of NPP, and only 10 percent of consumers had actually used NPP to make purchases.[599] NPPA announced in June 2019 that online car marketplace Carsales.com.au had become the first non-financial business to use the NPP for consumer purchases.[600]

In late 2019 fintech firm Azupay launched the first consumer-to-business payment service to use the NPP's PayID capabilities. Azupay enables businesses to create one-off PayID QR codes to make payments easier for customers. The consumer only needs to scan the QR code in their online or mobile banking app and confirm the amount, so there is no need to enter payment information or to share any sensitive information with the merchant.[601] One of the first business users was the New South Wales State Government's Department of Customer Service, which enabled Azupay payments for Liquor and Gaming license renewals.[602]

As of April 2020, there were more than 67 million Australian bank accounts accessible via the NPP (equal to about 90 percent of all accounts that will eventually be reachable) and around 4.7 million PayIDs had been registered. The Osko payment service processed over 34 million payments in June 2020, for a total value of AUD 48 billion (USD 34.5 billion).[603] Approximately one third of all NPP transactions are for payments to or from a business, although it is unclear what percentage of this total is for e-commerce payments. NPPA notes that the COVID-19 pandemic seems to have led to a rise in PayID acceptance by small businesses such as restaurants, cafes and salons to improve cash flow and to enable contactless payments.[604]

Conclusion

Australia's experience with the NPP platform shows that an organized industry-led and government enabled effort including the leading financial institutions can bring needed innovation to e-payments infrastructure at an efficient pace. However, merely introducing an effective new payment option in a crowded marketplace is not a guarantee that consumers will

[599] Reserve Bank of Australia, 'Consumer Payment Behaviour in Australia', 19 March 2020, Last accessed 3 August 2020, https://www.rba.gov.au/publications/bulletin/2020/mar/consumer-payment-behaviour-in-australia.html.
[600] Lovney, Adrian. 'New Payments Platform Update - 2nd Annual Real-Time Payments Summit', NPP Australia Limited, 14 June 2019, Last accessed 3 August 2020, https://www.rtpsummit.com/sydney/wp-content/uploads/2019/06/10.45-NPP.pdf.
[601] NPP Australia Limited, 'Azupay to use NPP's speed and PayID for real-time validation and processing for online payments', 8 October 2019, Last accessed 3 August 2020, https://nppa.com.au/azupay/.
[602] NPP Australia Limited, 'Five million PayIDs registered in Australia', 24 July 2020, Last accessed 3 August 2020, https://nppa.com.au/five-million-payids-registered-in-australia/.
[603] Reserve Bank of Australia, 'Statistical Tables C6 and C6.1', June 2020, Last accessed 3 August 2020, https://www.rba.gov.au/statistics/tables/.
[604] NPP Australia Limited, 'Update on the New Payments Platform Roadmap - Enhancing the platform's capabilities', 30 April 2020, Last accessed 3 August 2020, https://nppa.com.au/wp-content/uploads/2020/04/NPP-Roadmap-April-2020_final.pdf.

quickly embrace it or that financial institutions will fully support it. Further work is needed to communicate the NPP's benefits to the Australian public and merchants, possibly via promotional trials, and to persuade and/or compel through regulation financial institutions to support all functionality, including in the future cross-border payments.

Thailand

Thailand has a rapidly growing e-commerce market that still remains relatively small compared to its population size, and heavily concentrated on social media based transactions which typically do not support credit card payments. The government has taken ambitious steps to modernize the e-payments infrastructure to give more consumers and businesses access to convenient e-payment services, while at the same time pursuing cross-border payment agreements with multiple neighboring economies. The experience of Thailand with the recent launch of its RTP system, is informative for developing economies seeking to increase consumer adoption of e-payment systems and integration with other economies' e-commerce markets.

Cross-border e-commerce growth trends

With a population of 69 million and close proximity to major economies in the APEC region (e.g. China, Australia), Thailand has rich potential to expand its e-commerce market. With that said, the current cross-border e-commerce market is somewhat small relative to population. In total, the e-commerce market in Thailand is THB823 billion (USD 26.2 billion), roughly equal with Australia despite having nearly three times the population. Cross-border online spending is equivalent to 50 percent of total e-commerce spending, or approximately THB 412 billion (USD 13 billion).[605]

Technology barriers to e-commerce growth remain. The percentage of the population with internet access continues to grow steadily, but remains at 75 percent as of January 2020. Under the government's Thailand 4.0 policy, private firms have been working with the government to provide broadband infrastructure and 4G service in rural areas of the economy.[606]

Additionally, there are logistics challenges. Delivery infrastructure, including trucks and warehouses, is not fully developed outside urban centers, and major courier services need to supplement their networks to bring products to customers in rural areas. The government's logistics development strategy phase 3 for 2017-2021 is focused on general improvements to

[605] J.P. Morgan, 'E-commerce Payments Trends: Thailand', 2019, Last accessed 3 August 2020, https://www.jpmorgan.com/europe/merchant-services/insights/reports/thailand.
[606] Ibid.

capacity at all stages of the value chain in Thailand, notably including the development of e-commerce distribution channels.[607]

Nevertheless, as of 2019 there were 39.8 million e-commerce users in Thailand, a six percent increase over 2018.[608] The value of Thailand's e-commerce sector has expanded rapidly in recent years, with 48.7 percent growth in 2016 and 26.8 percent growth in 2017, and an expected compound annual growth rate of 12.5 percent in business to consumer e-commerce through 2021.[609]

Moreover, Thais that engage in e-commerce are spending significant amounts. The average annual online spend, at THB54,848 (USD1,746), is among the highest in Southeast Asia. The most popular online shopping category is travel (57 percent of total value), followed by consumer electronics (15 percent).[610]

E-payments motivation and adoption status

Cash is still the primary means of payment in Thailand for retail in general, in part because only 29 percent of the population has credit cards, and only 77 percent have debit cards.[611][612] Efforts by the government to promote electronic payments through the National e-Payment Master Plan and especially PromptPay, the Bank of Thailand (BOT) sponsored RTP system, are expected to more than triple the share of non-cash payments from 6 percent in 2014 to 22 percent by 2022.

The breakdown of payment types for e-commerce in Figure 5.2 shows that credit cards were the most widely used as of 2019, representing 30 percent of the total value of e-commerce transactions. However, bank transfers (including PromptPay) and digital wallets were close behind at 23 percent each. The use of digital wallets such as PayPal, TrueMoney and AirPay is forecast to rise at a compound annual growth rate of 18 percent through 2021, with its share of e-commerce transaction value rising to 28 percent.[613] As of 2019, 10.7 percent of the adult population of Thailand was using digital wallets, one of the highest rates in the world. Additionally, China, which at 35 percent of population has by far the world's highest rate of

[607] Krungsri Research, 'From Pipeline to Platform: New Wave of Change in Payment Business', February 2019, Last accessed 3 August 2020, https://www.krungsri.com/bank/getmedia/1e094a1b-ebf4-4a97-b170-b6315f0e4709/RI_Payment_Strategies_190204_EN.aspx.

[608] B., Katrina B. & L., Benedict, 'Who are Thailand's eCommerce Consumers?', Janio, 23 July 2019, Last accessed 3 August 2020, https://janio.asia/articles/who-are-thailands-ecommerce-consumers/.

[609] J.P. Morgan, "E-commerce Payments Trends: Thailand", 2019, Last accessed 3 August 2020, https://www.jpmorgan.com/europe/merchant-services/insights/reports/thailand.

[610] Ibid.

[611] Ibid.

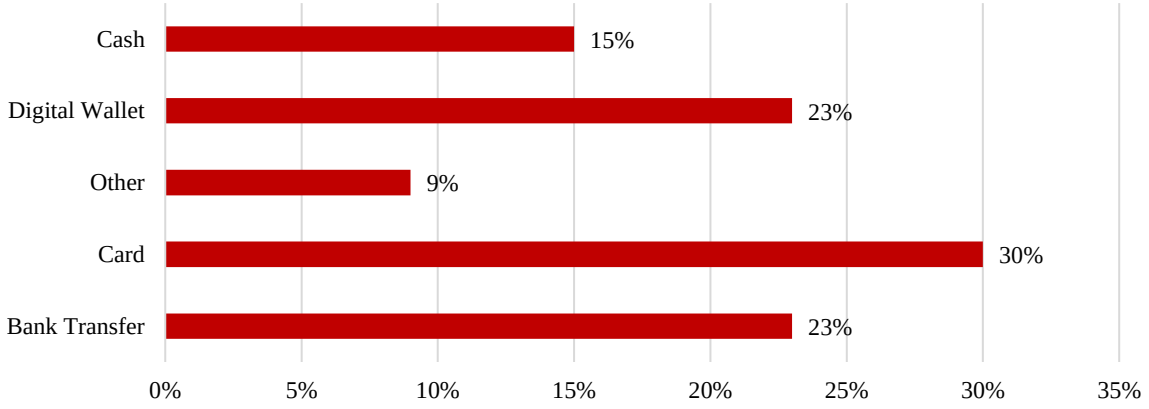
[612] Schellhas, John and Warden, Staci, 'Framing the Issues: The Future of Finance in Thailand', Milken Institute, July 2018, Last accessed 3 August 2020, https://milkeninstitute.org/sites/default/files/reports-pdf/Framing-the-Issues-Future-of-Finance-BOT.pdf.

[613] J.P. Morgan, 'E-commerce Payments Trends: Thailand', 2019, Last accessed 3 August 2020, https://www.jpmorgan.com/europe/merchant-services/insights/reports/thailand.

digital wallet usage and minimal credit card usage, is one of the top three economies for Thai cross-border e-commerce spending.[614] This is likely to further familiarize Thai consumers with non-card transactions.

The use of cash for e-commerce transactions has declined and is expected to fall to 12 percent by 2021, but it remains significant.[615] Consumers without credit or debit cards typically have to physically go to a bank or a convenience store to make a payment to an online retailer's account, or pay by cash on delivery. 48 percent of Thais who made internet purchases in 2017 paid by cash on delivery.[616]

Figure 5.2: Breakdown of payment types for e-commerce in Thailand



Source: J.P. Morgan, 'E-commerce Payments Trends: Thailand', 2019, Last accessed 2020, https://www.jpmorgan.com/europe/merchant-services/insights/reports/thailand.

It is important to consider that Thai consumers are unique in that they do most of their e-commerce shopping through social media apps such as Facebook, Facebook Messenger, and Line; rather than major e-commerce websites. As of 2016, Thailand was the most active social commerce market in the world, with 51 percent of online shoppers in Thailand placing orders through social media, compared with the global average of 16 percent.[617] In 2017 social media accounted for 40% of the value of B2C e-commerce transactions in Thailand, ahead of e-marketplaces and online retailers.[618]

[614] de Sartiges, Diego and Bharadwaj, Aparna et al. 'Southeast Asian Consumers Are Driving a Digital Payment Revolution', Boston Consulting Group, 20 May 2020, Last accessed 3 August 2020, https://www.bcg.com/publications/2020/southeast-asian-consumers-digital-payment-revolutions.

[615] J.P. Morgan, 'E-commerce Payments Trends: Thailand', 2019, Last accessed 3 August 2020, https://www.jpmorgan.com/europe/merchant-services/insights/reports/thailand.

[616] Fintech Alliance, 'PromptPay – two years of transforming Thai payments', 29 January 2019, Last accessed 3 August 2020, https://fintech-alliance.com/news-insights/article/33/promptpay-two-years-of-transforming-thai-payments/payments.

[617] B., Katrina B. & L., Benedict. "Who are Thailand's eCommerce Consumers?", Janio, 23 July 2019, Last accessed 3 August 2020, https://janio.asia/articles/who-are-thailands-ecommerce-consumers/.

[618] Ibid.

This is significant for e-payment behavior, because small businesses doing business through social media pages are more likely to accept easier and cheaper forms of payment (in terms of processing) such as PromptPay and digital wallets, as opposed to credit cards.

PromptPay

A. Background and development

In 2015, the Ministry of Finance and the BOT created the National e-Payment Master Plan in cooperation with related government and private entities to drive the development of payment infrastructures and to promote the use of e-payment services. This plan includes the PromptPay initiative, which sought to promote e-payment usage by establishing an RTP platform that enables users to make peer-to-peer transfers and payments from their bank account through their mobile phone using only the recipient's mobile number or economy ID number.[619]

In particular, PromptPay was intended to address the following goals for improving interbank transfers:

- Lower transaction fees
- Single integrated infrastructure - PromptPay is a centralized system that consolidated two switching providers in the legacy online retail fund transfer system. These two systems provided respective services for transactions made via ATMs and banks on the one hand, and for internet/mobile transactions on the other. It was considered too costly and inefficient to develop add-on services or improvements to both systems.
- Convenience – Can use proxy ID instead of typing long bank account number to make fund transfers.[620]

In 2017 the Thai government and BOT approached UK-based real-time payment systems provider Vocalink to develop the PromptPay platform to support their Financial Services Master Plan (FSMP) to transform Thailand's financial infrastructure. Amongst the plan's objectives were modernizing the economy's technology, driving innovation in financial services, addressing financial inclusion and reducing an over-reliance on cash – especially among the poor and rural populations.

Vocalink worked on the development of PromptPay with banks and National ITMX (National Interbank Transaction Management and Exchange), a developer and e-payments platform provider established by the Thai Bankers' Association under direction of Payment System

[619] Bank of Thailand, 'Payment Systems Roadmap No.4 (2019-2021)'. Last accessed 3 August 2020, https://www.bot.or.th/English/PaymentSystems/PolicyPS/Documents/PaymentRoadmap_2021.pdf.

[620] Lamsam, Atchana and Pinthong, Jaree et al., 'The Journey to Less-Cash Society: Thailand's Payment System at a Crossroads', Puey Ungphakorn Institute for Economic Research, December 2018, Last accessed 3 August 2020, https://www.pier.or.th/wp-content/uploads/2018/12/pier_dp_101.pdf.

Committee (PSC) and governed by BOT.[621] PromptPay's real-time clearing and settlement infrastructure is based on Vocalink's Instant Payment Service with a 'translator' for communicating between ISO 8583 - commonly used by banks and ATMs in Thailand - and ISO 20022 messages, combined with a proxy look-up service that links customer aliases to bank accounts.[622]

To help simplify PromptPay transactions and drive usage, the BOT collaborated with credit card issuers such as American Express and Visa in 2017 to introduce the Thai QR Code Payment standard. Although the most common application for QR codes is in physical retail, online merchants can generate a QR code for a transaction and send it to the customer to make payment by PromptPay or digital wallet.

B. Capabilities

Similar to NPP and other RTP systems, PromptPay enables users to make and receive payments via their bank accounts and/or digital wallets linked to their economy IDs, mobile phone numbers or email addresses. By supporting the use of established personal identifiers as proxies for a person's bank account or digital wallet, unbanked citizens can use digital wallets to make and receive free digital payments, using PromptPay through partnering banks to add funds to their wallets.[623] For example, digital wallet provider TrueMoney has such an arrangement with Siam Commercial Bank (SCB).[624]

One major appeal for consumers is that the PromptPay ID can be used for payment, so that there is no need to share sensitive financial information like a bank account number with a merchant. This is important, because Thais are very concerned about security online. A 2014 study found that 62 percent of online shoppers in Thailand did not want to provide their credit card information online.[625]

Additionally, if the merchant provides a QR code then the payer can simply scan the code in his/her banking or digital wallet app, and there is no need to enter any account or amount information. Major Thai banks like Kasikorn and SCB have released their own PromptPay-based merchant apps.

---

[621] Mastercard, 'Mastercard and National ITMX Widen E-Commerce Acceptance of Thai Debit Cards', 25 February 2019, Last accessed 3 August 2020, https://newsroom.mastercard.com/asia-pacific/press-releases/mastercard-and-national-itmx-widen-e-commerce-acceptance-of-thai-debit-cards/.

[622] Vocalink, 'PromptPay - Transforming Thailand towards a digital economy', Last accessed 3 August 2020, https://www.vocalink.com/news-insights/case-studies/case-study-thailand-promptpay/.

[623] Fintech Alliance, 'PromptPay – two years of transforming Thai payments', 29 January 2019, Last accessed 3 August 2020, https://fintech-alliance.com/news-insights/article/33/promptpay-two-years-of-transforming-thai-payments/payments.

[624] The Nation Thailand, 'TrueMoney and SCB offer PromptPay service', 17 September 2017, Last accessed 3 August 2020, https://www.nationthailand.com/business/30326933].

[625] Retail in Asia, 'RetailWATCH: Lifting the barriers to e-commerce in ASEAN', 16 February 2015, Last accessed 3 August 2020, http://www.retailinasia.com/article/tech/online-retailing/2015/02/retailwatch-lifting-barriers-e-commerce-asean.

Furthermore, fees for PromptPay payments, which are paid by the payer, are very low compared to alternatives like credit cards and PayPal. Compared to Thai banks, which had charged a minimum fee of THB25–35 (USD0.79 – 1.11) for interbank transfers, PromptPay transactions less than THB5,000 (USD159) are free, and cost only THB10 (USD0.32) for THB150,000 (USD4,765) transactions. This makes PromptPay competitive with digital wallets which also typically allow free transfers of funds. Micropayments as little as THB1 can be made with PromptPay for free, whereas with PayPal for example the fee would exceed the amount of the purchase.

In response to this new competition, Thai banks have lowered their interbank transfer fees. For example transferring THB100,000 (USD3,180) from Kasikorn Bank to SCB Bank used to cost THB70 (USD2.22 USD), but now is free.[626]

For merchants, it is appealing that PromptPay payments typically cannot be reversed, unlike PayPal and other digital wallet providers which allow customers to reverse charges in the case of a dispute, an ability that some customers abuse. PromptPay payments can only be reversed if there is a crime or bank error.[627]

C. Stakeholder engagement

In 2017, just after the launch of PromptPay, the BOT conducted a survey to learn more about the general public's understanding and behavior concerning e-payment services to inform the BOT's fourth Payment Systems Roadmap (2019-2021). Input was also solicited from industry stakeholders. The survey collected data from over 10,000 respondents, representing adults from all age groups and all provinces, including urban and rural areas.

The survey revealed that a majority of respondents had relatively limited knowledge and understanding of e-payments. Less than 50 percent were aware of mobile and internet banking. Moreover, although 68 percent of the respondents used at least one mode of e-payment, a majority of the respondents still preferred cash for small-value day-to-day transactions. For high-value transactions such as bill payments, e-payment was preferable as consumers perceived it to be safe and appreciated the ability to keep a record of past transactions.

Concerning wealthier consumers more likely to be knowledgeable about e-payments, the BOT determined the best approach to increase e-payments usage would be to offer additional convenient e-payment services to create pleasant experiences to induce repeat use. As for lower income consumers with less understanding of e-payments, the keys to increasing adoption include educational outreach and expansion of the government's welfare smart card project.[628]

---

[626] B., Bryan, 'Does PromptPay have a future?', Medium, 5 June 2018, Last accessed 3 August 2020, https://medium.com/mobiletopup/does-promptpay-have-a-future-a3c35efa6bb5.

[627] Ibid.

[628] Government welfare payments are made directly and immediately to recipients by transferring funds via PromptPay to smart state welfare cards, which can be used to purchase of goods via electronic data capture (EDC) terminals of participating

The BOT has urged all relevant stakeholders from government to retailers to e-payment service providers to promote e-payment service usage to the public by offering promotional trials and creating convenient e-payment user experiences.[629]

D. Implementation challenges and adoption status

Implementation of PromptPay was initially complicated by the fact that Thailand's major banks' systems and ATM networks use the ISO8583 messaging standard, and not ISO20022, the emerging global messaging standard for real-time payments. ISO8583 was originally introduced for card payments, but is not well-suited for RTP because the data field length is very short, making it difficult to include descriptive information on transactions such as originating parties and payment purposes.[630] Vocalink developed an adaptor to translate messages between ISO8583 and ISO20022 to resolve this conflict.

PromptPay has now been adopted by all the major banks in Thailand. Thai banks have in general been quick to provide new innovations in digital financial services on digital platforms to customers to improve engagement with current and new types of customers. Banks are facing increasing competition from technology companies offering financial services, and want to stay as close to customers as possible.[631]

The number of PromptPay transactions reached 2.9 million a day in June 2018, for a total value of THB 442 billion (USD 14 billion) for the month.[632] As of December 2018, 46.5 million users, two thirds of the economy's population, had registered for the system. Through January 2019, PromptPay had processed more than 765 million transactions with a cumulative value of over THB 3,848 billion (USD 123 billion).[633]

To develop and promote QR codes for PromptPay, the BOT encouraged international card networks (e.g., American Express, JCB, MasterCard, UnionPay International, and Visa), other financial institutions and local card networks and operators to collaborate, allowing banks and non-bank service providers to test the standardized QR Code on payments performed via mobile applications in a regulatory sandbox. Additionally, the BOT encouraged collaboration of the participants on development of related business rules, customer complaint handling

merchants. Bank of Thailand, 'Payment Systems Roadmap No.4 (2019-2021)', Last accessed 3 August 2020, https://www.bot.or.th/English/PaymentSystems/PolicyPS/Documents/PaymentRoadmap_2021.pdf.

[629] Bank of Thailand, 'Payment Systems Report 2017', Last accessed 3 August 2020, https://www.bot.or.th/English/PaymentSystems/Publication/PS_Annually_Report/Documents/Payment_2017_E.pdf.

[630] Long, Kimberly, 'Universal standard sought for real-time payments', Euromoney, 16 July 2015, Last accessed 3 August 2020, https://www.euromoney.com/article/b12kmh4sk6rvlv/universal-standard-sought-for-real-time-payments.

[631] Banchongduang, Somruedi, 'Cashless movement picks up steam', Bangkok Post, 1 August 2019, Last accessed 3 August 2020, https://www.bangkokpost.com/business/1722559/cashless-movement-picks-up-steam.

[632] Leong, Benedict, 'What's Happening in Thailand's eCommerce Market?', Janio, 5 July 2019, Last accessed 3 August 2020, https://janio.asia/sea/thailand/thailand-ecommerce-snapshot-trends/.

[633] Fintech Alliance, 'PromptPay – two years of transforming Thai payments', 29 January 2019, Last accessed 3 August 2020, https://fintech-alliance.com/news-insights/article/33/promptpay-two-years-of-transforming-thai-payments/payments.

arrangements, and the Thai QR Code Logo Guidelines. In 2017, nine banks and three non-bank payment service providers participated in the QR Code for PromptPay Project. The BOT subsequently granted permissions for 8 successful participants to provide QR Code services to the public. These banks are now providing consumer mobile applications that can scan the standardized QR Code for payments.[634]

PromptPay QR codes are said to be found at 20–30 percent of physical businesses in Thailand, promoted by banks seeking to build connections with customers. The quick adoption of PromptPay was fueled primarily by the Thai government's use of the platform to make social benefits and tax return payments to the public. Most government workers have been required to enroll in PromptPay.[635]

E. Interoperability with other economies

Thailand has been working with multiple jurisdictions, including Malaysia, Singapore, Cambodia, and other ASEAN economies, to facilitate cross-border real-time payments/remittances. A case in point here is a project to link remittance services between Thailand and Singapore, which is expected to be operational in 2021. Thais and Singaporeans will be able to exchange RTP payments between the PromptPay platform and Singapore's PayNow RTP platform.[636] DBS Bank in Singapore and Kasikorn Bank in Thailand have also privately collaborated to launch a real-time money transfer service in August 2018 through which DBS customers in Singapore could transfer up to THB 1.5 million (USD 47,600) per transaction in real-time via Kasikorn Bank to the bank accounts of 21 other Thai banks that are linked by a shared ATM network.[637] Singapore banks have already adopted ISO20022, and Thai and Malaysian banks are both working toward this goal to facilitate integration.

F. Impact on cross-border E-commerce

Several factors are driving rapid growth of Thailand's e-commerce market, among which rising e-payment adoption is a key factor. Fueled by the government's various initiatives to promote e-payments, cash transactions are expected to fall from 90 percent of all transactions in 2019 to 50 percent by the early 2020s, according to the U.S. Department of Commerce International Trade Administration.[638]

---

[634] Bank of Thailand, 'Payment Systems Report 2017', Last accessed 3 August 2020, https://www.bot.or.th/English/PaymentSystems/Publication/PS_Annually_Report/Documents/Payment_2017_E.pdf.

[635] B., Bryan, 'Does PromptPay have a future?', Medium, 5 June 2018, Last accessed 3 August 2020, https://medium.com/mobiletopup/does-promptpay-have-a-future-a3c35efa6bb5.

[636] Chan, Joelyn, 'Cross border payment systems in ASEAN gather steam', ASEAN Today, 16 August 2019, Last accessed 3 August 2020, https://www.aseantoday.com/2019/08/cross-border-payment-systems-in-asean-gather-steam/.

[637] Tan, Sherman, 'Crystal Ball Gazing: Retail Payments 2021', Innovar Pte Ltd, 29 August 2018, Last accessed 3 August 2020, https://www.linkedin.com/pulse/crystal-ball-gazing-retail-payments-2021-sherman-tan.

[638] U.S. International Trade Administration, 'Thailand – eCommerce', 9 August 2019, Last accessed 3 August 2020, https://www.export.gov/apex/article2?id=Thailand-ecommerce.

The adoption of secure digital payment options can help to boost e-commerce activity by offering greater convenience to consumers and online retailers. One obvious boost in cash-dependent Thailand is that e-payments can expand access to e-commerce vendors and the range of delivery options for e-commerce to include locations such as storage lockers, as the consumer no longer needs to be physically present to receive and pay for goods in cash.

PromptPay's cross-border linkages with Singapore, Cambodia and likely more economies to come will make it easier for cross-border e-commerce transactions to grow.[639]

Conclusion

Thailand's experience with the PromptPay platform shows a concerted effort to understand consumer needs and preferences along with concerted promotional efforts can achieve dramatic uptake in e-payments even among less sophisticated online shoppers. Care should also be taken to ensure that relevant stakeholders are engaged and their concerns sufficiently addressed (e.g., the development of an adaptor to translate messages between ISO8583 and ISO20022). Last but not least, close interaction with various stakeholders in other economies is essential to enhance payment system interoperability.

Key lessons

Success factors

- **Consultation with multiple stakeholders** – Engaging with stakeholders is critical for setting priorities, building support and fostering collaboration – Australia and Thailand began consulting with industry stakeholders early in the planning process for their RTP systems, and gave them an ongoing role in helping to form the approach and develop the system. In Thailand's case, where consumer literacy limitations on payment options is more of an issue, a wide-ranging survey was an important step to identifying the kinds of outreach and support that were needed for different types of consumers to encourage e-payment adoption. The development of China's E-commerce Law included public consultations. Moreover, two events were held to involve the international community in the process. Similarly, Chinese Taipei conducted public hearings during the entire process of enacting the Electronic Signatures Law to receive feedback from various stakeholders.
- **Flexibility** – Based on observations from surveys and/or market data on new payment innovations or needs, it is important for governments to be able to flexibly introduce and/or promote new services and technologies to seize opportunities in a timely manner that will support e-commerce and bolster international competitiveness. In the case of development of laws and regulations, flexibility entails being open to different perspectives and ensuring that the eventual laws and regulations endeavor to balance their varied interests while making sure that the primary objective is fulfilled.

[639] Leong, Benedict, 'What's Happening in Thailand's eCommerce Market?', Janio, 5 July 2019, Last accessed 3 August 2020, https://janio.asia/sea/thailand/thailand-ecommerce-snapshot-trends/.

- **Monitor and evaluate** – Economies need to recognize that it is critical for laws and regulations to be continuously adapted to the changing landscape. With regards to its Electronic Signatures Law, Chinese Taipei has noted several areas where improvements can be made. It is also open to public feedback via the public policy network participation platform. Acknowledging that the E-Commerce Law is relatively young and room for improvements may only be identified through implementation and operationalization, China indicated it would continue to monitor the impact of the law and introduces supporting regulations to clarify aspects of the law where relevant.
- **Promote trial** – The Thai government was able to achieve extremely rapid public uptake of PromptPay by starting to make instantaneous tax return and welfare payments via PromptPay. This naturally motivated the public to quickly sign up for PromptPay.[640]
- **Value proposition** – In Thailand the value of PromptPay was relatively easy to convey to consumers and businesses largely dependent on cash – fast, easy, secure and recorded transactions, as well as no need to wait around to make cash on delivery (COD) payments. In the highly mature and sophisticated payments market in Australia the value add of NPP has been harder to get across to a public with already numerous cashless options, and additional convenience features may be needed to make NPP more clearly stand out as a compelling option.

Key considerations and capabilities for supporting cross-border transactions

- **Standards –** It is clearly advantageous to adopt commonly accepted international standards in order to connect with other economies. In the case of e-payments that is ISO20022, which Australia has already adopted and Thailand is working toward. However, switching to ISO20022 is not a painless process and close collaboration with the payment industry is advisable.
- **Bilateral agreements –** Enabling cross-border payments is primarily a regulatory challenge,[641] and therefore direct agreements between governments may be the fastest way to facilitate e-payment system interoperability. Thailand has been making strong progress on enabling cross-border e-payments through a number of memorandums of understanding, with economies including Indonesia, Malaysia, the Philippines, Singapore, Cambodia, Laos, and Myanmar.[642]

Concluding remarks

Economies are starting to take bold steps to align payment infrastructure better with the needs of consumers to facilitate e-commerce transactions as much as possible. APEC can play a valuable role in assisting with the following challenges:

[640] Bank of Thailand, 'Payment Systems Roadmap No.4 (2019-2021)', Last accessed 3 August 2020, https://www.bot.or.th/English/PaymentSystems/PolicyPS/Documents/PaymentRoadmap_2021.pdf.
[641] Washington Core interview with John Ryan, Emerging Payments Asia (19 July 2020).
[642] Chan, Joelyn, 'Cross border payment systems in ASEAN gather steam', ASEAN Today, 16 August 2019, Last accessed 3 August 2020, https://www.aseantoday.com/2019/08/cross-border-payment-systems-in-asean-gather-steam/.

1. Outreach activities – Experiences in Australia and Thailand show the value of careful outreach to explain the value and usage of new payment tools. Likewise, Chinese Taipei held public events when the draft Electronic Signatures Law was completed to explain its purpose. Research on effective outreach tools may be beneficial for helping policymakers in other economies to create effective messaging in their own economies.
2. Standards adoption – In the interest of eventual region-wide integration, it is beneficial for all economies to embrace the ISO20022 standard. But this is not an easy transition to make for all economies and technical support may be needed. It may be beneficial for APEC to work on developing guidelines toward this end, or to hold workshops with standards bodies and the APEC Business Advisory Council (ABAC) to discuss the transition process.
3. Cross border cooperation – The most natural fit for APEC is to help promote cross-border cooperation and provide an avenue for experience sharing among economies. Both the case studies on China and Chinese Taipei noted the role that APEC can play in this regard as a regional forum. Specifically on payments, case study research on successful integration examples in APEC and beyond may be beneficial, and workshops that bring together central bank representatives to discuss the process and requirements for agreements would also be a valuable support mechanism.

5.2 FOCUS AREA B: OPENNESS AND CROSS-BORDER ISSUES

OVERVIEW

As digital trade becomes an increasingly important component of an economy's imports and exports—including trade in products that are open to digitalization, such as printed materials, and services that are delivered digitally, such as software—there are a range of challenges to be overcome.

Firstly, high costs related to logistics and compliance are some of the key issues limiting Micro, Small and Medium Enterprises' (MSMEs) ability to navigate cross-border e-commerce. The harmonization of regulations and adoption of internationally-recognized industry standards and best practices can help break down some of these trade barriers, but they may not be commonly understood by and therefore benefit all businesses, especially MSMEs. Membership in the APEC's Cross-Border Privacy Rules (CBPR) system, for example, may not translate into a large take-up if MSMEs find it too complex or too costly to register.

Secondly, a related issue is the need for clarity as to where liability rests when third parties are involved, which could include data processors, platform operators, or banks. This also includes the case of IP-enforcement for e-commerce platforms that may list—but not own or control—infringing content on their platforms.

Thirdly, there is a need to secure data portability and data-sharing arrangements to allow the e-commerce ecosystem to predict consumer purchases, optimize fraud detection, automate supply chains and streamline authentication processes.

Key Issues

Measures that APEC economies have taken to tackle the challenges mentioned above can be broadly categorized into three areas:

- **Cross-border data privacy:** measures taken to encourage the adoption of CBPR, especially by MSMEs, or otherwise promote or establish privacy safeguards when facilitating the cross-border exchange of data. Singapore's efforts to reduce the costs of data protection compliance and potential breaches through measures that facilitate secure data-sharing and cross-border data flows are set out within this case study.
- **Data exchange and portability:** measures taken to adopt international standards and application program interface (APIs) for data exchange between APEC and other economies, and for portability between vendors. Australia's data portability framework and the local conditions and priorities that informed its chosen approach are examined.
- **Policy innovation and adaptation:** measures taken to encourage more open and competitive digital markets. For example, the measures taken by the Philippines to adapt its approaches in IP enforcement through stakeholder cooperation.

CASE STUDIES

Australia

E-commerce and other digital businesses rely heavily on data to improve efficiency, personalize services, and ultimately maximize their profits. However, the ownership and analysis of this data is typically confined to the business and platforms that generate it. Some economies are setting up data portability schemes—which effectively allow users to transfer data they generated on one service to another—as a means to spur competition. Data portability is also being implemented on a sectoral basis with its most common form being open banking. Economies are taking various approaches to open banking that reflect their local needs, that are shaped by legal and technological elements. This section examines Australia's approach, and how it differs from other economies' due to the unique local premise that it was developed as part of the broader economy-wide consumer data right (CDR).

Competition Reform through Consumer Data Right (CDR) and Open Banking

Big data is being used in e-commerce to predict consumer purchases, optimize pricing, detect fraud and automate supply chains. In short, the ability to harness big data can help e-commerce players become more competitive. However, there are two constraints that e-commerce players may face in leveraging big data:

- Firstly, regulation may prevent the transfer of data across borders. This limits the ability of businesses to combine and analyze data sets that originate from different locations. Regulations that facilitate the secure transfer of data across borders addresses this.
- Secondly, MSMEs may not have access to sufficient data to reap the benefits of big data and analytics. As big data analytics and machine-learning technologies produce more accurate outcomes when they are fed large data sets, even with access to the same technology, smaller e-commerce players that do not have access to the same data are unable to produce the same degree of granularity or accuracy. On the other hand, larger platforms with higher usage generate more data. Vendors, advertisers and consumers may be inclined to gravitate towards larger players that can effectively turn these network externalities into greater value.[643]

To address this second issue, economies are increasingly looking to data portability as a means to increase data sharing, promote interoperability, customer mobility and ultimately boost competition.[644] Data portability would require that consumer data generated by one business or on one platform can be shared or transferred easily and securely to another. However, for data portability to be effective, the use of interoperable standards needs to be baked in. This not only makes it easier for new entrants to reuse existing data, but also lowers their costs of doing so.

Box 5.3: Definition and Characteristics of Standards

The International Organization for Standardization (ISO) defines a standard as a "document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context."[645]

Standards can be either mandatory or voluntary, and can be issued by either a public or a private body. While divergent standards can increase trade costs, harmonization through the use of internationally accepted standards reduces trade costs by standardizing processes and compliance.[646] International standards are typically developed in a transparent, consensus-based environment that includes a range of stakeholders. Stakeholders may include technical, legal, regulatory, social, cultural, finance and economic experts participating from related industry, government, and civil society. Because of the range of participants and levels of

[643] APEC, 'Competition Policy for Regulating Online Platforms in the APEC Region', 2019, https://www.apec.org/Publications/2019/08/Competition-Policy-for-Regulating-Online-Platforms-in-the-APEC-Region.

[644] APEC, 'APEC Economic Policy Report', 2019, https://www.apec.org/Publications/2019/11/2019-APEC-Economic-Policy-Report.

[645] International Organization for Standardization, 'Standardization and related activities – General vocabulary', 2004, https://isotc.iso.org/livelink/livelink/fetch/2000/2122/4230450/8389141/ISO_IEC_Guide_2_2004_%28Multilingual%29_-_Standardization_and_related_activities_--_General_vocabulary.pdf?nodeid=8387841&vernum=-2.

[646] APEC PSU, 'Developing Indicators to Assess the Strength of Standards and Conformance (S&C) Infrastructure in APEC', 2018, https://www.apec.org/Publications/2018/04/Developing-Indicators-to-Assess-the-Strength-of-Standards-and-Conformance-Infrastructure-in-APEC.

expertise of those participating, the standard-setting process (as compared to the development of regulations) is able to more quickly respond to changing technological, business and regulatory conditions.

This characteristic is especially important in the context of e-commerce given the pace at which technologies that underpin business models and the ecosystem are developing. Standards are therefore assuming an increasingly significant role in providing governments and industry with a more flexible means to adapt to the evolving digital trade environment.

In Australia, the Consumer Data Right (CDR) was created with this exact objective.[647] In 2017, the Productivity Commission (PC) launched an Inquiry into Data Availability and Use to address recommendations from a 2014 Financial System Inquiry[648] and a 2015 Competition Policy Review[649] that the government should review the costs of benefits of increasing the availability and use of data, and consider ways to improve individuals' access to data for greater consumer choice.

The 2017 PC Inquiry highlighted gaps and barriers to improve public data sharing, including over 500 secrecy provisions restricting the sharing of public sector data.[650] The government responded by announcing a suite of reforms aimed at balancing privacy and security concerns with the benefits of releasing and sharing data, which included the establishment of an Office of the National Data Commissioner (ONDC), and the creation of the CDR. Introduced primarily through changes to the Competition and Consumer Act 2010, which were passed in August 2019,[651] the CDR regime was envisioned to be "a new competition and consumer measure to allow consumers to harness and have greater control over their data" and created a framework for the disclosure of two types of data: i) standardized product data; and ii) customer data.

While the implementation of the CDR was led by the Treasury, the governance of the CDR involved a cross-sectoral undertaking across multiple government agencies and public-private groups. Together with the ONDC, a new National Data Advisory Council, which comprises members across government, business and civil society, was also created to advise the ONDC on ethical data use, technical best practices and industry and international developments, in

[647] Australian Competition and Consumer Commission (ACCC), Consumer Data Right (CDR), https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0.

[648] Australian Treasury, 'Financial System Inquiry Final Report', 2014, https://treasury.gov.au/publication/c2014-fsi-final-report.

[649] Australian Treasury, 'Competition Policy Review – Final Report', 2015, https://treasury.gov.au/publication/p2015-cpr-final-report.

[650] Australian Government Productivity Commission, 'Data Availability and Use', 2017, https://www.pc.gov.au/inquiries/completed/data-access#report.

[651] Parliament of Australia, 'Treasury Laws Amendment (Consumer Data Right) Bill 2019', 2019, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fbills%2Fr6370_aspassed%2F0000%22;rec=0.

order to help the ONDC "find the right balance between the sharing and release of data and ensuring the protection or privacy and confidentiality".[652] In addition, Australia's national science agency, the Commonwealth Scientific and Industrial Research Organization's (CSIRO) data and digital research unit, Data61, was named the Data Standards Body (DSB) and oversaw the development of CDR standards (see Box 5.4). In the process of doing so, it undertook stakeholder surveys and worked closely with the Australian Competition and Consumer Commission (ACCC) and the privacy regulator, the Office of the Australian Information Commissioner (OAIC), which were tasked with assuming complementary enforcement roles in the regulation of the CDR:[653]

- OAIC with the primary responsibility of handling consumer complaints from individuals;
- ACCC with responsibility for ensuring that the CDR supports the competition and consumer outcomes it was intended for, and is also responsible for the accreditation of data recipients.

In October 2020, it was announced that the Treasury, as leading implementer of the CDR, would take over the rule making functions and sectoral assessments previously assigned to the ACCC, as well as the hosting of the DSB from the CSIRO.[654] This change consolidates some of the regulatory functions around CDR, reflecting industry feedback that fragmented regulatory oversight had resulted in "ongoing ambiguity between the rules and technical data standards", and that a consolidation of regulatory functions would streamline the rule-making process, while increasing regulatory accountability, clarity and effectiveness.[655]

---

[652] Office of the National Data Commissioner, 'National Data Advisory Council', https://www.datacommissioner.gov.au/about/advisory-council#:~:text=The%20National%20Data%20Advisory%20Council,and%20industry%20and%20international%20developments.&text=During%20its%20first%20year%2C%20the,Data%20Sharing%20and%20Release%20legislation.

[653] Consumer Data Standards Program, 'Consultations', https://consumerdatastandards.gov.au/standards/consultations/.

[654] Australian Government (2020) Budget 2020-21: Budget Documents, https://budget.gov.au/2020-21/content/documents.htm; The Mandarin (2020) Budget 2020: public service commitments and funding requests, https://www.themandarin.com.au/141467-budget-2020-funding/

[655] The Senate (2020) Select Committee on Financial Technology and Regulatory Technology – Interim report, https://parlinfo.aph.gov.au/parlInfo/download/committees/reportsen/024366/toc_pdf/SelectCommitteeonFinancialTechnologyandRegulatoryTechnology.pdf;fileType=application%2Fpdf

Box 5.4: CDR Standards

In principle, open data and data portability should place fintech start-ups and MSMEs in a better competitive position, as it grants them access to bank-held data that can help them better understand consumer trends and develop products based on that understanding. These data-driven insights can translate to developments in e-payments, an essential part of the e-commerce ecosystem. Access to customer data also makes it easier for consumers to switch bank accounts, credit card providers and so on, creating more opportunities for smaller and newer competitors with innovative products to gain market share. However, these outcomes require the use of common standards that allow data to be seamlessly ported from one system to another.

Australia's CDR is underpinned by common data standards known as the Consumer Data Standards (CDS).[656] The CDS comprises technical standards, such as data format, transfer and security, and consumer experience (CX) standards that shape consent flows, language and accessibility. In a process that was intentionally designed to be transparent and conducive for developing standards that would be implementable by industry, the DSB ran a series of working groups and consultations with industry, which were all carried out in an inclusive and transparent manner using the collaborative software development platform GitHub,[657] and received guidance from a well-balanced advisory committee that comprised both banks and fintech groups (the key stakeholders involved in the first application of CDR, Open Banking).[658] As a result of such efforts, both technical and CX standards have been developed in reference to international best practices, including:

- Following advice from the Open Banking review,[659] the DSB has looked to the UK's Consumer Experience (CX) Guidelines[660] in the creation of its CDR CX standards.[661]
- The use of open Application Programming Interface (API) standards is one of the principles that formed the basis of the CDS.[662] To help lower implementation costs and leverage well-established security practices by the banking sector, the CDS uses open industry standards where possible, such as the Financial-Grade API (FAPI)[663] and UK Open Banking.[664] FAPI incorporates industry open standards OpenID Connect and OAuth 2.0, which standardize authentication and authorization protocols for open APIs, and also formed the security foundation of the UK's Open Banking protocols.

[656] Consumer Data Standards Program, 'Consumer Data Standards', 2020, https://consumerdatastandardsaustralia.github.io/standards/#principles.

[657] TRPC Interview (26 August 2020) Victoria Richardson, Chief Strategy Officer, Australian Payments Network.

[658] CSIRO, Advisory Committee for the Data Standards Body announced, 2018, https://www.csiro.au/en/News/News-releases/2018/Advisory-Committee-for-the-Data-Standards-Body-announced.

The first sector targeted by the CDR was the banking sector, where its implementation is also known as Open Banking. Retail banking customers are usually only able to view their data through their bank's platform, which makes it difficult for them to share that data with other businesses and platforms. Moreover, only limited data access was given to corporate customers through Application Programming Interfaces (APIs).[665] As Australia's four largest banks collectively control more than 90 percent market share of Australia's financial industry,[666] fintech companies were relying on less effective and more resource-intensive 'screen scraping' to collect financial data.

The first phase of opening up consumer data, which was rolled out on 1 July 2020, was therefore to require the four major banks to make consumer data relating to credit and debit card, deposit accounts and transaction accounts available to accredited data recipients (see Box 5.7). Noting the sensitivities in sharing financial personal data and likelihood of consumer concerns, the ACCC at the outset stated "maintaining security and privacy are top priorities"[667] and as such is responsible for accrediting data recipients (e.g., ensuring that the businesses part of the system are able to receive and manage data securely in line with CDR system rules and safeguards).[668] In principle, open data and data portability should place fintech start-ups and MSMEs in a better competitive position, as it grants them access to bank-held data that can help them better understand consumer trends and develop products based on that understanding. These data-driven insights can translate to developments in e-payments, an essential part of the e-commerce ecosystem.

The ACCC's decision to have the CDR obligation first applied to the economy's four major banks was also made to reduce the burden of new data portability obligations on smaller organizations, which would have a chance to first learn from their larger counterparts' experience in opening up APIs.[669]

---

[659] Australian Government Treasury, 'Review into Open Banking in Australia', 2018, https://treasury.gov.au/consultation/c2018-t247313.

[660] Open Banking Limited, 'Open Banking Customer Experience Guidelines', 2018, https://www.openbanking.org.uk/wp-content/uploads/Customer-Experience-Guidelines.pdf.

[661] Consumer Data Standards Program, 'Consumer Experience Standards', 2020, https://consumerdatastandards.gov.au/wp-content/uploads/2020/08/CX-Standards_v1.4.0.pdf.

[662] Consumer Data Standards Program, 'Consumer Data Standards', 2020, https://consumerdatastandardsaustralia.github.io/standards/#principles.

[663] OpenID, 'Financial-grade API (FAPI) WG', 2019, https://openid.net/wg/fapi/.

[664] Fortian, 'Consumer Data Right Security Review', 2019, https://consumerdatastandards.gov.au/wp-content/uploads/2019/07/Consumer_Data_Right_Security_Review_Final.pdf.

[665] An Application Programming Interface (API) is a set of functions and procedures that enables programmers or app developers to access data and features of other applications, services, or operating systems. API Friends (2019), What is an API?, https://apifriends.com/api-management/what-is-an-api/.

[666] Iisi, 'How will Open Banking impact payments?', 2019, https://ipsi.com.au/how-will-open-banking-impact-payments/.

[667] ACCC, 'Consumer Data Right goes live for data sharing', 2020, https://www.accc.gov.au/media-release/consumer-data-right-goes-live-for-data-sharing.

[668] OAIC, 'CDR participants', 2020 , https://www.oaic.gov.au/consumer-data-right/cdr-participants/

[669] iTnews, 'Consumer Data Right for banking goes live', 2020 , https://www.itnews.com.au/news/consumer-data-right-for-banking-goes-live-549932

An important distinguishing factor between the CDR data-sharing regime and other open banking initiatives, is that the CDR has the ultimate goal of cross-sectoral interoperability where customers will be able to request data from a company in one sector to provide that data to a company in a different sector. Because of this foundation and objective, Australia's approach towards open banking through the CDR framework differs from other economies' in a few ways. For example, it not only applies to Australian banks, but all Authorized Deposit-taking Institutions, which include building societies and credit unions. It is also currently read-only, which means that customers can share their data, but not the operation of the accounts generating that data (see Box 5.5).

Box 5.5: Australia's Read-Only Access

Australia's open banking implementation has also been shaped by its prioritization of security over speed. For example, efforts to address concerns over data testing and security resulted in Australia's open banking reforms being delayed by six months, with the ACCC finalizing its CDR rules in February 2020.[670] Unlike other APEC economies—such as Hong Kong, China; Japan; Mexico; Singapore; and the United States—which included payments initiation in their open banking regimes, Australia's decision to have CDR data be (initially) read-only means that its open banking approach does not directly facilitate e-payments.[671] This decision stems from its 2017 Open Banking Review, which notes that customers with write access could become targeted by cyber-criminals, hence increasing security risks. It recommends the success of 'read access' should be evaluated first to ensure that there is enough trust in open banking before write access reforms are made.[672] The implication of having open banking data be limited to read-only formats means that the most significant benefit of open banking to e-commerce—for payment initiation where through integration of APIs bank accounts can be used directly [673] by e-commerce websites to satisfy transactions—will not be available to Australia in the short term.[674]

With a framework in place, the next hurdle for the CDR will be in proving its operational effectiveness, which will be measured by its impact on innovation and competition. Despite the regime still being in its infancy, the Treasury in January 2020 announced a new inquiry into the CDR to examine how the CDR regime can be improved to further boost innovation and

[670] Fintech Futures, 'Regional Australia Bank approves first Aussie open banking loan', 2020, https://www.fintechfutures.com/2020/07/regional-australia-bank-approves-first-aussie-open-banking-loan/

[671] The Paypers, 'Exclusive interview with Scott Farrell on Open Banking in Australia', 2019, https://thepaypers.com/interviews/exclusive-interview-with-scott-farrell-on-open-banking-in-australia--1239651

[672] Australian Government 'Open Banking – customers, choice, convenience, confidence', 2017, https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-_For-web-1.pdf

[673] Currently, merchants that appear to provide direct payment services on their websites actually rely on intermediaries such as electronic payment providers, that connect with credit card companies that in turn charge the transaction to customers' bank accounts. Write access has the potential to eliminate the need for such intermediaries, and thus reduce the costs of payments.

[674] PaymentsSource, 'Inside BBVA's flirtation with e-commerce and open banking', 2020, https://www.paymentssource.com/news/inside-bbvas-flirtation-with-e-commerce-and-open-banking

competition. One aspect of this inquiry was on the expansion of the CDR to include write access services for payments initiation.[675] An option under consideration is to align CDR with the economy's New Payments Platform (NPP), which has adopted an API Framework defining the key technical approach and mandatory data attributes for NPP APIs aligned with ISO 20022 standards.[676] As Australia expects the CDR to become an export driver (see Box 5.6), this alignment could bring Australia one step closer to establishing an internationally interoperable data portability system firstly by facilitating cross-border payment initiation. However, the government will also pay close attention to concurrent developments on the NPP, which has a roadmap for participating financial institutions to implement third-party payment initiation capabilities by December 2021.[677] This will be a consideration when the government determines whether it is a necessity to mandate third-party payment initiation through the CDR scheme, or if the benefits of write-access can be achieved through voluntary participation in the NPP.

Box 5.6: CDR as an Export Driver

Australia believes that being front runner in the development of CDR and data standards could place it in an advantageous position to align and facilitate data movements between other economies.[678] In the short term, Australia believes this could boost its export of fintech services, for example, which is a key component of the recently-signed Digital Economy Agreement (DEA) between Australia and Singapore. The DEA, which is an update of the Singapore-Australia Free Trade Agreement (FTA), saw the two economies specifically make new commitments to creating compatible e-payment frameworks based on international standards.[679] Moreover, a recently-launched public consultation by the New Zealand's Ministry of Business, Innovation and Employment (MBIE) seeking input on the possibility of developing a consumer data right for New Zealand recognizes the benefits of aligning the possible consumer data right with Australia's to increase access to finance for trans-Tasman trade activities.[680]

An export opportunity may be created if Singapore, New Zealand and/or other key trading partners decide to recognize and align their data portability regimes with Australia's CDR

[675] Australian Government, 'Inquiry into Future Directions for the Consumer Data Right', 2020, https://treasury.gov.au/sites/default/files/2020-03/200305_issues_paper.pdf

[676] ISO 20022 is the universal financial industry message scheme. ISO 20022, About ISO 20022, https://www.iso20022.org/about-iso-20022

[677] NPP Australia Limited, 'New Payments Platform Roadmap 2019', 2019, https://nppa.com.au/wp-content/uploads/2019/10/NPP-Roadmap-2019_28-Oct-2019-final.pdf

[678] The Australian Financial Review, ''Fintech bridge' to Singapore in the works to lift digital trade', 2020, https://www.afr.com/companies/financial-services/fintech-bridge-to-singapore-in-the-works-to-lift-the-export-of-services-20200610-p55147

[679] Australia Department of Foreign Affairs and Trade, Australia-Singapore Digital Economy Agreement, https://www.dfat.gov.au/trade/services-and-digital-trade/Pages/australia-and-singapore-digital-economy-agreement

[680] New Zealand Ministry of Business, Innovation and Employment, 'Options for establishing a consumer data right in New Zealand', 2020, https://www.mbie.govt.nz/have-your-say/options-for-establishing-a-consumer-data-right-in-new-zealand/

and adopt its data standards, allowing software that has been built by Australian companies based on these standards to be exported to those economies.

Another significant attribute of Australia's open banking regime is the principle of reciprocity, meaning that anyone accredited to receive data must also respond to requests to share data at their customer's request. Because of this reciprocity principle, unlike Japan and Singapore which allow banks and third-parties to negotiate terms and conditions through bilateral contracts or agreements, the charging of fees for data-sharing is not allowed at all in Australia.[681] This concept of reciprocity was introduced during the 2017 Open Banking Review with the objective of creating a more vibrant and dynamic competitive environment.[682]

Australia's reciprocity requirement is only possible because of its choice to adopt a legally-mandated regulatory regime, a contrast to New Zealand and Singapore's choice for industry-led, voluntary-based approach to open banking.[683] To ensure that such requirements can be enforced, the ACCC and OAIC jointly released the CDR Compliance and Enforcement policy in May 2020, which introduces penalties for non-compliance. The regulators plan to use a range of information sources and monitoring tools to assess compliance, and non-compliance could result in administrative notices, suspension or revocation of accreditation, or fines.[684]

[681] The Paypers, 'The Open Banking Report 2019 – Insights into the Global Open Banking Landscape', 2019, https://thepaypers.com/reports/download/the-open-banking-report-2019-insights-into-the-global-open-banking-landscape-2?cid=aae0ae95718a8acc402cd4da7d85c3c6.

[682] Australian Government, 'Open Banking – customers, choice, convenience, confidence', 2017, https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-_For-web-1.pdf.

[683] The Association of Banks in Singapore (ABS) and the Monetary Authority of Singapore (MAS) collaboratively developed an open API framework, the 'Finance-as-a-Service: API Playbook', while New Zealand industry body Payments NZ led the development of common payment-related APIs. The Association of Banks in Singapore (2016), ABS-MAS Financial World | Finance-as-a-Service: API PlayBook, https://abs.org.sg/docs/library/abs-api-playbook.pdf; Payments NZ, 'Our 'open banking' journey', https://www.apicentre.paymentsnz.co.nz/documents/251/Payments_NZ_paper_-_Our_open_banking_journey.pdf.

[684] ACCC/OAIC, 'ACCC/OAIC Compliance and Enforcement Policy for the Consumer Data Right', 2020, https://www.accc.gov.au/system/files/CDR%20-%20CE%20-%20Joint%20ACCC%20and%20OAIC%20compliance%20and%20enforcement%20policy%20-%208%20May%202020.pdf.

Box 5.7: Concept of an Accredited Data Recipient

While CDR seeks to equip customers with the ability to direct businesses that hold their data to transfer that data to a third party, this ability is limited by the fact that recipient third parties must be accredited. The ACCC's accreditation scheme currently offers a single, 'unrestricted' level of accreditation and, in order to participate in the CDR system, businesses go through a rigorous process to demonstrate compliance with security and privacy standards.

Fintech companies seeking to participate in the CDR system must first pass through a rigorous accreditation process which takes up to three months, and has been described by some as complex and onerous.[685]

Only one fintech company, Frollo, was accredited as a CDR data recipient when the scheme launched on 1 July.[686] Frollo admits that the accreditation process is challenging for fintech companies, especially small firms, as it requires the company to "think like a bank in terms of security and governance processes". Some difficulties Frollo faced were in finding an auditor to assist with the accreditation process, and a 300 percent increase in insurance costs.[687] Insurance cover that is commensurate with the risk of handling CDR data and strict information security control requirements are some key conditions for 'unrestricted' accreditation.[688]

For the average fintech start-up, the high compliance cost of participating in the CDR may be prohibitive. Indeed, FinTech Australia estimated costs of between AUD50,000 to AUD100,000 (USD36,304 to USD722,607) to become an accredited data recipient.[689] This calls for flexibility to the regime so more start-ups can access its advantages.

As noted in an interview, it is still far too early in the CDR rollout to judge the success of the scheme.[690] But this has not stopped the ACCC from already pursuing improvements to the CDR that take on board feedback from industry's experience so far. For example:

- Treasury is planning to launch a **Conformance Test Suite** in November, which is expected reduce the costs and time for prospective participants by semi-automating the process of testing system security and compliance.
- Following feedback from fintechs that a tiered approach to accreditation is what would make the CDR scheme more accessible and financially viable for data recipients, the ACCC is consulting **on adopting such a tiered approach** in order to improve the ability for data recipients. Australian Payments Network noted that the decision to first set a high security standard for accreditation before introducing a more complex tiered model would allow observations and a better understanding of risks to inform a more granular management of security risk at each tier.[691]
- To further streamline the cost and time to participate in the CDR regime the ACCC is also consulting on **amending rules to allow data recipients to outsource** the

establishment and maintenance of CDR-compliant systems to third-party service providers.[692]

Conclusion

Australia pursued the development of an economy-wide CDR with the objective of increasing the availability and usage of data as a competition and consumer measure. This not only entailed regulatory reform, but the establishment of new data authorities and collaboration between multiple regulators that oversee different aspects of the regime. Importantly, the CDR was, and continues to be, heavily shaped by industry feedback, which was recognized from the beginning as necessary to ensure it would be fit for practical implementation. To this goal, Australian regulators have sought to leverage international best practices in the development of CDR standards in order to help reduce compliance costs for implementing organizations.

Australia's approach to open banking, by being part of the broader goal of the CDR for cross-sectoral interoperability, has resulted in decisions that differed from other economies' on two fronts: (i) enforcement of a legal reciprocity requirement; and (ii) a lack of prioritization for payment-initiation.

The Philippines

The rise in online piracy and counterfeiting under the anonymity provided by the Internet, coupled with the increasing use of marketplace and social media platforms for purchases, has resulted in debate around the role of intermediaries and the need for new regulatory tools to strengthen IP enforcement while, at the same time, supporting sustainable e-commerce growth. However, with no clear set of global guidelines, economies have taken different approaches towards tackling IP infringement. This section explores the measures taken by the Philippines, specifically the Intellectual Property Office of the Philippines (IPOPHL), to adapt its

[685] InnovationAus.com, 'Open banking's majestically slow start', 2020, https://www.innovationaus.com/open-bankings-majestically-slow-start/.
[686] Consumer Data Right, 'Current providers', 2020, https://www.cdr.gov.au/find-a-provider.
[687] InnovationAus.com, 'Open banking's majestically slow start', 2020, https://www.innovationaus.com/open-bankings-majestically-slow-start/.
[688] Australian Competition and Consumer Commission, 'Finalised CDR accreditation guidelines', 2020, https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0/finalised-cdr-accreditation-guidelines.
[689] Senate Inquiry into Financial Technology and Regulatory Technology, 'FinTech Australia Submission', 2019, https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Financial_Technology_and_Regulatory_Technology/FinancialRegulatoryTech/Submissions.
[690] TRPC Interview (26 August 2020) Victoria Richardson, Chief Strategy Officer, Australian Payments Network.
[691] TRPC Interview (26 August 2020) Victoria Richardson, Chief Strategy Officer, Australian Payments Network.
[692] Australian Competition and Consumer Commission, 'ACCC consultation on facilitating participation of intermediaries in the CDR regime', 2019, https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0/accc-consultation-on-facilitating-participation-of-intermediaries-in-the-cdr-regime.

approaches in IP enforcement to the e-commerce environment through intensive stakeholder consultation.

Strengthening Online IPR Enforcement and Addressing Intermediary Liability

The protection of IPRs in e-commerce markets is vital for consumer protection and fair competition as IPRs safeguard the value and reputation of branded goods and services offered online. Online IPRs infringement can involve the illegal sale and distribution of pirated or counterfeit goods[693] and services online. Further, infringers may use domain names that resemble another company's website or brand name to facilitate such sales.[694] E-commerce has therefore added a new dimension to IPRs enforcement as it requires that the IPRs-enforcing authority cooperate with relevant public and private stakeholders, such as network service providers and marketplace operators, who have the respective abilities to remove access to the infringing websites or products.

Additionally, because IPRs are generally awarded and enforced on a jurisdictional basis, firms may seek registration of IPRs for assurance of due recourse over infringement. In some cases, this not only creates a cost and administrative burden on cross-border e-commerce but, after a long and costly process of getting IPRs registered and approved in another jurisdiction, weak enforcement mechanisms and lengthy judicial processes may disincentive companies, especially MSMEs, from engaging in cross-border sales. Strengthening IPRs enforcement and advancing towards cross-border consistency is therefore equally important in lowering IPRs-related barriers to e-commerce.

The Philippines has an enforceable IPRs legal framework. The economy's main IPRs legislation is Republic Act No. 8293 or the Intellectual Property Code of the Philippines (the 'IP Code'), which recognizes that an effective IPRs system is vital for developing domestic and creative activity, facilitating the transfer of technology, attracting foreign investment, and ensuring market access for products.[695] This IPRs legal framework is compliant with international standards, facilitated the Philippines' accession to the World Intellectual Property Organization (WIPO)'s Copyright Treaty (WCT)[696], its Performance and Phonograms Treaty (WPPT)[697]; as well as the World Trade Organization's (WTO) Agreement on Trade Related Aspects of Intellectual Property rights (TRIPS Agreement).[698] However, gaps in the Philippines'

[693] Branded goods are usually protected, among others, by copyrights and/or trademarks and counterfeits may therefore violate one or more of these IP rights.

[694] While a domain name itself is not protected by IP rights, it may include words such as brand names which have been trademarked.

[695] IPOPHL, Intellectual Property Code of the Philippines [Republic Act No. 8293, passed on 6 June 1997, 2015 Edition - The Intellectual Property Code as amended by R.A.s 9150, 9502 and 10372], https://boi.gov.ph/wp-content/uploads/2018/02/RA-8293.pdf.

[696] WIPO, 'WIPO Copyright Treaty', 1996, https://www.wipo.int/treaties/en/ip/wct/.

[697] WIPO, 'WIPO Performances and Phonograms Treaty', 1996, https://www.wipo.int/treaties/en/ip/wppt/.

[698] WTO, 'Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement)', 1995, https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm.

IPRs framework means that the IPOPHL's enforcement powers in the online sphere are limited. The IPOPHL's enforcement rules[699] have not been revised since its implementation in 2013 and are not readily applicable to e-commerce.[700] Currently, while the rights holder is able to request a take-down of IPR-infringing websites or product listings, competent authorities have no power to oblige the platform or ISP to act on such a request.[701] IPOPHL is addressing these limitations through a series of measures.

A. Coordinated approach to IPR enforcement measures

Firstly, the IPOPHL is updating rules to expand its purview of IPRs enforcement and enhancing cooperation with other agencies. Noting that existing rules for IPRs enforcement do not explicitly apply to IPRs-infringing activities conducted in the online space, the IPOPHL Enforcement Office (IEO) pushed for the revision of its 'Rules and Regulations in the Exercise of Enforcement Functions and Visitorial Power' to boost the enforcement capabilities of the agency.[702] According to the IEO, the revision would allow it to issue a warning notice and enforcement order to the platform for the take-down of any IPRs-infringing products listed on its website. According to the proposed revision, an enforcement order could involve the "permanent take down, blocking, and removal of the infringing online sites or accounts; a cease and desist order; an order to remove counterfeit and pirated goods from digital and/or electronic platforms or physical establishments."[703] Should the violating seller resist the enforcement order, the proposed revisions will also allow the IEO to work with the DTI or other relevant authority to cancel the seller's business permit.

This can potentially strengthen IPRs enforcement, as such processes were previously only granted to the Philippine National Police, the National Bureau of Investigation, and the Bureau of Customs and the Optical Media Board, all of which have different interests and limited purview.[704] The IPOPHL has also worked with the DTI to streamline and reduce overlap in enforcement functions, as while the IPOPHL was responsible for addressing complaints against the infringement of IPRs, the responsibility for fake and counterfeit goods typically fell under the purview of the DTI.[705] The revised rules also means that, when implemented, the National

[699] IPOPHL, 'Rules and Regulations in the Exercise of Enforcement Functions and Visitorial Power of the Intellectual Property Office, and Creating Thereby and Intellectual Property Rights (IPR) Enforcement Office', 2013, https://drive.google.com/file/d/1uuPN9KxMuWLwiB1bOR5zptuWQbzV1WI6/view.

[700] Manila Bulletin, 'IPOPHL to take down posts, websites violating intellectual property laws', 2020, https://mb.com.ph/2020/07/06/ipophl-to-take-down-posts-websites-violating-intellectual-property-laws/.

[701] Business World, 'Reports of counterfeiting, piracy spike in first half', 2020, https://www.bworldonline.com/reports-of-counterfeiting-piracy-spike-in-first-half/.

[702] IPOPHL, 'Revised Rules and Regulations in the Exercise of Enforcement Functions and Visitorial Power of the Intellectual Property Office', 2020, https://drive.google.com/file/d/1QDaGJsUlERfxkAkyn-wVvIecsEUM5ltf/view.

[703] IPOPHL, 'Revised Rules and Regulations in the Exercise of Enforcement Functions and Visitorial Power of the Intellectual Property Office', 2020, https://drive.google.com/file/d/1QDaGJsUlERfxkAkyn-wVvIecsEUM5ltf/view.

[704] Competition and Consumer Commission Singapore, 'Handbook on Competition & E-Commerce in ASEAN', 2017, https://www.cccs.gov.sg/resources/publications/other-publications/asean-ecommerce-handbook.

[705] IPOPHL, 'IPOPHL and E-commerce Players Tackle How to Better Protect IP Rights Online', 2019, https://www.ipophil.gov.ph/news/ipophl-and-e-commerce-players-tackle-how-to-better-protect-ip-rights-online/.

Telecommunications Commission (NTC) will be bound to the IPOPHL's order to cut access to an IPRs violating site, greatly strengthening the enforcement capabilities of the IPOPHL.[706] This consolidation of enforcement powers could speed up the enforcement process since the NTC is usually confined to following court orders. In addition, it may also reduce regulatory risks for online intermediaries who, when multiple authorities are involved, often find themselves having to explain how their businesses work to different agencies who may have differing views on intermediaries, or risk being over-regulated by a regulator.[707]

B. Intermediary liability

Under the Electronic Commerce Act, Internet intermediaries that are neither aware nor receive direct financial benefit from an infringing activity are afforded protection from civil and criminal liability.[708] However, the Act adopts a narrow definition of such intermediaries[709] which means that these 'safe harbor' provisions have limited applicability to popular e-commerce platforms, such as online marketplaces and social media channels.[710] In 2018, the IPOPHL proposed amendments to the IP Code to require online platforms to assume responsibility of ensuring the genuineness of products listed on their platform,[711] and contemplated using mandatory registration of e-commerce platforms as a means to hold them accountable for listing counterfeit products.[712] This proposal stood to be problematic for e-commerce platforms—which are a form of intermediary connecting buyers and sellers online—as it meant that they would be legally responsible for counterfeit products that appeared on their platform, even though the counterfeits may have been uploaded by third-parties without their knowledge. For the e-commerce platform, it may not be feasible to filter through high volumes of content to accurately determine which are counterfeit. Moreover, trademark infringement (which is the more common type of IP infringement in counterfeits) presents more challenges than copyright infringement since unlike copyright infringement—which relies on identifying unauthorized copies that are either a close or exact match to the reference file—counterfeiters may even use images of genuine products in their product listings, making them

---

[706] IPOPHL, 'IPOPHL Updates Enforcement Rules to Add Teeth to Online Counterfeiting', Piracy Crackdown, https://www.ipophil.gov.ph/news/ipophl-updates-enforcement-rules-to-add-teeth-to-online-counterfeiting-piracy-crackdown/.

[707] TRPC Interview (14 August 2020) E-commerce company.

[708] The Philippines, 'Electronic Commerce Act of 2000 [Republic Act No. 8792]', 2000, https://dtiwebfiles.s3-ap-southeast-1.amazonaws.com/Laws+and+Policies/Related+Laws/RA8792+-+Electronic+Commerce+Act.pdf.

[709] Intermediaries that are protected by the Electronic Commerce Act of 2000, however, are limited to 'Service Providers' that provide: 1) on-line services or network access, or the operator of facilities thereof, including entities offering the transmission, routing, or providing of connections for online communications, digital or otherwise, between or among points specified by a user, of electronic documents of the user's choosing; or 2) the necessary technical means by which electronic documents of an originator may be stored and made accessible to a designated or undesignated third party.

[710] Arvin Kristopher Razon, 'Decoding the Role of the 'Gatekeepers of Cyberspace' in the Internet Economy: Analyzing the Legal Foundation of Intermediary Liability of Online Providers', 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3414058.

[711] PhilStar, 'IPOPHL wants power to shutdown sites infringing on IP rights', 2018, https://www.philstar.com/business/2018/12/03/1873617/ipophl-wants-power-shutdown-sites-infringing-ip-rights

[712] Manila Bulletin, 'Intellectual Property policy for e-commerce mulled', 2018, https://mb.com.ph/2018/12/02/intellectual-property-policy-for-e-commerce-mulled/.

difficult for automated systems, or even rights holders, to identify.[713] Attempting to do so could come at a cost to user choice and privacy, since intermediaries may decide to take preventive measures such as user surveillance and content censorship to avoid liability.

In 2019, IPOPHL conducted a focus group discussion with brand owners and the Philippines' largest online retail platforms (including Facebook, Lazada, Shopee and Zalora) to discuss how to more effectively respond to IP violation notices and pre-emptively intervene to preclude online access to counterfeit goods.[714] Through the discussions, IPOPHL learnt about the measures e-commerce platforms are already taking to address IPRs infringement on their platforms. For example, Lazada and Shoppee require sellers to undergo an incubation period, typically lasting three months, which familiarizes them with the laws and standard practices, including IP, for future compliance.

Through engagement and cooperation with e-commerce platforms on IPRs issues, the IPOPHL's 2020 proposed amendments to the Rules and Regulations in the Exercise of Enforcement Functions and Visitorial Power reflect a different take towards intermediary liability—as compared to its 2018 proposed amendments—by requiring the e-commerce platform to comply with 'notice-and-takedown' measures, but stops short at holding the online intermediary accountable for counterfeit products listed by third-parties.[715]

In addition, the IPOPHL in February 2020 organized a workshop to improve IPRs protection in e-commerce in collaboration with the UK Prosperity Fund, which was also attended by Facebook, Lazada, Shopee and Zalora. It is exploring the possibility of undertaking an MoU modelled after the 2016 Brussels 'MoU on the sale of counterfeit goods via the Internet',[716] which e-commerce platforms, including Facebook, are signatories. The MoU will create a uniform notice-and-takedown mechanism that can be used by e-commerce platforms in handling complaints from rights owners and taking down infringers' accounts, simplifying and expediting the process.[717] Coupled with the proposed revisions to enforcement rules, undertaking this MoU could help reduce enforcement costs for rights holders and increase effectiveness of the notice-and-takedown system.

---

[713] WIPO, 'Study on Approaches to Online Trademark Infringements', 2017, https://www.wipo.int/edocs/mdocs/enforcement/en/wipo_ace_12/wipo_ace_12_9_rev_2.pdf.

[714] U.S. Chamber International IP Index, 'Philippines', 2020, https://www.theglobalipcenter.com/wp-content/uploads/2020/01/Philippines.pdf.

[715] IPOPHL, 'Revised Rules and Regulations in the Exercise of Enforcement Functions and Visitorial Power of the Intellectual Property Office', 2020, https://drive.google.com/file/d/1QDaGJsUlERfxkAkyn-wVvIecsEUM5ltf/view.

[716] The original, non-binding MoU was concluded in 2011. A 2013 review that found that measuring the effects of the MoU was necessary, and the 2016 version of the MoU incorporates a set of key performance indicators (KPIs) to measure its effectiveness. Signatories of the 2016 MoU include Alibaba, Amazon, eBay and Facebook Marketplace.
European Commission, 'Memorandum of Understanding on the online sale of counterfeit goods', 2016, http://ec.europa.eu/DocsRoom/documents/18023/attachments/1/translations/.

[717] IPOPHL, 'IPOPHL helps build trust between IP rights owners and e-commerce players in anti-counterfeiting, piracy endeavor', 2020, https://www.ipophil.gov.ph/news/ipophl-helps-build-trust-between-ip-rights-owners-and-e-commerce-players-in-anti-counterfeiting-piracy-endeavor/.

However, while the Philippines' proposed adoption of the notice-and-takedown mechanism is a positive approach to IPRs enforcement against counterfeits that is in line with industry best practices, additional steps may be required to define and limit intermediary liability.

Box 5.8: Notice-and-takedown Approach

The US' 1998 Digital Millennium Copyright Act (DMCA) established the 'notice-and-takedown' approach where the copyright owner may send a notice of copyright infringement to an Internet intermediary.[718] The Internet intermediary must then 'expeditiously' disable access to, or remove, the content in question. Although notice and take-down practices were initially developed to combat copyright infringements, Internet intermediaries have since used them to help rights owners protect trademarks as well.[719]

This notice-and-takedown mechanism places the onus of the identification of infringing activity on the rights owner, not the e-commerce site. In the absence of clear global rules defining liability for online intermediaries, a notice-and-takedown system exemplifies a cooperative online IPRs enforcement mechanism, and has been adopted by different economies. E-commerce sites have also developed their own voluntary notice-and-takedown systems and processes, which can be used by IPRs holders to remove infringing content.[720] Without a notice-and-takedown, or similar, system, IPRs holders are forced to seek enforcement action through court procedures, which are not only expensive and time-consuming, but also ineffective against infringers operating under anonymity.

As it currently stands, the Philippines' proposed notice-and-takedown procedure does not appear to create the same 'safe harbor' conditions as the US' 1998 Digital Millennium Copyright Act (DMCA). Safe harbor provisions allow e-commerce platforms to take certain actions, such as having IP policies and responding in a timely manner to take-down notices, to protect themselves from the monetary liability arising from their users' infringement. As long as the e-commerce platform takes action to expeditiously remove or disable the content after learning about its existence, the e-commerce platform will be protected from legal liability arising from the existence of illegal content on its platform.

An e-commerce platform operating in the Philippines explains that addressing IPR in the economy is currently guided by the spirit of collaboration rather than an enforcement

[718] U.S. Copyright Office, 'The Digital Millennium Copyright Act of 1998', 1998, https://www.copyright.gov/legislation/dmca.pdf.

[719] WIPO, 'Study on Approaches to Online Trademark Infringements', 2017, https://www.wipo.int/edocs/mdocs/enforcement/en/wipo_ace_12/wipo_ace_12_9_rev_2.pdf.

[720] WIPO, 'Study on Approaches to Online Trademark Infringements', 2017, https://www.wipo.int/edocs/mdocs/enforcement/en/wipo_ace_12/wipo_ace_12_9_rev_2.pdf.

mechanism.[721] How this translates into practice is that although only IPR holders have the legal standing to request the take-down of IPR-infringing material, the IEO has entered into separate arrangement with online platforms to recognize a report from the IEO as a basis for take-down.[722] Nonetheless, the e-commerce platform notes that safe harbor provisions would still be much welcomed for business certainty.[723] This holds true across APEC economies, where a lack of clarity on intermediary liability and safe harbor provisions creates uncertainty for the e-commerce platform, and may result in a departure from the original objective of the notice-and-takedown system, which is to strike a balance between innovation and the free flow of information, and IPR enforcement. It is also worth noting that there is no consensus that the notice-and-takedown system is the best approach for determining intermediary liability, and APEC economies have adopted different systems that require intermediaries to go beyond the baseline 'notice-and-takedown' measures to qualify for safe harbor (see Box 5.9 for some examples).

Box 5.9: Alternative Approaches to Notice-and-takedown of Counterfeits

China has adopted 'notice-and-trackdown' measures which allow the disclosure of online counterfeit sellers' contact details for investigation and enforcement purposes.

- These measures oblige online intermediaries to "publicly condemn" the infringer, downgrade their trustworthiness rating, prohibit the infringer from selling certain products, and so on, to avoid liability. In addition, intermediaries are subject to additional duties including adopting technical measures to monitor IP infringements, conducting daily online monitoring and reporting to the authorities.[724]
- China's E-Commerce Law, which took effect on 1 January 2019, provides an economy-wide legal framework for intermediary liability in trademark infringement that further reinforces some of these expectations.[725]
- China has also worked with dominant e-commerce Alibaba which uses big data analytics and machine learning in an automated system that is taught to detect counterfeits. Once a counterfeit product is detected, the associated account information, shipping and return addresses and payment information is pulled and passed on to Chinese law enforcement authorities. This information is then used to support investigations and facilitate the law enforcement process.[726]

[721] TRPC Interview (14 August 2020) E-commerce company.
[722] TRPC Interview (24 August 2020) IPOPHL.
[723] TRPC Interview (14 August 2020) E-commerce company.
[724] Ministry of Commerce of the People's Republic of China, 'Further promoting the fight against infringement of intellectual property rights and systems in the field of online shopping Notice on the action of selling counterfeit and shoddy goods', 2011, http://www.mofcom.gov.cn/article/h/redht/201104/20110407512137.shtml.
[725] Lexology, 'China passes new e-commerce law – a "safe harbour" with Chinese characteristics', 2018, https://www.lexology.com/library/detail.aspx?g=266f8b18-da86-4247-aa41-c582e9c4a98a.
[726] Alizila, 'Alibaba, Brands Step up Cooperation on IPR Protection', 2018, https://www.alizila.com/alibaba-brands-step-up-cooperation-on-ipr-protection/.

Korea adopts a 'notice-and-staydown' approach, where intermediaries that are issued infringement notices are required to take measures to prevent the same infringing products from being listed again.

- Intermediary liability is assessed based on the implementation of such measures.[727]
- In September 2019, the Korean Intellectual Property Office (KIPO) and major e-commerce platforms including Naver and Kakao, signed a MoU to allow KIPO to more easily and quickly acquire information from the platform companies to aid its investigations into counterfeit goods being distributed online.[728]

As for the Philippines, the IPOPHL is pushing for the ratification of House Bill No. 6122 or the Internet Transactions Act, which would require online businesses to register with the DTI.[729] The IPOPHL argues that sellers on platforms such as Facebook are able to sell their products without having registered businesses and this leads to problems in IPRs enforcement as it becomes very difficult to trace these seller accounts.

By making it compulsory for seller accounts to be associated with a registered business (which is currently not a pre-requisite), the IPOPHL believes it will be able to take more effective enforcement action over infringers as it resolves the issue of easily being able to continue distributing infringing content by setting up new seller accounts even if accounts are blocked or taken down.[730] It also intends to seek assistance from the NTC in asking Facebook to take down illegal pages.[731] If passed into law, the bill may strengthen the Philippines' IP enforcement capabilities, but could prove challenging to operationalize and may result in the exclusion of legitimate cross-border e-commerce sellers if overseas vendors find it complex or costly to register with the domestic authority.

Conclusion

IPRs-related regulations may need to be updated to ensure a fair and competitive e-commerce environment. In the Philippines, the IPOPHL has leaned towards existing international practices when setting new rules to combat online IPRs infringers. Stakeholder discussions were crucial in shaping a balanced regulatory perception of e-commerce platforms and other intermediaries.

[727] WIPO, 'Study on Approaches to Online Trademark Infringements', 2017, https://www.wipo.int/edocs/mdocs/enforcement/en/wipo_ace_12/wipo_ace_12_9_rev_2.pdf.

[728] European Commission, 'Report on the protection and enforcement of intellectual property rights in third countries', 2020, https://trade.ec.europa.eu/doclib/docs/2020/january/tradoc_158561.pdf.

[729] The Philippines, 'House Bill No. 6122, An Act Protecting Consumers and merchants Engaged in Internet Transactions, Creating for This Purpose the Ecommerce Bureau and Appropriating Funds Therefor', 2020, http://www.congress.gov.ph/legisdocs/basic_18/HB06122.pdf.

[730] Philippine News Agency, 'IPOPHL pushes for registration of online sellers', 2019, https://www.pna.gov.ph/articles/1064833.

[731] Rouse, 'Facebook Marketplace and IP Infringement In the Philippines', 2019, https:/www.rouse.com/magazine/news/facebook-marketplace-and-ip-infringement-in-the-philippines/?tag=philippines.

However, to give further clarity to intermediary liability, the notice and take-down measures that the IPOPHL seeks to implement should form a pre-requisite for limited intermediary liability, i.e. by creating safe harbor conditions, which would reduce regulatory uncertainty for platform intermediaries. Moreover, an expectation of the timeframe required for intermediaries to act on take-down notices may also improve clarity and may also reduce the financial costs for IP rights owners as slow responses allow the infringer to continue to profit off infringing material.

Further, the Philippines is seeking to boost accountability and IP enforcement by proposing that e-commerce vendors be identified through their business registration numbers. While this will address the problem of re-emerging infringing material where sellers that have been banned can easily create a different account under user anonymity, the possible impact this may have on privacy and cross-border trade may need to be considered. The establishment of APEC-level best practices for online IPRs enforcement may be useful for the harmonization of regulatory approaches.

Singapore

This section examines the measures Singapore has taken to address underlying security concerns by using accountability measures to boost data protection standards, while ensuring that the economy's data protection framework remains interoperable with international frameworks, and supportive of cross-border data flows.

Promoting Secure Data Flows

Whilst limitations to cross-border data flows could effectively restrict e-commerce and other forms of trade, important considerations to the protection of in-transit data flows and personal data that lies in another jurisdiction are issues economies continue to grapple with. Some economies have pursued privacy reforms to address these issues (see Box 5.10).

Box 5.10: Recent Privacy Reforms Safeguard and Clarify Cross-border Data Flows

In June 2020, New Zealand passed a bill reforming the economy's privacy legislation. Effective from 1 December 2020, New Zealand's Privacy Act 2020 will replace the existing Privacy Act 1993.[732] The two key changes were the implementation of mandatory data breach reporting and strengthening of protections for cross-border data flows. The new law also clarified that it had extra-territorial application to foreign entities that carried out business in New Zealand.

[732] New Zealand Government Ministry of Justice, Privacy, https://www.justice.govt.nz/justice-sector-policy/key-initiatives/privacy/#:~:text=The%20Privacy%20Act%202020%20(the,role%20of%20the%20Privacy%20Coissioner.

The new Privacy Act requires that, for the disclosure of personal information to overseas recipients, the organization should first ensure that either consent from the individual has been received, or that the personal data would be protected by comparable privacy standards. Comparable safeguards can be achieved by either through contractual clauses, or by ensuring that recipients are located in jurisdictions that have been 'whitelisted' in regulations.

Significantly, the new rules for cross-border transfers only apply to *disclosures,* and not the storage and processing of personal data in overseas locations. This gives clarity to organizations that the rules do not apply to the transfer of data to organizations that only store or process personal data in overseas locations, such as cloud service providers (CSPs), and is important because it is a deliberate attempt to reduce restrictions to cross-border data flows.[733]

In the same month, a bill to amend Japan's Act on the Protection of Personal Information (APPI) was promulgated.[734] The bill, which came into effect in June 2020, seeks to broaden consumers' rights over their data, introduce the concept of pseudonymized data and mandatory data breach notifications, create additional restrictions to cross-border data transfers and establish new extraterritorial enforcement options.

The new APPI includes an update to the consent principle by requiring organizations to inform the data subjects it seeks consent for cross-border data transfers from of the details of the overseas third-party, including the data protection regulations and safeguards the third-party adopts. It should be noted that the UK, European Economic Area (EEA) members and APEC Cross-Border Privacy Rules (CBPR)-certified organizations are exempt from the consent requirement.

To further support secure cross-border data flows, Singapore recognized the need to create a strong foundation of data protection practices at a domestic level that can build a high level of consumer trust.[735] While cybersecurity and privacy regimes provide good policies and procedures for building trust, organizations may not implement them in practice. This led to the creation of the Data Protection Trust Mark (DPTM),[736] a voluntary enterprise-wide certification scheme developed by the Infocomm Media Development Authority of Singapore (IMDA) and adapted from the Personal Data Protection Act (PDPA)[737] and international

[733] New Zealand Privacy Commissioner, 'Privacy 2.0: Cross-border disclosures – introducing new privacy principle 12', 2020, https://privacy.org.nz/blog/privacy-2-0/.

[734] Personal Information Protection Commission of Japan, 'Promulgation of the Amendment Act of the Act on the Protection of Personal Information', 2020, https://www.ppc.go.jp/en/news/archives/2020/20200618/.

[735] Infocomm Media Development Authority of Singapore, 'DPTM Success Stories', 2020, https://www.imda.gov.sg/-/media/Imda/Files/Programme/DPTM/DPTM-Success-Stories-130820.pdf?la=en.

[736] The DPTM is a voluntary certification that businesses can apply for to demonstrate compliance with Singapore's PDPA. The DPTM seeks to increase the standard of data protection practices among Singapore organizations and promote consistency in data protection standards across different sectors. IMDA, Data Protection Trustmark Certification, https://www.imda.gov.sg/dptm.

[737] Singapore, 'Personal Data Protection Act 2012', 2012, https://sso.agc.gov.sg/Act/PDPA2012.

benchmarks and practices. While codes of conduct and certifications are both voluntary, certification (including seals and trust marks) involves third parties that certify and validate data protection standards. The use of trust marks for privacy is comparable to the use of regionally or globally recognized standards such as ISO/IEC 27001 to demonstrate cybersecurity adequacy.

Box 5.11: About ISO/IEC 27001

As outlined above, in order to accelerate digital trade availability and growth, international standards are often coming to play the role that regulation has traditionally played by: i) facilitating market access and participation; ii) reducing compliance costs; and iii) ensuring competition.

The ISO/IEC 27000 family of standards are often referenced and have become the foundational security standards that enable robust and consistent data protection and privacy measures, which increase community trust in all types of digital initiatives, driving adoption and use. For example, Singapore's Personal Data Protection Commission (PDPC) recently released guidelines on cloud services and data access requests.[738] In these guidelines, PDPC encourages organizations to ensure that the CSP they engage meets relevant industry standards (e.g., ISO/IEC 27001) or to obtain assurance from the CSP that all data centers/sub-processors in overseas locations comply with similar standards—highlighting the importance and recognition that ISO/IEC 27001 holds.

ISO/IEC 27001 is one out of more than a dozen information security management standards in the ISO 27000 family, and is one of the most commonly applied cybersecurity standards as it brings together all the essential terminology.[739] ISO/IEC 27001 specifies:

- The requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization.
- These requirements are generic and are intended to be applicable to all organizations, regardless of type, size or nature.[740]

[738] Singapore Personal Data Protection Commission (PDPC) Advisory Guidelines on the PDPA for Selected Topics, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Selected-Topics/Chapter-8-9-Oct-2019.pdf.

[739] ISO, 'ISO/IEC 27000 – key International Standard for information security revised', 2018 https://www.iso.org/news/ref2266.html.

[740] ISO, 'ISO/IEC 27000 – key International Standard for information security revised', 2018 https://www.iso.org/news/ref2266.html.

In contrast to more established codes of conduct, certification is a relatively new tool for demonstrating compliance in the data protection scene. The notion of certification was introduced in Article 43 of the EU's 2016 General Data Protection Regulation (GDPR)[741] as a means to demonstrate compliance and as legal ground to transfer personal data outside of the EU. In line with new trends around data protection, Singapore launched the DPTM in January 2019, shortly after the GDPR entered into force in May 2018,[742] and following a pilot scheme involving the recruitment of early adopters to test the robustness of the data protection framework and help fine-tune its certification controls and processes.

Amongst the requirements of the DPTM are principles based on international frameworks such as the EU's GDPR, the APEC Privacy Framework,[743] and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[744] This inclusion of elements of the APEC CBPR and Privacy Recognition for Processors (PRP)[745] systems' requirements in the DPTM scheme is what allowed the IMDA to integrate the two certifications' application and assessment processes, making it cheaper and easier for organizations to receive both certifications (see Box 5.12). Because of its alignment with international frameworks, despite being developed as a domestic certification, DPTM certification has proved to be an advantage to achieving cross-border privacy compliance since it demonstrates that the company's data protection policies are aligned with these international benchmarks and best practices.

[741] European Union, 'Regulation (EU) 2016/679 of the European Parliament and of the Council', 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

[742] Lee Soo Chye, Teo Yi Ting Jacqueline and Sheam Zenglin, 'Towards Codes and Certifications – The Protection of Personal Data in the Digital Age', 2019, https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/2019-personal-data-protection-digest.pdf.

[743] APEC, 'APEC Privacy Framework', 2015, https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)

[744] Infocomm Media Development Authority and Personal Data Protection Commission Singapore, 'IMDA and PDPC launch pilot for Data Protection Trustmark certification scheme', 2018, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/PDP-Seminar-2018/Media-Release---IMDA-and-PDPC-launch-DPTM-pilot-(250718).pdf.

[745] The CBPR, which applies to data controllers, is complemented by the APEC Privacy Recognition for Processors (PRP) System, a certification mechanism for data processors to demonstrate their ability to implement the data controller's privacy obligations.

Box 5.12: Singapore's APEC CBPR Participation Brings Practical Benefits for Businesses

In APEC, the APEC Privacy Framework and the Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) systems are flexible approaches towards standardizing data protection and enabling cross-border data flows[746] that can even help achieve interoperability between frameworks. For instance, the APEC CBPR can be used as a basis for organizations applying for the European Union (EU) Binding Corporate Rules (BCRs) [747] , [748] while the new United States-Canada-Mexico Agreement (USMCA) recognizes APEC CBPR as a "valid mechanism to facilitate cross-border information transfers while protecting personal information".[749]

Recognizing that fragmented global data flows regulatory landscape was making it challenging for companies to navigate and comply with the different data protection frameworks, and that the CBPR system was the only multilateral framework that allowed personal data to be transferred seamlessly with accountability in the APEC region,[750] Singapore in July 2017 submitted its Notice of Intent to participate in the APEC CBPR and PRP systems, which was approved in February 2018, making it the sixth economy to participate in the CBPR system and second economy to participate in the PRP system.[751]

In July 2019, IMDA was appointed as the economy's Accountability Agent responsible for ensuring organizations' privacy policies have been verified through independent third-party assessments before granting them CBPR and/or PRP certifications.[752] Since its appointment, the IMDA has conducted outreach programs and industry workshops in partnership with various Trade Associations and Chambers[753] to raise awareness of CBPR benefits. Through these programs and workshops, the IMDA learnt that there were three major obstacles inhibiting participation in CBPR certification: concerns with its costs and validity period, and low awareness of the certification system.[754]

With the full operationalization of the CBPR system, Singapore has been able to implement practical measures that reduce the costs for companies both directly (by reducing certification fees) and indirectly (by easing compliance requirements for cross-border data transfers). The IMDA streamlined its privacy certification process to allow businesses to apply for both the domestic DPTM and APEC CBPR certifications at the same time, through a one-time application fee of SGD500 (USD367).[755] Singapore has also put in place additional cost incentives for CBPR certification through the waiver of application fees for SMEs and grant support for certification assessment fees.[756]

In addition, the IMDA is also addressing companies' feedback that the current one-year validity of the CBPR certification is too short and yearly recertification may be onerous and require huge effort on their part. IMDA has acted on this and has provided feedback to APEC to look into extending the certification validity period.[757]

In terms of raising awareness, the IMDA realized that many companies had not heard of the CBPR until they attended its outreach sessions, and thus continues to work closely with Trade Associations and Chambers to raise awareness of the CBPR. The IMDA noted in an interview that Trade Associations and Chambers are willing to work with them because they first recognize the benefits of the CBPR certification and the value it brings to their members.[758]

To encourage further uptake, greater awareness may need to be built specifically around the available cost subsidies. IMDA notes that out of the five companies currently in the application process for CBPR certification, just one is an SME that qualified for the application fee waiver. However, none had applied for grant support to defray the other certification costs (e.g. assessment and consultancy fees).[759]

To address the challenge of privacy compliance in the cross-border transfer of data resulting from the absence of privacy harmonization, Singapore published PDPA guidelines that provide examples of specific measures organizations can take to ensure that their overseas transfers of personal data comply with the PDPA, such as by making sure that: (i) personal data is only transferred to overseas jurisdictions that have comparable data protection laws; or (ii) the recipient is legally bound by similar contractual standards; or (iii) all data centers and sub-processors that may handle the personal data are compliant with ISO/IEC 27001.

[746] Japan, for example, exempts CBPR-certified organizations from a consent requirement for cross-border data transfer.
[747] EU's BCRs allows organizations with a presence in the EU to transfer personal information from the EU to members of the same corporate group, located outside the EU.
[748] APEC PSU, 'Case Studies on Addressing Connectivity Challenges in APEC Economies', 2018, https://www.apec.org/Publications/2018/11/Case-Studies-on-Addressing-Connectivity-Challenges-in-APEC-Economies.
[749] USTR, 'Agreement between the United States of America, the United Mexican States and Canada', Chapter 19 Digital Trade, https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf.
[750] TRPC Interview (19 August 2020) Singapore Government.
[751] Ministry of Communications and Information Singapore, 'Singapore joins APEC Cross-Border Privacy Rules and Privacy Recognition for Processor Systems', 2018, https://www.mci.gov.sg/-/media/mcicorp/images/budget-workplan/cos-2018/factsheets/factsheet---singapore-joins-apec-cross-border-privacy-rules-and-privacy-recognition-for-processors-systems.ashx#:~:text=With%20approval%20from%20the%20APEC,the%20PRP%20system%20alongside%20USA.
[752] APEC, 'APEC Strengthens Trust with Data Protection System', 2019, https://www.apec.org/Press/News-Releases/2019/0723_IMDA.
[753] Singapore Business Federation, Trade Associations & Chambers, https://www.sbf.org.sg/membership/trade-associations-chambers.
[754] TRPC Interview (28 August 2020) Singapore Government.
[755] IMDA, APEC Cross Border Privacy Rules (CBPR) System, https://www.imda.gov.sg/programme-listing/Cross-Border-Privacy-Rules-Certification.
[756] According to the IMDA, eligible local enterprises can tap on Enterprise Singapore's Enterprise Development Grant to help defray the certification costs (e.g. assessment fee, consultancy). TRPC Interview (28 August 2020) Singapore Government.
[757] TRPC Interview (28 August 2020) Singapore Government.
[758] TRPC Interview (28 August 2020) Singapore Government.
[759] TRPC Interview (28 August 2020) Singapore Government.

By recognizing compliance with international standard ISO/IEC 27001 as suitable for personal data protection, the PDPA both acknowledges the suitability of international standards to secure cross-border data flows and saves certified overseas data processors the trouble of navigating the domestic framework. In June 2020, Singapore also gave the condition of "comparable data protection" much clarity when it amended its Personal Data Protection Regulations to recognize CBPR-certified overseas recipients of personal data as having comparable protection to domestic organizations legally bound by the PDPA.[760] Both these measures significantly reduce the compliance barriers to secure cross-border data transfers to make it easier for local organizations to transfer data to overseas recipients without meeting additional requirements.

Domestic and cross-border enforcement

To operationalize the DPTM and establish a clear financial incentive even for organizations not currently and actively conducting cross-border data transfers to seek DPTM certification, the Personal Data Protection Commission (PDPC) has suggested that an organization's DPTM certification status is a consideration factor when evaluating whether the organization's undertaking was acceptable and deciding whether or not to discharge enforcement action against data breaches.[761] Since it is well-understood that the financial penalties of a potential data breach will be much more costly than the DPTM certification fee, this has in no small part driven take-up, with 33 organizations having achieved DPTM certification as of 13 August 2020.[762]

In terms of cross-border enforcement, the CBPR system provides mechanisms for cross-border enforcement through the APEC Cross Border Privacy Enforcement Arrangement (CPEA), a multilateral arrangement for privacy enforcement authorities to voluntarily share information and provide assistance for cross-border data privacy enforcement, as well as the use of accountability agents, which have been appointed in three economies (including Singapore) thus far. Cooperation in cross-border enforcement can also be forged through negotiation with overseas data privacy authorities, and by joining international or regional privacy enforcement cooperation networks such as the Asia Pacific Privacy Authorities (APPA)[763] and the Global Privacy Enforcement Network (GPEN), which facilitate information-sharing between authorities in different economies for enforcement action. In addition to its membership in APPA and GPEN, Singapore is also exploring the enhancement of cross-border cooperation

[760] Personal Data Protection Commission Singapore, 'Singapore Now Recognises APEC CBPR and PRP Certifications Under PDPA', 2020, https://www.pdpc.gov.sg/news-and-events/announcements/2020/06/singapore-now-recognises-apec-cbpr-and-prp-certifications-under-pdpa.

[761] Wong Partnership, 'Changes to the Data Protection Regulatory Landscape', 2019, https://www.wongpartnership.com/upload/medias/KnowledgeInsight/document/9037/IPMTUpdate-ChangestotheDataProtectionRegulatoryLandscape.pdf.

[762] Infocomm Media Development Authority of Singapore, 'List of Data Protection Trustmark Certified Organisations (as of 13 Aug 2020)', 2020, https://www.imda.gov.sg/-/media/Imda/Files/Programme/DPTM/DPTM-Certified-Organisations-130820.pdf?la=en.

[763] Asia Pacific Privacy Authorities (APPA) About, https://www.appaforum.org/about/.

through trade agreements.[764] The Singapore-Australia Digital Economy Agreement (DEA),[765] for example, included a MoU with Australia to develop interoperable data transfer mechanisms and coordinate to jointly investigate cross-border incidents involving personal data.[766] Singapore has also signed a similar cross-border enforcement agreement with the Philippines.[767] These bilateral agreements and international frameworks are designed to facilitate law enforcement access to data across borders and define mechanisms for coordinated action.

Conclusion

Singapore's use of certifications such as DPTM, CBPR and ISO/IEC 27001, ensures accountability in the use of personal data, which is key to creating robust data protection practices. Singapore's approach to incentivizing take-up of privacy certification has been to streamline the process of achieving multiple certifications, and explicitly acknowledge privacy certification as a valid demonstration of legal compliance that reduces businesses' risk of enforcement action. It should be noted that this approach is underpinned by the alignment of Singapore's domestic privacy certification with international frameworks and best practices, which establish the harmonized baseline privacy standards that facilitate secure cross-border data flows.

Key Lessons

The approaches taken by Australia; the Philippines; and Singapore, highlight the following takeaways for APEC member economies, and the region, when engaging in and encouraging openness and cross-border e-commerce.

1. **Cross-agency collaboration and public-private cooperation** are equally important for the creation and implementation of balanced and effective e-commerce policies. Consultations with stakeholders are key to shaping regulatory approaches that are in-tune with business models/ applications and appropriate for achieving the intended regulatory outcomes. Consolidating related or overlapping functions, or creating a central e-commerce agency to oversee and coordinate may also be necessary for the effective implementation of e-commerce related reform.

[764] Personal Data Protection Commission of Singapore, 'Keynote Speech by Deputy Commissioner, Mr Yeong Zee Kin, at Data Interconnection and Security Development Summit, on Sunday, 5 January 2020, at Zhuhai, People's Republic of China', 2020, https://www.pdpc.gov.sg/news-and-events/press-room/2020/01/keynote-by-dy-commr-at-data-interconnection-and-security-development-summit-on-5-jan-2020-in-zhuhai.

[765] Ministry of Trade and Industry Singapore, 'Singapore-Australia Digital Economy Agreement (SADEA)', https://www.mti.gov.sg/Improving-Trade/Digital-Economy-Agreements/The-Singapore-Australia-Digital-Economy-Agreement.

[766] Personal Data Protection Commission of Singapore, 'Memorandum of Understanding Between OAIC and PDPC', 2020, https://www.pdpc.gov.sg/news-and-events/announcements/2020/03/memorandum-of-understanding-between-oaic-and-pdpc.

[767] National Privacy Commission of the Philippines, 'PH, Singapore sign MoU on Personal Data Protection', 2019, https://www.privacy.gov.ph/2019/09/ph-singapore-sign-mou-on-personal-data-protection/.

2. **The use of privacy certification such as trust marks to signal data protection adequacy** complements privacy regulation and enforcement frameworks and can even be used to incentivize compliance. Basing these off internationally-recognized baseline standards creates further opportunities for cross-border interoperability, as well as across certification schemes.
3. In order to foster competition in data-heavy industries, **competition reform through the introduction of data portability** may be required to allow consumers greater control over their information, better ability to compare products and services, and boost data transparency and competition between service providers. While differences in objectives, priorities and domestic circumstances shape how economies choose to implement their data portability schemes, industry standards should be used as a baseline to ensure that these differences do not hamper cross-border opportunities.
4. Economies should ensure that they take a **holistic approach to policymaking** to ensure that intended outcomes can be realized. For example, while data portability usually has competition and consumer-protection driven objectives, it needs to be accompanied by the development of interoperable data standards and robust privacy safeguards in order to be operationalized effectively. This not only requires inter-agency collaboration, but also private sector capacity-building and a concrete understanding and alignment with international frameworks and best practices.

5.3 FOCUS AREA C: CONSUMER PROTECTION AND PRIVACY ISSUES

OVERVIEW

Consumer Protection and Online Dispute Resolution (ODR)

Dispute resolution regarding e-commerce transactions between consumers and vendors, and between the platforms themselves constitute an essential aspect to e-commerce markets, as well as to the broader digital economy. For example, Online Dispute Resolution (ODR), an outgrowth of alternative dispute resolution (ADR),[768] provides an alternative to traditional legal proceedings via civil courts with regard to high-volume, low-value transactions between consumers and vendors.[769] The availability of ADR systems, such as ODR, could encourage more participation in e-commerce. In fact, in their WTO submissions regarding consumer protection, economies acknowledged the importance of establishing mechanisms to protect

[768] According to the Cornell University Legal Information Institute, "Alternative Dispute Resolution (ADR) refers to any means of settling disputes outside of the courtroom" and "typically includes early neutral evaluation, negotiation, conciliation, mediation, and arbitration." Tala Esmaili and Krystyna Blokhina Gilkis, 'Alternative Dispute Resolution', Cornell University Legal Information Institute, June 2017, [Online] Available at https://www.law.cornell.edu/wex/alternative_dispute_resolution [accessed: 24 August 2020].

[769] Woojong Kim, 'Critical Evaluation of the Online Dispute Resolution for Cross-Border Consumer Transaction Under E-Commerce', Social Science Research Network (SSRN), May 2016, Last accessed 24 August 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2853303.

consumers engaged in e-commerce and redress for fraudulent and deceptive commercial activities.

However, ODR is not a silver bullet. It faces costs and regulatory challenges, particularly for MSMEs planning to offer ODR themselves (vis-a-vis large platforms). In addition, language and cultural barriers, differences in consumer protection law, cost and enforcement challenges complicate the prospect of cross-border ODR. As a result, the use of ODR is not widespread for resolving disputes across APEC economies.[770] Understanding how ODR functions in some economies can provide useful learning points for those considering to establish one. The experiences of China, Japan and Mexico are elaborated below.

Privacy issues: Data Protection

Personal data protection regulations play an increasingly important role in e-commerce markets. On the one hand, data analytics can be used by businesses to better tailor offerings to potential customers, hence enhancing their browsing and shopping experience. Having accurate data pertaining to customers such as contact details and credit card numbers ready also make for more efficient and smoother transactions. On the other hand, the increasing dependency on data requires consumers' personal information to be protected and secured from hacking incidents and data leaks (among others). These events can significantly harm consumers and affect their trust. Furthermore, the significant adoption of digital tools as a result of COVID-19 are likely to increase the occurrence of such hacking and data leakage incidents.

At the level of APEC economies, various regulations to support public policy objectives such as ensuring better data protection and security are already in place. The case study on China's Regulation for Protecting Children's Personal Information discussed below provides some learning points.

CASE STUDIES

China

China's ecommerce market is one of the largest in the world and is expected to grow from 17 percent of total retail sales in 2017 to 25 percent by 2020.[771] As of 3Q 2019, its online retail market was found to total RMB7.32 trillion with online sales of physical goods valued at

[770] World Bank, 'Doing Business 2017: Equal Opportunity for All', World Bank Publications, October 2016, Last accessed 24 August 2020, https://www.doingbusiness.org/en/reports/global-reports/doing-business-2017.
[771] PwC, 'The continued momentum of e-commerce growth in China', Last accessed 15 October 2020, https://www.pwc.in/consulting/financial-services/fintech/fintech-insights/the-continued-momentum-of-e-commerce-growth-in-china.html.

RMB5.77 trillion. Within the first three quarters of 2019, market trends include[772]: 1) the increased participation of rural communities in e-commerce; 2) the growth of cross-border e-commerce, with retail imports increasing by 30 percent year-on-year; and 3) the increased integration of e-commerce and social media.

The e-commerce market can be expected to continue expanding considering that more than half of China's population have gained access to the internet (54.3 percent as of 2018)[773]. COVID-19 is likely to contribute towards a further increase in demand, as more consumers shift to online purchases. For instance, Meituan Dianping, China's biggest on-demand delivery services firm, clocked a net profit of RMB2.2 billion in the second quarter of 2020, an increase of more than 152 percent compared to the previous year.[774]

Consumer Protection and E-Commerce

A facilitative environment is needed for e-commerce to thrive. A critical contributing factor to the development of such an environment is having in place various laws/regulations, initiatives and mechanisms aimed at consumer protection. Although consumer protection is important both in the offline and online worlds, it has taken added significance for the latter because of the nature of e-commerce transactions (e.g., sellers and buyers located in different cities/towns, buyers not having the opportunity to physically assess the goods). Put simply, should disputes arise, there need to be clear laws/regulations specifying the rights and obligations of the various parties in the transactions. There should also be credible, efficient consumer protection mechanisms by which parties can resolve their disputes.

Related to the issue of consumer protection is the issue of data protection. While data can lead to a more enjoyable shopping experience (e.g., allow for targeted offering) and facilitate the transaction process (e.g., automated form filling), the illegal collection and transfer of personal data could lead to less desirable experiences (e.g., receiving unsolicited emails and phone calls from third parties). As such, having laws/regulations which pertain to data protection and privacy is an important component towards creating a facilitative e-commerce environment.

China has introduced many measures to improve consumer protection and data privacy in the economy. On consumer protection, for example, China has introduced a web-based economy-wide platform to deal with consumer complaints and issues pertaining to product quality[775].

---

[772] China, 'Head of Department of Electronic Commerce and Informatization of the Ministry of Commerce Comments on the Development of Online Retail Market in the First Three Quarters of 2019', Last updated 31 October 2019, http://english.mofcom.gov.cn/article/newsrelease/policyreleasing/201911/20191102910844.shtml.

[773] International Telecommunication Union Statistics – Percentage of individuals using the internet. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

[774] CNBC, 'China's e-commerce giants get a boost as consumers continue to shift online after coronavirus', Last accessed 15 October 2020, https://www.cnbc.com/2020/08/24/china-e-commerce-boosted-by-shift-to-online-shopping-after-coronavirus.html.

[775] Xinhuanet, 'China intensifies efforts to protect consumer rights', Last updated May 2018, http://www.xinhuanet.com/english/2018-03/15/c_137041448.htm.

Pertaining to data privacy, China has issued the Data Protection Regulatory Guideline in 2019 to lay out the specific rules that internet companies should abide by when collecting consumer data. Apart from these initiatives China has also introduced Online Courts and Regulations on the Protection of Children's Personal Information Online, both of which will be discussed within this case study.

Regulations on the Protection of Children's Personal Information Online[776,777]

A. Pre-reform situation

The introduction of the "Regulations on the Protection of Children's Personal Information Online" could largely be attributed to China's proactive approach to identifying gaps within its current regulations. While the existing laws and regulations such as Cyber Security Law[778], Civil Code[779], E-Commerce Law[780] and the Provisions on the Protection of Personal Information of Telecommunications and Internet Users[781] had included provisions to safeguard personal information, China identified a need for more detailed regulations to better protect children, particularly their personal information. This need was intensified by the fact that the total number of underage internet users (i.e., between the ages of 6 and 19) were in excess of 170 million and accounted for more than 20 percent of all internet users in the economy. Additionally, minors are increasingly being exposed to the internet early (some even before they are of school age) when their cognitive ability are yet to be fully developed and therefore, more prone to issues such as inadvertent sharing of personal information and online violence.

---

[776] China, 'Regulations on the Protection of Children's Personal Information Online', Last accessed August 19, 2020, http://www.cac.gov.cn/2019-08/23/c_1124913903.htm.

[777] Information in this section are mostly obtained from an interview conducted on 12 August 2020 with Mr. Li Min, Director and Ms. Xu Xiu'an, Offcial, Cyberspace Administration of China.

[778] China, Cybersecurity Law of the People's Republic of China. http://www.csrc.gov.cn/pub/newsite/flb/flfg/flxzsf/201805/t20180518_338285.htmlhttp://www.npc.gov.cn/wxzl/gongbao/2017-02/20/content_2007531.htm. Examples of related provisions include: Article 22 which indicates that "If a network product or service has the function of collecting user information, its provider shall clearly indicate this and obtain consent from the user; and if this involves a user's personal information, the provider shall also comply with the provisions of this law and relevant laws and administrative regulations on the protection of personal information."; and Article 41 which indicates that "Network operators collecting and using personal information shall abide by the principles of legality, propriety, and necessity; they shall publish rules for collection and use, explicitly stating the purposes, means, and scope for collecting or using information, and obtain the consent of the persons whose data is gathered."

[779] The Civil Code of China. Examples of relevant provisions include those pertaining to the right to privacy and protection of personal data.

[780] China's E-Commerce Law of the People's Republic of China, http://www.npc.gov.cn/zgrdw/npc/lfzt/rlyw/2018-08/31/content_2060827.htm. An example of related provision is Article 23 which indicates that "E-commerce operators shall abide by the laws and administrative regulations on personal information protection when collecting and using the personal information of their users."

[781] China's Provision on Protecting the Personal Information of Telecommunication and Internet Users, http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057724/n3057729/c4700145/content.html. Examples of related provisions include: Article 5 which indicates that "Telecommunications service operators and Internet information service providers shall, when collecting and using users' personal information in the process of providing services, adhere to the principles of legality, propriety and necessity."; and Article 6 which indicates that "Telecommunications service operators and Internet information service providers shall be responsible for the security of users' personal information collected and used by them in the process of providing services."

Some examples of incidents that have warranted a need for greater protection includes the excessive use of children's personal information for targeted advertisements by mobile applications and the illegal sales of children's personal information to third parties. Specifically on the former, while the privacy policies of some applications indicates only limited scope of information would be collected, many have gone beyond to collect other information (e.g. location, phone numbers). On the latter, parents had started voicing their concerns when they started receiving unsolicited calls from third parties days after providing information pertaining to their children through some websites.

B. Process of introducing the "Regulations on the Protection of Children's Personal Information Online"

Recognizing the issues, Cyberspace Administration of China (CAC) decided to introduce a special legislation to protect children's personal information. In accordance with the Regulations on the Procedures for Rulemaking, the CAC drafting department conducted an in-depth study and collected opinions from various stakeholders which includes relevant departments, agencies, companies, academia, public, as well as parents and minors. Subsequently, the CAC examination department assessed the legality of the contents when the draft was ready.

Referencing existing laws and regulations while ensuring the inclusion of economy-specific elements

In the course of developing the regulations, China had referred to existing laws and regulations in other economies such as the United States' Children's Online Privacy Protection Rule (COPPA). However, noting that there were not many laws which are specific to children in this area, it also referred to available general data protection laws such as the EU General Data Protection Regulation (GDPR), as well as those introduced in other economies (e.g., Canada, Korea and Japan).

While these laws provide useful reference, China indicated that it is also important to ensure that the regulations fit its own needs and therefore, had included elements that are specific to the economy. For instance, while most economies often have legal liabilities that are pecuniary in nature, penalties for violating certain provisions/articles in the Regulations on the Protection of Children's Personal Information Online could have other implications as well. More specifically, Article 27 of the Regulations indicated that "*When there is conduct violating the provisions of this Law, it shall be recorded in credit files and made public in accordance with relevant laws and administrative regulations."*

Another example would be in the area of security assessments – Article 17 of the regulations required network operators to carry out safety assessments of a third party prior to transferring personal information to them. Essentially, the recipient third party has to be assessed as adhering to certain list of data privacy principles. In its opinion, unlike situations in economies

where pre-transfer safety assessments are not required and enforcement only takes place after an infringement has occurred, the inclusion of this article could potentially minimize the total number of infringements.

Balancing the interests of different stakeholders

One purpose for conducting extensive consultations during the development of a regulation is to ensure that various views are heard and their concerns addressed. Specifically for this regulation, the CAC tried to balance the interests of different stakeholders that were likely to be affected by the regulation. As an illustration, one of the earlier drafts had article which required companies and platforms to receive express consent prior to collecting children's information. This essentially means that information should not be collected unless an individual has actively given their consent to it. However, upon receiving feedback from companies and platforms that the requirement of certain forms of consent might not be suitable for different formats and products, the CAC eventually revised the requirement only to consent, and it was made clear that consent has to be provided in a clear manner. Another instance where CAC tried to address the concerns of some companies and platforms is with regards to those which collected information automatically and yet, are unable to distinguish if the collected information belongs to a child or not. Article 28 stipulates that network operators collecting information via computer information system automatically and are not able to distinguish if the information collected is that of a child will not be taken to have infringed the law. At the same time, noting that the regulation has to achieve its intended objective of protecting children's personal information and minimize the concerns of parents with regards to how their children's information are used, Article 8 requires network operators to establish special children's personal information protection rules and user agreement, and assign specific person to be in charge of children's personal information protection. Article 15 requires that network operators must strictly set the threshold for information access and control the number of people who have access to children's personal information. Where a staff member accesses children's personal information, he/she must be subject to the examination and approval by the children's personal information protection director or his/her authorized management, record the access, and take technical measures to avoid illegal copying and downloading of children's personal information.

Encouraging industry self-regulation

The CAC recognizes that the efficacy of the regulations is very much dependent on the extent that stakeholders would go to uphold its intended objective voluntarily. In the context of this regulation, for example, CAC opined that companies and platforms should have the motivation to protect children's personal information themselves (i.e., self-motivated). In this regard, as part of the regulation's comprehensive management approach, Article 6 encourages internet industrial organization to formulate industrial standards. The idea is that while the regulation sets the minimum requirement, companies and platforms have to be encouraged to introduce new codes of conducts. Indeed, they should have sufficient incentive to introduce such codes

of conducts themselves as it could be used to further promote their commitment to data protection and therefore, gain consumer confidence.

The regulation was promulgated in August 2019 and entered into force on 1 October 2019. The 40-day transition between promulgation and entry into force was set to allow companies and platforms to comply. Relevant government departments, as authorized by the law, are in charge of various aspects of the regulation.

C. Post-Reform Situation

Since the regulation was introduced, China has attempted to raise awareness about the regulatory changes by making use of various channels to do so. These include conducting information sessions in collaboration with schools; organizing panel discussions, creating videos, providing relevant training to internet companies, as well as law enforcement personnel. Most companies and platforms have now introduced comprehensive policies in accordance to the regulations. Additionally, they continue to improve their approach to protecting children's personal information.

While the regulation is relatively new and more time is needed to better assess its implementation, China has identified potential room for improvements. For example, although Article 9 stated that "*Parental or guardian consent must be obtained prior to the collection, use, transfer, or disclosure of children's personal information,*" in practice, it is challenging to determine if every provided consent is indeed coming from parents or guardians.

D. Way Forward

China has identified the need for continued evaluation of the regulation, particularly considering the rapid advancements in many areas including technology, formats and products. It foresees that the regulation would have to be adapted accordingly to better protect children's personal information in the future. On the role of APEC, China opines that the forum can contribute to greater exchange and collaboration among economies to jointly improve the level of children's personal information protection in the Asia-Pacific.

Internet Courts[782]

A. Pre-reform situation

Several reasons contributed to China's decision to establish the Internet Courts. One, the growth of e-commerce has naturally also led to an increase in the number of disputes between consumers and sellers. As the value of transacted goods and services tend to be small, pursuing

[782] Information in this section are mostly obtained from an interview conducted on 12 August 2020 with Mr. He Fan, Director, the Supreme People's Court of China and Ms. Zhang Wen, Chief Judge, Internet Court of Beijing Municipality.

cases via the traditional court system is often not a viable option for consumers, in particular if one is to consider the cost and time of doing so. Often, individuals end up not pursuing any grievances they have against sellers or platforms. The development of an alternative dispute resolution mechanism (where cases involving relatively small value can be resolved at low cost) will therefore spur more consumers to take action against erroneous sellers.

Second, although some e-commerce platforms, especially the larger ones have put in place mechanisms to resolve disputes, there is a need to complement them with the public sector mechanism such as the Internet Courts for various reasons. For a start, some of the smaller platforms may not have such mechanism in place. Furthermore, the issues behind certain disputes may be too complex to be resolved by such private mediation efforts. Additionally, in situations where the firms establishing these private mechanisms are themselves parties in the disputes, it is important to ensure that the judicial process is impartial and not perceived as biased against one party. Moreover, while private mechanisms can resolve majority of the common disputes, there are situations when one party views the proposed solution as not aligned to his/her interest and therefore, decides not to abide by it. In such cases, it would be challenging to enforce the solution as it arguably has no legal underpinning/force.

The use of technology to facilitate the provision of legal services is not a new occurrence in China where it had previously allowed the submission of documents digitally among others. Indeed, in this information age, the public has come to expect a judiciary which leverages technology to a greater extent in order to enhance impartiality, efficiency, convenience, accuracy and transparency among others. However, despite these advances, there are room for improvements. For example, until the establishment of the Internet Courts, individuals are still required to be present physically for court hearings. The Internet Courts are means to further integrate the role of technology in the daily functioning of the judiciary and increase efficiency of proceedings.

B. Process of introducing Internet Courts

Prior to setting up the Internet Courts, China conducted extensive research to better understand how other economies had pursued similar endeavors. In particular, China has tried to learn from the experiences of the United Kingdom and the United States in introducing their online courts. China noted that while having advanced technology is key to successful implementation, it needs to be complemented by sufficient resources and people with the right mindset. For example, while a state within one economy had introduced these courts as early as 2011, challenges with financing had made it difficult to operationalize them. Additionally, judges who are conservative and often prefer physical courts may be against taking the courts online.

To test the feasibility of the Internet Courts in China, the High People's Court of Zhejiang Province introduced pilot online e-commerce tribunals in April 2015 in three district courts in

Hangzhou to handle cases such as online trade, copyright and financial services disputes[783]. Hangzhou was a natural location for the pilot programme because many of the e-commerce firms are headquartered there (e.g., Alibaba). Additionally, the fact that many elements needed to resolve disputes are already stored virtually by these firms (e.g., evidence) made it an ideal location to pilot the first Internet Court where technology would be a key enabler.

Following the success of the pilot programme, the 36th meeting of the Central Leading Group for Comprehensively Deepening Reforms deliberated and adopted the "Plan on the Establishment of Hangzhou Internet Court", which officially led to the establishment the Hangzhou Internet Court in 2017.[784] Two additional courts were established in Beijing and Guangzhou about a year later (i.e., in September 2018).[785] All three courts operate under the same standards and can handle 11 types of cases (e.g. electronic payment, intellectual property, competition). However, their locations meant that they may differ in terms of share of specific cases handled. For instance, the Hangzhou Internet Court, by virtue of its location (i.e., close to e-commerce firms), often deals with issues pertaining to online payments, while the Beijing Internet Court handles many IPRs cases as many tech firms are located there.

Box 5.13: How does the Internet Court work?

With the introduction of the Online Courts, the procedure to resolve disputes have been streamlined. It consists of only 6 main steps, which can all be carried out virtually:

Step 1: Account creation
To create an account, an individual first needs to provide their particulars by completing the online form and uploading copies of his/her identification documents online. Subsequently, the Internet Courts platform will automatically create a QR code, for which the individual will have to scan with their mobile phone. This will redirect the user to a page where they can verify themselves through facial recognition, after which an account will be created.

Step 2: Case submission
An individual (i.e., the complainant) can login into the website to submit and create a case file. She/he has to provide information pertaining to the dispute (e.g., issue of dispute, value of transaction and personal details). A statement of dispute can either be uploaded to the website or filled on the platform itself. The individual can also upload the relevant evidence via the platform

[783] Xinhua Net, 'China Focus: China launches first Internet court in e-commerce hub', Last updated 18 August 2017, http://www.xinhuanet.com//english/2017-08/18/c_136537234.htm.
[784] China Daily, 'China first internet court handles over 10,000 cases', Last updated 18 August 2018, https://www.chinadaily.com.cn/a/201808/18/WS5b77c8f4a310add14f386801.html.
[785] Xinhua Net, 'China's online courts reduce case handling time by half: white paper', Last updated 5 December 2019, http://www.xinhuanet.com/english/2019-12/05/c_138605947.htm.

Step 3: Case review
Judges from the Internet Court will review the submitted application and assess the viability of a case. The results of the review will be sent to the individual through text message. If the case is assessed to be viable, the defendant will also have the opportunity to review the case file as this stage.

Step 4: Decision to mediate or proceed to trial
The individual can choose either the mediation or trial option. Should she/he choose the mediation option, there are several alternative mediation agencies at hand to help. However, should mediation be unsuccessful or should the individual prefers the trial option, the case will then be referred to the judicial system for trial procedures.

Step 5: Hearing
If the trial option is selected, a hearing time would be decided. Both the complainant and the defendant will receive a text notification and a summon via the platform. They can then participate in the hearing through the same platform.

Step 6: Verdict
The result of the trial will be communicated to the participants through their preferred mode of contact (e.g. SMS, email). Subsequently, the participants can decide whether to accept or decline to accept the ruling made by the Internet Court. Should both or either participant decline, an appeal can be filed within the stipulated time period.

Source:
- Beijing Internet Court Guide, https://www.youtube.com/watch?v=WPAkF-7bT_U&feature=youtu.be

C. Post-Reform Situation

The establishment of the Internet Courts has brought greater convenience to parties involved in disputes. The full implementation of Online Filing and Cross-regional Filing Mechanisms, as well as One-Stop Diversified Dispute Resolution and One-Stop Litigation Service have improved access to justice. Besides saving cost and time, the adoption of advanced tools such as big data and Artificial Intelligence (AI) has enabled consumers to predict the likely outcome of a potential case and therefore, decide whether to submit a case. This self-screening procedure arguably allows the Internet Courts to reduce the number of cases handled, particularly those whose odds are stacked against the consumers.

It is important to note that the benefits of advanced tools extends to facilitating the work of the judges as well. For example, the use of online database allows judges to quickly consolidate past judgements pertaining to similar cases when conducting legal research. At the same time, recognizing that technology is not a silver bullet and still needs to be further developed prior to them being employed more extensively (e.g., AI), China indicated that technology is only

used to assist the process and make it more efficient where applicable. Judgements in the Internet Courts continue to be made carefully by judges who have been legally-trained.

Being at the forefront of a relatively new field, have also led to the Internet Courts handling many contemporary issues pertaining to the digital economy, which have no precedents to rely upon in many situations. For instance, the Beijing Internet Court recently handled cases involving user data infringement and ruled against Tencent and ByteDance.[786]

As of 31st October 2019, the Internet Courts in Hangzhou, Beijing and Guangzhou had accepted 118,764 cases and concluded close to 75 percent of these cases (i.e., 88,401 cases). Online filing (i.e., cases filed via the Internet) stood at a high 96.8 percent, and 80,819 of the concluded cases were conducted online throughout the entire process. In terms of efficiency, the Internet Courts were found to take an average of 45 minutes for online hearings and 38 days to conclude a case, which was about 60 and 50 percent shorter than conventional courts, respectively. Additionally, about 98 percent of the parties accepted the first judgments.

Impartiality of the courts

Despite these positive developments, the Internet Courts have had their fair share of challenges and have worked to remedy them over time. For example, in the earlier days of the Internet Courts, there were questions on their impartiality. The fact that they are co-located in the same areas as many e-commerce and tech firms, some of which even offered to contribute equipment and technologies to facilitate the operations of the courts, adds to this suspicion. On their part, the Internet Courts did not accept these contributions and worked hard to prove their impartiality. As more judgements against these firms were delivered (such as the cases involving Tencent and ByteDance mentioned earlier), perceptions of their perceived biasedness in favor of these firms change.

Ensuring inclusion

There was also an issue pertaining to the inclusiveness of the services offered by the Internet Courts. Initially, passwords in the Internet Courts websites involved a mixture of letters and numbers, but the non-familiarity of the elderly individuals with English language made it a struggle for them to remember these passwords. In response, the Internet Courts changed the requirements such that passwords now include only numbers and symbols.

Reliability of technology

Last but not least, the extensive use of technology by the Internet Courts have resulted in the need to constantly assess the reliability of such technology and hence the extent to which they

[786] SCMP, 'Beijing internet court rules against Tencent, ByteDance in user data infringement cases', Last updated 3 August 2020, https://www.scmp.com/tech/apps-social/article/3095790/beijing-internet-court-rules-against-tencent-bytedance-user-data.

are being adopted in the day-to-day work of the courts. For instance, although blockchain technology has been argued to be tamper-proof and therefore used to secure evidence, parties are always welcome to raise their concerns should they believe that certain evidence may have been tampered with.

D. Way Forward

China continues to improve on the functioning of the Internet Courts. In December 2019, the decision to allow judgements to be provided online in 20 cities was formally passed. It is currently on trial and applies to all cases (i.e., not exclusive to the judgements of the Internet Courts). If the trial is successful, formal amendments to the Civil Code would be carried out.

The growth of cross-border e-commerce would also lead to an increase in extra-territorial disputes. However, at the moment, the Internet Courts cannot yet handle extra-territorial disputes. This is one area where viable solutions need to be explored.

Key messages

With the growth of e-commerce comes the need for better consumer protection and data privacy, in particular ensuring that they can address contemporary issues associated with the online world. China has made considerable efforts in this area, as reflected in this case study which focuses on the Regulation for the Protection of Children's Personal Information Online and Internet Courts, both of which has had several important takeaways.

Acknowledging that underage users now made up a significant share of all internet users in the economy and yet, may not have the cognitive ability to properly respond to pervasive issues (e.g., those pertaining to the sharing of personal information), the Regulation for the Protection of Children's Personal Information Online aims to provide more detailed regulations to better protect children, particularly their personal data. Some key elements of this regulation include: 1) requiring companies and platforms to receive consent from parent/guardian prior to collecting children's information; 2) additional legal liabilities beyond those which are pecuniary in nature; and 3) encouraging self-regulation by the industry.

Recognizing that the traditional court system is often not a viable option to resolve e-commerce disputes, in particular considering their relatively small value, the Internet Courts were established to provide an alternative avenue for doing so. Some key learnings include: 1) how technology can be better integrated into the daily functioning of the judiciary so as to increase efficiency of proceedings; 2) how technology can be adopted without compromising on the courts' ability to provide impartial justice; and 3) how the courts have continued to evolve across various metrics (e.g., type of contemporary issues handled, ensuring inclusive access to justice).

Japan

Background

A. Legal framework for dispute resolution in Japan

In Japan, a law called the Specified Commercial Transaction Act governs matters related to e-commerce, while a variety of other laws regulate false or deceptive advertisements. Furthermore, government accredited consumer organizations (called Specified Qualified Consumer Organizations) are given the right to file injunction requests in a collective lawsuit against a business operator who violates the Specified Commercial Transaction Act.[787]

The Act on Promotion of Use of Alternative Dispute Resolution (The ADR Act) regulates the mediation of settlements that occur outside of courts, although the process is still interpreted as a legal affair requiring professional lawyers (including legal fees). Compared to economies like the United States, where the handling of consumer disputes is largely left in the hands of the free market, and a settlement or a lower monetary amount is considered acceptable if consumers agree to it, the Japanese system places a greater emphasis on substantive justice. It is implied that the ADR Act standards will be applied to ODR in Japan. Therefore, if a private company is to perform ODR (for a fee), they must set up a system where legal advice from a lawyer is made available. In theory, this provision could complicate the ODR procedures of large platform companies.[788]

B. Mechanisms for dispute resolution

According to Habuka (2015), the dispute resolution options available to Japanese consumers are insufficient to address the growing number of transaction issues.[789] A 2015 survey by the Mitsubishi Research Institute found that only 33 percent of e-commerce disputes were resolved, with 12 percent of resolutions being unsatisfactory to the customer.[790] Consumers can choose civil litigation, conducted entirely in-person, for transactions under USD 5,455. The process takes around two months from the filing of the case to the final judgement and includes a filing cost of USD 36.40, which is about half the value of an average e-commerce purchase. Furthermore, the consumer is responsible for preparing a written petition and submitting

[787] Interview Memo. Atsushi Moriya, Legal System Planning Division, Consumer Affairs Agency (CAA); Ayumi Edakubo, Dispute Resolution Committee, National Consumer Affairs Center (NCAC); Naoko Iwasaki (& 2 staff members), National Consumer Affairs Center (NCAC); Kazuhito (or Kazuto) Kobayashi, General Office for the Economic Revitalization of Japan, Cabinet Secretariat; Tadayoshi Hiraki, APEC Office, METI. (July 29, 2020). Phone interview.
[788] Interview Memo. Professor Aya Yamada, Kyoto University. (July 30, 2020). Phone interview.
[789] Hiroki Habuka, 'The Promise and Potential of Online Dispute Resolution in Japan', International Journal of Online Dispute Resolution 2, 2017, Last accessed 24 August 2020, https://www.elevenjournals.com/tijdschrift/ijodr/2017/2/IJODR_2352-5002_2017_004_002_017.
[790] Mitsubishi Research Institute, Inc., '越境ＥＣ（電子商取引）の動向', Consumer Affairs Agency, Government of Japan, September 2015, Last August 2020, https://www.caa.go.jp/policies/policy/consumer_policy/policy_coordination/internet_committee/pdf/150930shiryo1.pdf.

evidence which usually requires advice from a lawyer. The process is costly and complex, and thus only 11,030 cases were processed through this mechanism in 2015.[791]

Japan's National Consumer Affairs Center (NCAC) is the most common option for consumers seeking redress of disputes with core functions. NCAC reported that it received 77,318 e-commerce complaints in 2017, more than double the number in 2012 (31,934 cases).[792] NCAC responds by encouraging the two parties to negotiate and reach a settlement, while consumers can also receive 'consultations' which are essentially legal advice to assist them in negotiating with the company. While 6 percent of cases are resolved at the negotiation stage, the advice and recommendations are non-binding and it is possible that a vendor does not reply to contacts from NCAC or disagrees with the suggested settlement. Some cases that are categorized by NCAC as 'important consumer disputes' can be subject to a more formal mediation and arbitration processes. However, these only include mass claims impacting a large group of consumers or products that could cause physical harm, excluding most B2C e-commerce claims. In fact, only 172 cases were subject to this process in 2017. [793]

Recent experience with ODR in Japan

A. Motivation: Rise of cross-border e-commerce and related disputes

Japan is the fourth largest B2C e-commerce market in the world, representing USD122 billion in 2018[794] and trailing only China, the United States and the United Kingdom. Though only about 10 percent of Japanese consumers purchase goods from foreign websites, with its population of 126.5 million, Japan is an enticing market for cross-border traders and sellers. Japan's cross-border e-commerce market was valued at approximately USD2.52 billion[795] in FY 2018 and was forecast to reach almost USD2.87 billion[796] by FY 2022.[797]

At the same time, Japanese consumers are particularly concerned about the prospect of dealing with commercial disputes, indicating possibly that existing redress options are insufficient. Surveys demonstrate a higher level of concern than in the US, UK, Germany and China.[798]

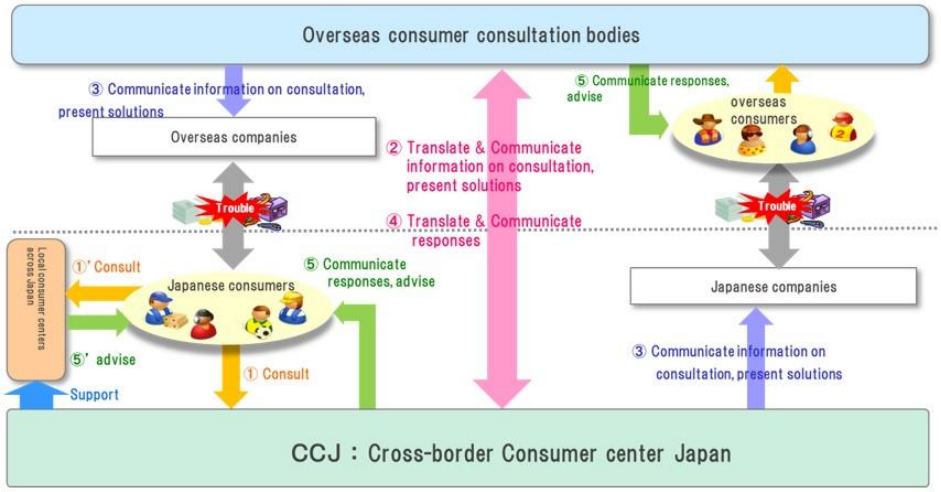
[791] Ibid.
[792] Hiroki Habuka, (2017).
[793] Ibid.
[794] Jacqueline Dooley, 'A Comprehensive Guide to the Japanese Ecommerce Market', ClickZ, February 2020, Last accessed 24 August 2020, https://www.clickz.com/a-comprehensive-guide-to-the-japanese-ecommerce-market/260277/.
[795] 277 billion Japanese yen. *Forecast. 1 Japanese yen equals 0.0091 U.S. dollars as of May 2019.
[796] 315 billion Japanese yen. *Forecast. 1 Japanese yen equals 0.0091 U.S. dollars as of May 2019.
[797] Statista Research Department, 'Cross-border e-commerce market size in Japan from fiscal year 2017 to 2022', Statista, May 2019, Last accessed 24 August 2020, https://www.statista.com/statistics/892681/japan-cross-border-e-commerce-market-size/.
[798] Hiroki Habuka, (2017).

B. Measures to address cross-border disputes

The Code of Civil Procedure in Japan was amended in 2012 to give Japanese courts jurisdiction over disputes lodged by Japanese consumers against foreign companies, although such judgements are "nearly impossible to enforce". Despite this challenge, the NCAC established the Cross-Border Consumer Center of Japan (CCJ) to address disputes involving Japanese consumers purchasing from foreign vendors. CCJ was established in 2011 as a pilot program to address communication challenges and language barriers faced in cross-border disputes, albeit it does not provide mediation and arbitration services. CCJ functions by establishing relationships with foreign consumer agencies to support negotiations between Japanese consumers and foreign vendors. CCJ has partnerships with 15 organizations and 26 economies around the world.[799] CCJ received about 6,200 cross-border consumer complaints in FY 2018, a 50% increase over FY 2017.[800][801]

CCJ accepts complaints from Japanese vendors and sends English-language translations to foreign partner agencies to establish communications with the vendor, which will in turn make a request to the business operator to resolve the issue. The process also works in reverse with CCJ receiving complaints on behalf of consumers from partner agencies and contacting Japanese vendors.

Figure 5.3: CCJ relationship with partner consumer support agencies



Source: NCAC[802]

[799] These economies include: the United States; Canada; Mexico; Chinese Taipei; Singapore; Viet Nam; Russia; Thailand; the Philippines; United Kingdom; Malaysia; Hong Kong, China; Latvia; Estonia; Spain; Argentina; Chile; Uruguay; Paraguay; Bolivia; Brazil; Peru; Columbia; Venezuela; Costa Rica; and Mexico.

[800] Yoshihisa Hayakawa, 'Japanese Experiences and Coming New UNCITRAL ODR Rules', UNCITRAL, 2012, Last accessed 24 August 2020, http://uncitralrcap.org/wp-content/uploads/2015/11/Day2_Panel2_A_3_Yoshihisa-Hayakawa_JAPANESE-EXPERIENCES.pdf.

[801] National Consumer Affairs Center of Japan, 'FY2018 Summary of Inquiries about Cross-Border Consumer Disputes Received by Cross-Border Consumer Center Japan (CCJ)', August 2019, Last accessed 24 August 2020, http://www.kokusen.go.jp/e-hello/news/data/n-20190808_5.html.

[802] "National Consumer Affairs Center of Japan (NCAC)," National Consumer Affairs Center of Japan, August 2020, Last accessed 24 August 2020, http://www.kokusen.go.jp/hello/pdf/mi-gyoumu_01_en.pdf

C. Private dispute resolution options

In Japan, three e-commerce marketplace platforms—Rakuten, Amazon, Yahoo Shopping—account for over one-third of e-commerce transactions. [803] These platform providers have been able to establish their own ODR systems, including both domestic and foreign e-disputes. NCAC's surveys demonstrate that consumers place a large degree of trust in these platforms and their dispute resolution mechanisms. In contrast, MSMEs usually lack the capacity to offer ODR services, particularly for cross-border e-disputes. In this respect, efforts by the government to promote ODR may help to alleviate this competitive disadvantage faced by MSMEs.[804]

Government strategy

A. Government promotion of ODR via the cabinet's ODR committee

Japan has lagged behind other economies in terms of attention to ODR. The increasing number of online disputes and the lack of accessible ODR options has become a burden that may impede the growth of the e-commerce market in Japan. As part of broader e-government and court digitization efforts, the Japanese government established the Online Dispute Resolution Committee ("ODR Committee") to identify the current e-commerce market's challenges as well as to facilitate the adoption of ODR. Through the ODR Committee's study sessions, the government has attempted to raise the private sector's awareness of the potential of ODR.

The Japanese government issued a Growth Strategy in June 2019 that required the government to formulate a basic plan on ODR before April 2020. Based on this Growth Strategy, Japan established the ODR Study Group in 2019, which is responsible for studying ODR and accelerating its launch.[805] The effort also seeks to address the decreasing number of civil litigation cases for commercial disputes, which NCAC speculates is due to many consumers' complaints going unreported.[806] These efforts aim to synergize e-government efforts with broader goals related to legal and judicial reforms to increase access to justice.[807]

The Cabinet's ODR Study Group has engaged stakeholders such as: The Financial Services Agency; The Consumer Affairs Agency; The Ministry of Justice; The Ministry of Economy, Trade and Industry; The Small and Medium Enterprise Agency; The Supreme Court (which

[803] Marcia Kaplan, 'Japan is an Enticing Market for Cross-Border Ecommerce', Practical Ecommerce, May 2020, Last accessed 24 August 2020, https://www.practicalecommerce.com/japan-is-a-enticing-market-for-cross-border-ecommerce.
[804] Interview Memo. Dr. Michael Dennis and Professor Yoshihisa Hayakawa (July 1, 2020). Phone Interview.
[805] Prime Minister's Office of Japan, 'About the Launch of ODR Committee (ODR 活性化検討会の開催について)', 2019, Last accessed 24 August 2020, https://www.kantei.go.jp/jp/singi/keizaisaisei/odrkasseika/pdf/konkyo.pdf.
[806] Interview Memo. Atsushi Moriya, Legal System Planning Division, Consumer Affairs Agency (CAA); Ayumi Edakubo, Dispute Resolution Committee, National Consumer Affairs Center (NCAS); Naoko Iwasaki (& 2 staff members), National Consumer Affairs Center (NCAS); Kazuhito (or Kazuto) Kobayashi, General Office for the Economic Revitalization of Japan, Cabinet Secretariat; Tadayoshi Hiraki, APEC Office, METI. (July 29, 2020). Phone interview.
[807] Interview Memo, Professor Aya Yamada, Professor of Law- Kyoto University. (July 30, 2020). Phone.

also participated as an observer); university professors (experts on ADR law, civil litigation law, and the intersection of law and IT); lawyers (who were to provide legal background commentary and support); a representative of an e-commerce platform (Yahoo!); and a consumer group representative (EC network).

The ODR Study Group has met regularly since September 2019 to collect various information.[808] The ODR Basic Plan was developed and issued by the ODR Committee in March 2020, addressing the current challenges and opportunities for implementing an ODR system in Japan.[809] The government's position in the ODR Basic Plan is to support initiatives led by private companies, while public authorities could launch efforts to improve the reliability and safety of ODR, such as the development of certification systems.[810] The plan is intended to launch a verification trial in 2020 of a new ODR system. Petitions and claims would be submitted via computers, smartphones or other such devices, and a neutral third party would use AI to present possible solutions.[811]

B. International outreach: APEC collaborative framework for ODR

In addition to this work, Japan has taken an active role within APEC to promote work to establish the APEC Collaborative Framework for ODR, including providing funding for workshops that led to the publication of the APEC Procedural Rules for ODR. This effort will establish a framework under which platform hosts/ODR providers, including regional arbitration and mediation centers, could provide dispute resolution services utilizing the procedural rules, with a central list of providers managed by APEC. The project is currently focused on business-to-business (B2B) disputes given the lack of options for MSMEs but is planned to expand its focus to B2C disputes in the next two to five years. The project represents a promising development in cross-border dispute resolution given its broad acceptance by APEC members.[812]

C. Challenges towards establishing consumer ODR in Japan

Habuka (2015) considers that the main question around ODR in Japan is which actor will develop and host the system. Courts are deemed as non-viable due to the conservative management style of the Japanese judiciary, while NCAC is considered as a potential option.

---

[808] Prime Minister's Office of Japan, ODR Committee, 'ODR Committee (ODR 活性化検討会)', June 2019, Last accessed 24 August 2020, https://www.kantei.go.jp/jp/singi/keizaisaisei/odrkasseika/.

[809] Prime Minister's Office of Japan, ODR Committee, 'ODR Basic Plan (ODR 活性化に向けた取りまとめ)', March 2020, Last accessed 24 August 2020, https://www.kantei.go.jp/jp/singi/keizaisaisei/odrkasseika/pdf/report.pdf.

[810] Interview Memo. Atsushi Moriya, Legal System Planning Division, Consumer Affairs Agency (CAA); Ayumi Edakubo, Dispute Resolution Committee, National Consumer Affairs Center (NCAS); Naoko Iwasaki (& 2 staff members), National Consumer Affairs Center (NCAS); Kazuhito (or Kazuto) Kobayashi, General Office for the Economic Revitalization of Japan, Cabinet Secretariat; Tadayoshi Hiraki, APEC Office, METI. (July 29, 2020). Phone interview.

[811] Asia News Network, "AI system for small claims settlement eyed," Asia News Network, January 2020, Last accessed 24 August 2020, http://ftp.asianews.network/content/ai-system-small-claims-settlement-eyed-112692?qt-most_downloaded=0.

[812] Interview Memo. Prof. Yoshi Hayakawa (July 7, 2020). Phone Interview.

Meanwhile, private businesses may be open to developing ODR systems integrated with their own transactions, potentially boosted by public incentives. However, this option raises concerns over the independence and impartiality of ODR.[813] As mentioned earlier, incentivizing parties to participate in ODR is a major challenge. Given that Japan currently lacks an effective ODR option, simply passing a regulatory mandate for ODR adoption would not be a viable option. Enforceability may be a challenge for cases in which a settlement is not reached via negotiation, given that Japanese law precludes the use of binding pre-dispute arbitration agreements. Relative to other economies, providing ODR in Japan may also be more expensive due to ODR Act requirements (neutrals must be attorneys or judicial scriveners).[814]

Assessment: Stakeholder perspectives

A. Merchants and platforms

During the ODR Committee's study sessions, merchants and platforms have expressed concerns over challenges related to developing and deploying ODR systems. Businesses are concerned about the costs of building ODR systems as well as their effectiveness in addressing consumer e-disputes, and thus would favor incentives from the government to support the adoption of ODR.[815]

Generally, dominant e-commerce platforms like Rakuten have already invested in internal complaint handling systems and are more hesitant about participating in government efforts. Habuka (2015) finds that e-commerce platforms themselves have the strongest economic incentive to invest in their own ODR systems to secure a sustainable competitive advantage over those that do not.[816] Meanwhile, small and mid-sized e-commerce stakeholders have a more positive outlook on government ODR efforts due to their lack of resources to establish their own quality complaint handling systems.[817]

Furthermore, some perspectives on ODR are impacted by general perceptions of ADR within Japan. Companies might prefer bringing cases to court because it is very difficult to internally justify (to shareholders) the amount of payment made as part of an ADR settlement, raising internal compliance issues.[818]

[813] Hiroki Habuka, 2017.
[814] Ibid.
[815] Prime Minister's Office of Japan ODR Committee, 'ODR Committee's Study Session (3rd Meeting) Summary (ODR 活性化検討会（第3回）議事要旨)', 2019, p.15, Last accessed 24 August 2020, https://www.kantei.go.jp/jp/singi/keizaisaisei/odrkasseika/dai3/gijiyousi.pdf.
[816] Hiroki Habuka, 2017.
[817] Interview Memo. Dr. Michael Dennis and Professor Yoshihisa Hayakawa (July 1, 2020). Phone Interview.
[818] Interview Memo. Professor Aya Yamada, Kyoto University. (July 30, 2020). Phone interview.

B. Consumers

Surveys by NCAC show that 30 percent of consumers prefer e-commerce platforms to resolve their disputes, with NCAC consultation services coming in second place. Regarding these consultative services, there is a concern that careful, personalized consultation services which have been traditionally offered by the NCAC would no longer be available if ODR is introduced.[819]

C. Government

From the perspective of government stakeholders such as NCAC, there is a lack of visibility into the magnitude of disputes in the e-commerce segment amidst a declining number of civil litigations related to commercial disputes. In this context, NCAC believes that the promotion of ODR could expand access to dispute resolution services to address the true magnitude of disputes.[820] From the government's perspective, internal ODR mechanisms of e-commerce platforms may be insufficient from the standpoint of consumer justice under a variety of scenarios, including; when a company causes harm to a great number of consumers; or when a company may be able to offer a smaller settlement than would be instituted by a civil court.[821]

Conclusion

The NCAC personalized consultative services are undeniably favorable and useful to consumers in understanding their rights and negotiating with businesses in Japan. However, it is increasingly clear that the NCAC and civil courts are not adequately equipped to address the rise in e-commerce disputes. Meanwhile, the experience of CCJ demonstrates some potential lessons for handling cross-border disputes via bilateral cooperation, as well as a demand for such services in Japan. As such, the availability of cross-border ODR systems may increase consumer confidence in making purchases internationally.

The Japanese government has initiated efforts to study options for implementation of an ODR system utilizing a participatory approach in which the ODR Committee engages with different stakeholders and considers various options carefully. At the same time, the government is actively promoting the establishment of an international standard framework for ODR at international forums such as APEC. However, challenges remain. These include uncertainty over the funding and custody of the mechanism, legal and regulatory challenges related to ADR, as well as hesitation by some stakeholders. CCJ's cross-border mechanism also lacks the ability to achieve final settlement for customers absent mediation and arbitration functions. As to

[819] Interview Memo. Professor Aya Yamada, Kyoto University. (July 30, 2020). Phone interview.
[820] Interview Memo. Atsushi Moriya, Legal System Planning Division, Consumer Affairs Agency (CAA); Ayumi Edakubo, Dispute Resolution Committee, National Consumer Affairs Center (NCAS); Naoko Iwasaki (& 2 staff members), National Consumer Affairs Center (NCAS); Kazuhito (or Kazuto) Kobayashi, General Office for the Economic Revitalization of Japan, Cabinet Secretariat; Tadayoshi Hiraki, APEC Office, METI. (July 29, 2020). Phone interview.
[821] Interview Memo. Professor Aya Yamada, Kyoto University. (July 30, 2020). Phone interview.

whether this could potentially change in the future, the economies of scale of such a service remains unclear.

Mexico

Background

Mexican consumer protection law requires businesses to negotiate with consumers who lodge complaints, for which the Federal Consumer Protection Agency of Mexico (PROFECO) provides a variety of options including in-person hearings, telephone-based hearings, and online hearings through an ODR platform known as Concilianet. Mexican federal law does not regulate B2C cross-border electronic disputes due to the absence of jurisdiction and competence of the Law to address conflicts of Mexican consumers against foreign providers.[822]

Rise of e-commerce

The e-commerce segment in Mexico grew to about USD50 billion in 2018 with growth fueled by increasing internet penetration through mobile and fixed broadband expansion, increasing consumer credit and payment options, above-average logistics performance in Mexico, and a growing middle class.[823][824] A 2017 survey found that out of 16.8 million Mexican citizens who purchased goods online, 11 million made cross-border purchases. The survey also reported that reliability and convenience were key factors for Mexican consumers when making cross-border purchases. Given these preferences, 68 percent of e-commerce consumers reported that they made their purchases via large global platforms such as Amazon.[825]

Concilianet as an ODR service

PROFECO established Concilianet as a pilot project in 2008 to test whether consumer conflict resolution processes could be migrated online using ICT. The pilot program was implemented under the independent initiative of PROFECO and it was launched with just two companies registered (Hewlett Packard and Aeroméxico).[826]

---

[822] Dr. Amada Arley, 2020.

[823] Antonio Gonzalez et al., 'Mexican E-commerce Sector', Credit Suisse Securities Research & Analytics, October 2015, Last accessed 24 August 2020, https://research-doc.credit-suisse.com/docView?source_id=eqgl&document_id=1054125581&format=PDF&language=ENG&serialid=5l74YkjWPazn7e0Faj%2B3lOBmJTf%2Ftmi2kM9bqiL5kZs%3D.

[824] National Institute of Statistics, Geography and Computing (INEGI), 'Electronic Commerce', 2020, Last accessed 24 August 2020, https://www.inegi.org.mx/temas/vabcoel/.

[825] Claudia Juárez Escalona, 'Cross-Border E-commerce Rises to 113,600 Million Pesos', The Economist, 2018, Last accessed 24 August 2020, https://www.eleconomista.com.mx/empresas/Comercio-electronico-transfronterizo-asciende-a-113600-millones-de-pesos-20180913-0225.html.

[826] Dr. Amada Arley, 2020.

The resulting Concilianet platform is a free, digital tool that aims to facilitate communication during the conciliation process in disputes. Concilianet handles disputes arising from both online and offline transactions, and offers significant improvements over the in-person complaint handling system in terms of logistics, efficiency, and accessibility.[827] Furthermore, the fact that Concilianet is an online platform allows it to be centralized yet accessible anywhere in the economy. This allows PROFECO to hire professionalized conciliators to handle disputes, whereas regional and local consumer protection offices face greater challenges in securing highly capable human resources. Concilianet is a "passive software" in that it helps to facilitate communication between the parties, but does not resolve, evaluate, or suggest agreements. An online chat system is used to establish direct communication with the vendor, consumer and a professional conciliator at PROFECO. The platform only includes "participant providers" who have signed an agreement to register with Concilianet.[828]

A consumer is able to fill out an online complaint form and attach relevant documents. Then, the conciliator evaluates the documents (e.g., receipts) and determines if the complaint is legitimate. The hearing itself is later conducted via a synchronous chat system which automatically generates an agreement if the parties reach a mutually accepted settlement. If the parties are unable to reach an agreement, the consumer has the right to seek resolution through the courts, while PROFECO assesses the probable violations of consumer law on the part of the company (if any). Despite the swift resolutions of disputes via Concilianet, the consumer may face a number of barriers in seeking the execution of this agreement, as elaborated below.[829]

Although PROFECO lacks the tools and legal authority to process cross-border disputes, it does contain the Department of Conciliation for Residents Abroad (CARE), which is in charge of receiving complaints from consumers residing outside of the economy. PROFECO has established a portal to electronically formulate this type of complaints, in three languages: Spanish, English and French. While foreign consumers have the option to use this for e-commerce transactions, it provides no protection to Mexican consumers who make purchases from other economies.

A. Facts and figures

In 2010, there were 18 companies registered within the Concilianet system, which grew to over 97 by 2018, including five e-commerce platforms.[830] Out of the five e-commerce platforms who participate in Concilianet, Groupon is the smallest with a market capitalization of just

[827] Gabriela Szlak, 'Online Dispute Resolution in Latin America', Online Dispute Resolution Theory and Practice, 2012, ed. Mohamed S. Abdel Wahab at al., Eleven International Publishing. Last accessed 24 August 2020, https://www.mediate.com/pdf/szlak.pdf.

[828] Interview Memo. Dr. Amada Arley. (July 9th, 2020). Phone interview.

[829] Interview Memo. Dr. Amada Arley. (July 9th, 2020). Phone interview.

[830] PROFECO, 'Concilianet- Participating Providers', n.d., Last accessed 24 August 2020, https://concilianet.profeco.gob.mx/Concilianet/proveedores_que_concilian.jsp.

under US$0.5 billion[831], while Mercado Libre[832] is the dominant platform in Latin America[833], and Amazon is among the largest in the world.

At 36 days per case in 2017, Concilianet's performance is comparable to other ODR services in terms of the duration to resolve cases (e.g., 30 days for the public ODR platform PARLe in Quebec (Canada), and 36 days for eBay).[834] In 2009, 318 claims were processed by Concilianet representing 0.2 percent of total claims to PROFECO. By 2019, the system handled a total of 6,790 claims, representing 7.29 percent of total claims to PROFECO. In 2012, there were 1,766 complaints filed with a conciliation rate of 95.3 percent and an average processing time of 23 days, while in 2018, there were 6,790 cases, an 86.5 percent resolution rate and with 34 days average taken per case. Cases resolved by Concilianet led to the recovery of almost 18 million pesos, or nearly USD800,000, representing 103 percent[835] of the total value of claims.[836]

B. Challenges

Mexican consumer protection via Concilianet's ODR platform is a positive development and has succeeded in creating more efficient online versions of PROFECO consumer dispute processes. But overall Concilianet is still an adequate means accessing justice considering the high amount of B2C transactions in the Mexican e-commerce market. The most prominent reasons are the following:

- ***Concilianet only handles a small portion of claims originating from the mainly large firms in the e-commerce sector***

Out of nearly USD 500 million Amazon sales in Mexico in 2016, Concilianet only received 122 claims against the platform. The total volume of transactions processed by Concilianet is under 7,000 with under USD1 million in recovered funds, while e-commerce sales in Mexico in 2019 exceeded USD 50 billion. These figures seem to be driven by the high amount of trust of Mexican consumers in private dispute resolution mechanisms. This is understandable given that companies like Amazon offer generous customer guarantees and have the ability to easily resolve disputes by refunding purchases or replacing products. Furthermore, the only e-commerce platforms registered are large multinational firms, meaning that Concilianet does

[831] Macrotrends, 'Groupon Market Cap 2009-2020', 2020, Last accessed 24 August 2020, https://www.macrotrends.net/stocks/charts/GRPN/groupon/market-cap.
[832] Mercado Libre, 'Mercado Libre Acquired Deremate in 2008', Mercado Libre, August 2008, Last accessed 24 August 2020, http://investor.mercadolibre.com/news-releases/news-release-details/mercadolibre-inc-announces-agreement-acquire-operations-deremate.
[833] José Gabriel Navarro, 'Most Popular Online Retailers in Latin America as of May 2018, Based on Number of Unique Visitors', Statista, July 2020, Last accessed 24 August 2020, https://www.statista.com/statistics/321543/latin-america-online-retailer-visitors/#:~:text=As%20of%20May%202018%2C%20Mercado,sites%20with%2022.4%20million%20visitors.
[834] Dr. Amada Arley, 2020.
[835] Indicating various fines and levies were collected by PROFECO in addition to consumer funds recovered.
[836] Senate of the Republic of Mexico, 'Initiative to add a Chapter XVI on the Consumer Ombudsman to the Federal Law on Consumer Protection', 2020, Last accessed 24 August 2020, https://infosen.senado.gob.mx/sgsp/gaceta/64/2/2020-02-18-1/assets/documentos/Inic_Morena_Sen_Monreal_Proteccion_Consumidor.pdf.

not provide ODR services for MSME online retailers.[837] It could also be speculated that the large market share captured by these platforms and the lack of accessible dispute resolution options may drive small and mid-sized retailers to instead choose to sell their goods via large platforms rather than directly to consumers.

- ***The settlements reached by Concilianet and PROFECO face enforceability challenges***

A recent decision by Mexico's Supreme Court found that agreements from PROFECO (and thus Concilianet) were not binding or enforceable and merely considered technical opinions. Thus, if a consumer receives an agreement through Concilianet and the involved company does not comply with it, the consumer must initiate a court proceeding and rely on the judge's interpretation of PROFECO's 'technical opinion.'[838] However, after a failed execution of an agreement from PROFECO, the consumer rarely goes to the Court to enforce the fulfillment of the agreement because of the perceived time, money and familiarity with the legal system that it requires. This challenge constitutes a gap. Thus, the effectiveness of the conciliation process is also highly dependent on the willingness of the vendor to comply with the agreement.[839]

- ***The effectiveness of the enforcement power of PROFECO through the issuance of fines is low in comparison to the actual power of platforms over their vendors***

PROFECO in general is only able to levy small fines on providers who are determined to have violated the law or repeatedly missed hearings.[840] Meanwhile, large e-commerce platform have a high degree of control over vendors on the platform as well as payment methods.

- ***Concilianet does not have sufficient human capital***

The ability of Concilianet to process a greater number of disputes is dependent on professionalized conciliators who require considerable education and training. In fact, the relative benefits of Concilianet over the processing of consumer complaints can be partially attributed to the professionalization of conciliators versus less capable conciliators in regional PROFECO offices where consumers would otherwise file complaints. The entirety of Concilianet is operated by two offices with around twelve conciliators who face large caseloads. However, PROFECO currently lacks the budget to contract more staff in order to more quickly process disputes and incorporate more participating providers in the system. Given these limitations, Concilianet has experienced increases in the average number of days required to resolve disputes in the past few years.[841] These challenges have been exacerbated by the

[837] Dr. Amada Arley, 2020
[838] Interview Memo. Dr. Amada Arley. (July 9th, 2020). Phone interview.
[839] Dr. Amada Arley, 2020.
[840] Interview Memo. Dr. Amada Arley. (July 9th, 2020). Phone interview.
[841] Interview Memo. Maestro Filiberto, General Director of Claims and Conciliation - PROFECO. (August 10, 2020). Videoconference.

ongoing coronavirus pandemic that has limited access to in-person PROFECO services, thereby increasing the number of claims received via Concilianet. This has nearly doubled the number of cases that each conciliator is responsible for and increased urgency around the need to automate parts of the process to reduce the burden on conciliators.[842]

- ***Budgetary restrictions for the acquisition of automatization technologies***

While there is an emerging discussion[843][844][845][846] surrounding the use of AI in various phases of ODR to reduce the need for human intervention to achieve settlements, PROFECO currents lack the budgetary resources to procure and implement such a system.[847]

- ***Cross-border disputes***

The lack of provisions in Mexican law establishing protections for Mexican consumers engaged in cross-border e-commerce limits Concilianet to domestic transactions. The CARE Office within PROFECO also does not provide protection to Mexican consumers making cross-border purchases.

Assessment: Stakeholder perspectives

Overall, stakeholder groups in the Mexican e-commerce segment, including large e-commerce platforms and consumers, seem to have a positive outlook on Concilianet.

A. Consumers

User surveys carried out by PROFECO in 2017 and 2018 revealed 93% and 89.2% of consumers were satisfied with the platform, making it one of the most popular e-government services.[848]

[842] Interview Memo. Maestro Filiberto, General Director of Claims and Conciliation - PROFECO. (August 10, 2020). Videoconference.
[843] David Carneiro et al., 'Online dispute resolution: An artificial intelligence perspective', Artificial Intelligence Review 41 (2), February 2014, Last accessed 24 August 2020, https://www.researchgate.net/publication/257512757_Online_dispute_resolution_An_artificial_intelligence_perspective.
[844] Arno Lodder and John Zeleznikow, 2012.
[845] Dr. Amada Arley, 2020.
[846] Mike Dennis, 'APEC Collaborative Framework for Online Dispute Resolution', APEC Economic Committee ODR Policy Dialogue, 2019, Last accessed 24 August 2020, http://mddb.apec.org/Documents/2019/EC/EC1/19_ec1_012.pdf.
[847] Interview Memo. Dr. Amada Arley. (July 9, 2020). Phone interview.
[848] PROFECO, 'Concilianet - Participating Providers', n.d., Last accessed 24 August 2020, https://concilianet.profeco.gob.mx/Concilianet/proveedores_que_concilian.jsp.

B. Platforms

E-commerce platforms including Amazon, Mercado Libre, Deremate, Groupon and Rappi are registered providers in Concilianet, and thus consumers dissatisfied with the outcomes of private negotiations have the option to pursue an agreement through Concilianet.[849] It seems that such platforms have determined that it is in their best interest to provide this option to maximize customer satisfaction. For example, Amazon reportedly has a good relationship with PROFECO, according to statements from officials, given its internal policy of keeping as many customers inside the platform as possible.

The largest e-commerce platform in Latin America, Mercado Libre, also considers that Concilianet considerably speeds up conciliation procedures and provides an effective option to avoid in-person proceedings or courts. Mercado Libre finds that Concilianet is a helpful source of data on consumer issues to inform efforts to improve the user experience. As the platform also experiences challenges with officers from the small local consumer protection offices of PROFECO, Mercado Libre sees the increasing value of services provided by Concilianet.[850]

Mercado Libre also suggested certain measures that may improve Concilianet (some of which are reflected in the challenges mentioned above), such as:

- PROFECO should work to increase the number of participant providers in the platform through information and advertising campaigns as well as incentivizing businesses to register with Concilianet;
- The human resources of Concilianet should be increased by a significant amount;
- A professionalization plan should be implemented, so the officers handling the procedures strengthen their knowledge in e-commerce matters, to enhance the quality of service which they provide;
- Concilianet's interface should permit a face-to-face interaction between the provider and the consumer.[851]

C. Government: PROFECO

PROFECO faces challenges with certain e-commerce operators who do not proactively cooperate with the agency; this includes large multinational e-commerce companies who are both not registered with Concilianet and often found to be non-compliant with Mexican consumer law.[852] As a solution to these issues, the agency indicated it would work on a "digital stamp" to distinguish which e-commerce platforms were compliant with Mexican consumer

[849] PROFECO, 'Providers that conciliate', n.d., Last accessed 24 August 2020, https://concilianet.profeco.gob.mx/Concilianet/proveedores_que_concilian.jsp.
[850] Interview Memo. Carlos Hassey Artigas, Mercado Libre. (August 10, 2020). Written interview response.
[851] Interview Memo. Carlos Hassey Artigas, Mercado Libre. (August 10, 2020). Written interview response.
[852] Interview Memo. Dr. Amada Arley. (July 9, 2020). Phone interview.

law. This would effectively create a system of reputation for consumers to evaluate platforms.[853]

Conclusion

The experience of PROFECO and Concilianet demonstrates the clear advantages of moving conventional legal and administrative processes for consumer protection and dispute resolution online. From the perspective of consumers and the government, Concilianet provides an alternative to increase access to consumer justice and reduce costs and efforts associated with conventional dispute settlement processes (especially during the COVID-19 pandemic). For e-commerce platforms, Concilianet provides a free option to provide consumer ODR that can increase their reputation as a trustworthy business in addition to the internal ODR mechanism which they may already offer.

Yet, Concilianet also has its limitations. The platform only processes a small number of domestic e-commerce transactions relative to those handled internally by e-commerce platforms such as Amazon and Mercado Libre, and lacks cross-border capabilities. It is clear that e-commerce platforms themselves largely supply the majority of dispute resolution services demanded in the e-commerce market. Thus, the prospect of Concilianet to make a significant impact on the rising number of domestic e-commerce transaction disputes is dependent on increasing its budgetary resources as well as overcoming the challenges identified in this case study.

Key lessons from the case studies on Japan and Mexico

Success factors

Key lessons from Japan's ongoing efforts to promote ODR include:

- Stakeholder engagement efforts surrounding ODR reveal divergent perspectives on certain issues. Stakeholder engagement efforts should be undertaken by governments when considering various ODR options to maximize the likelihood of adoption.
- CCJ was established to address the challenge of cross-border e-commerce disputes. Such cooperation between economies may provide some benefits in overcoming language barriers and differences in legal and commercial customs.
- NCAC's consultative services for consumers in relation to e-commerce disputes are popular, indicating that consumers may benefit from services that assist them to negotiate with vendors and understand their options under consumer law.

Key lessons from Mexico's Concilianet include:

- Concilianet's main benefits stem from the efficiency benefits provided by creating a faster, cheaper, online option for consumer protection proceedings. Public investment

[853] Ivan Nava, 'E-commerce firms are condemned by PROFECO', February 2020, Last accessed 24 August 2020, https://www.merca20.com/alibaba-y-didi-sob-reprobadas-por-la-profeco-algo-que-el-consumidor-podria-usar-en-su-contra/.

in ODR may be justified by the potential for significant improvements over the preexisting consumer protection regime.
- The cooperation of some major e-commerce platforms indicates they perceive benefits in participating in Concilianet, showing that public ODR platforms can play a role in expanding consumer justice while coexisting with private mechanisms.

Challenges and limitations

Key challenges for dispute resolution in Japan include:
- Civil courts in Japan represent a costly and time-consuming option to resolve low-value commercial disputes. Therefore, civil courts under certain circumstances may be poorly equipped to address the challenge of rising e-commerce disputes. ODR may present a favorable option to meet this challenge.
- NCAC lacks data on the impact of increasing disputes in the e-commerce sector. A lack of accessible options for dispute resolution such as ODR may limit visibility into the challenge of e-commerce disputes, while consumers may simply abandon disputes thus depressing expansion of the e-commerce sector.
- The government determined its best option is to support private ODR initiatives. Under these circumstances, governments must consider how costs to finance the system are shared to ensure actors have incentives to participate.
- MSMEs lack the resources to provide ODR. Therefore, government efforts to promote or support the adoption of ODR should consider how such efforts can be inclusive of MSMEs.

Key challenges for PROFECO's ODR platform Concilianet include:
- Legal and regulatory challenges limit consumers' ability to achieve final resolution of disputes if the vendor does not comply. Public-run ODR may be hampered by existing legal and regulatory measures related to consumer protection and limited ability to compel businesses to comply.
- Concilianet's impact is limited by budget and human capital challenges, which may have negative implications on its ability to make significant progress in addressing the challenge of low-value e-commerce disputes.
- Concilianet exclusively processes cases related to large multinational e-commerce platforms. Governments should consider how ODR interventions may improve or exacerbate inequities between larger, mid-sized and small businesses.
- Concilianet faces legal and practical challenges that limit the platform to domestic transactions. Public ODR operated by a single economy may face challenges in addressing the growing volume of cross-border e-commerce disputes.

Potential Solutions

Potential solutions to challenges faced in Japan to resolve e-commerce disputes include:
- A publicly-supported private ODR platform may provide an effective dispute resolution

option in the context of growing e-commerce sales and a legal environment that is ill-equipped for low-value, high-volume transactions.
- The launching of an ODR platform in Japan may lead to the generation of more data on the magnitude of commercial disputes as consumers may be more likely to engage with a system that simplifies the process of seeking a resolution.
- Declining engagement with civil litigation and a lack of digitization in court proceedings creates an opportunity for ODR to greatly reduce the cost, time and effort required for consumers and businesses alike to access dispute resolution.

Potential solutions to challenges faced by Concilianet include:
- AI represents a promising option for addressing the aforementioned human capital costs in various stages of the Concilianet process. The ability of public-run ODR platforms to address increasing e-commerce disputes may require investment in automated systems.
- Legal and regulatory reforms in Mexico could provide PROFECO agreements with legal enforceability and binding status, highlighting the importance of a supportive legal and regulatory environment for ODR.

Concluding remarks

Consumer ODR may be a promising policy option for APEC economies to address the growth of e-commerce transactions. The experiences of Japan and Mexico reveal common challenges, the impact of various policy options, and the role of ODR in cross-border e-commerce.

However, features of the e-commerce sector such as high-volume, low-value cross-border transactions create challenges for ODR. Mexico's Concilianet has a limited impact on e-commerce given that major international e-commerce companies handle the vast majority of disputes, while PROFECO lacks the human resources to do so. In Japan, consumers have a high degree of trust in the dispute resolution services provided by major e-commerce platforms and the government currently lacks the tools and capacity to deliver speedy resolution of low-value disputes. Meanwhile, officials from both governments have expressed the view that internal ODR mechanisms offered by e-commerce platforms are insufficient from a consumer justice standpoint. Experts on ODR have raised the potential of AI as a tool to address cost-related challenges by automating various tasks; officials in Mexico have spoken regarding future plans to automate portions of the Concilianet process, while Japan's ODR efforts include significant attention to AI.

Public investment in ODR must also consider the variety of practical and legal challenges posed by cross-border transactions. Concilianet lacks the legal authority and resources to handle cross-border disputes. Both economies have introduced programs (Japan's CCJ and Mexico's CARE) to address a small number of cross-border disputes. However, it is difficult to draw conclusions from these efforts due to the small number of claims. Given these challenges, ODR efforts that are the initiative of a single economy may largely be relegated to

transactions between domestic parties. Therefore, APEC economies interested in addressing the barriers to growth in cross-border e-commerce may consider international cooperation to work towards a cross-border ODR platform for low-value disputes. Within APEC, the Collaborative Framework for Online Dispute Resolution of Cross Border Business-to-Business Disputes may provide an effective venue for this. Economies may consider participating in the effort and opting-in to the APEC ODR Framework in order to advance discussions on a truly international ODR framework that may eventually provide an effective option for cross-border disputes.

5.4 FOCUS AREA D: CYBERSECURITY / NETWORK SECURITY

OVERVIEW

There are several ways in which cybersecurity intersects with and underpins e-commerce. The fundamental connection is the secure protection of personal information and sensitive business records. Customers rightly expect their information will be protected from unauthorized disclosure. From this expectation, and some public skepticism as breaches become public news, there is a risk of loss of trust and consumer confidence. Businesses too require the protection of their digital assets, including business records and trade secrets (and other IPRs). Further, as more devices—products—small and large, get connected to the Internet, there are two consequences, first, consumers will want to understand how they will be able to trust these innovations, what information will be collected and how it will be protected. Second, new 'access points' are created, resulting in vulnerabilities to business computer systems.

Governments and the private sector share the responsibility to protect citizens and the economy from cybersecurity risks. Developers and manufacturers are aware of the importance of consumer trust, and understand that network security, cybersecurity more generally (e.g., business security), and product safety (which can be undermined by a cyberattack) are essential components to building that trust. Historically, the private sector has often led in the development of best practices, standards and methods of ensuring greater cybersecurity, and in many cases, these have been adopted by governments as guidance or requirements. This paradigm of private sector leadership can be illustrated in several different contexts:

- In Chile, private sector expertise is brought to bear to help the government to develop its cybersecurity strategy and government capacity;
- In Japan, the private sector cybersecurity activity is organized across industries and complements the government's efforts to create a legal framework; and
- In the United States, the private sector works hand in glove with the government, developing cyber-response capabilities, a cybersecurity framework adaptable to any business or enterprise, and collaborative exercises to test capacity and resilience.

The common thread across these contexts is the recognition that adopting technical standards and good practices developed by the private sector is a good approach to cybersecurity for any economy. A benefit of referencing industry practices over government-developed technical

regulatory requirements has been the agility with which industry can adapt to constantly changing threat landscapes. Furthermore, commonly adopted standards and practices enable more consistent compliance from economy to economy, maintaining the highest standards for security. These case studies closely examine several government initiatives and private-sector led initiatives to illustrate how critical it is for governments to engage with the private sector on cybersecurity.

Key Issues

Cybersecurity underpins all activities on the Internet—whether business operations of an e-commerce website, the transactions conducted from point of sale to the customer, or the management of logistics—all are susceptible to cybersecurity threats. Governments and every industry must take defensive measures, employ sufficient resources trained in cybersecurity, and ensure all employees are sensitive to their role in protecting their employer from cyberattacks.

These case studies will examine these issues through the following lenses:

- **Private sector leadership:** Examining data governance and cybersecurity measures; public-private-partnerships (PPP); and the talent gap. This is exemplified by economies such as the United States, where the private sector has contributed to efforts by the public sector to update and maintain high standards of cybersecurity.
- **Public sector activities, supported by the private sector:** Encompassing cybersecurity laws and public policy issues; and development of a resilient society and economy. In addition, the private sector has demonstrated capacity and capabilities to support and inform public sector activities, or in some cases, lead reforms and capacity building. The example of Chile has been informative, with the government enlisting the expertise of private sector firms to formulate and implement over-arching plans for cybersecurity.
- **Changing threat landscape:** Impact on cybersecurity in the new paradigms of mobile devices and remote working, Internet of Things (IoT) such as autonomous vehicles, smart cities and smart health devices. These innovations are radically expanding the threats by opening up numerous vulnerabilities. In many cases, the relevant industries are not prioritizing cybersecurity as they bring new products to market. Some governments are enacting laws to elevate cybersecurity as a concern and area for investment and resources for IoT developers. Efforts by economies such as Japan and the United States to enshrine cybersecurity principles, information sharing and capacity building into legislation are important steps in developing resilience to new and unexpected threat scenarios.

CASE STUDIES

Chile

Beginning in 2016, in pursuit of improving cybersecurity, Chile looked to resources within government to enact laws and develop a cybersecurity strategy. After a highly publicized breach in 2018, the government, with Inter-American Development Bank (IDB) support, engaged an Israel-based cybersecurity consulting firm, Toka, to guide their efforts. Toka began a process of accelerating government capacity building and supporting government efforts to enact a cybersecurity law and other legal reforms to protect critical infrastructure and society as a whole. The process of improving Chile's cybersecurity capacity has been interrupted by internal political dynamics as well as the COVID-19 constraints on travel and meetings, but is expected to resume in early 2021.

Public-Private Partnerships

Significant amounts of sensitive information and critical infrastructure is controlled by the private sector across all economies. In some, the private sector—including both domestic operators and multinational corporations (MNCS)—have greater capacity, agility and expertise to address the dynamic and challenging cybersecurity landscape. In other cases, as in the case of Chile, private sector expertise is necessary to guide the development of effective public sector cybersecurity strategies. Often, such efforts can include capacity building for the government. Thus, there are opportunities to cultivate collaborative, mutually beneficial partnerships between the public and private sectors.

Toka selected by Chile and IDB to bolster cybersecurity effort

In 2017, the Government of Chile's Inter-ministerial Committee on Cybersecurity, comprised of government stakeholders and representatives from critical infrastructure sectors such as banking and energy, issued the 'National Cybersecurity Policy 2017-2022' (Cybersecurity Policy) in which it set out a cybersecurity framework to support the government's 'Digital Agenda 2020'.[854]

In mid-2018, a major cyberattack on the Banco de Chile occurred resulting in losses of USD10m due to fraudulent SWIFT wire transfers.[855] The theft occurred as the bank was dealing with disruptions across hundreds of workstations and servers.[856] Such SWIFT-related

[854] Government of Chile, 'National Cybersecurity Policy (NCSP) 2017-2022', 2017, https://www.ciberseguridad.gob.cl/media/2017/05/NCSP-ENG.pdf see also, Interview with Nir Peleg, VP Technology & Global Services, Toka, 8/3/20 (Toka Interview) .

[855] We Live Security, 'Chile to revolutionize cybersecurity after the recent cyberattack', 2018, https://www.welivesecurity.com/2018/06/14/chile-revolutionize-cybersecurity-cyberattack/.

[856] Bank Info Security, 'Banco de Chile Loses $10 Million in SWIFT-Related Attack', 2018, https://www.bankinfosecurity.com/banco-de-chile-loses-10-million-in-swift-related-attack-a-11075.

thefts date back to 2013, with more recent incidents in the Philippines (undisclosed bank and loss) and Viet Nam (USD1m).[857] With public pressure on the Chilean government and the banks to improve security—and on SWIFT to do similarly or remove the bank from the SWIFT international network[858]—Chile committed to accelerate implementation of the Cybersecurity Policy, which had made limited progress, but lacked full institutional support.[859] Most importantly, this event raised the priority of the cybersecurity due to media attention and resulting high-level government discussion. In many cases, large-scale cyber incidents create increased awareness to the gaps and new priorities to invest in cybersecurity.[860]

In the immediate aftermath of the 2018 incident, the Superintendent of Banks and Financial Institutions (SBIF) conducted an investigation of the incident and took steps to amend banking regulations regarding notification to SBIF of operational incidents.[861] In July 2018, the Treasury Minister announced a financial cybersecurity bill, followed soon after by the government's announcement of the intention to establish a broader cybersecurity bill for critical infrastructure.[862]

By May 2019, Toka, an Israeli cybersecurity consulting firm who has extensive experience developing cybersecurity capacity for governments, was selected by the Government of Chile and the IDB to advise Chile on expedited development of the economy's cybersecurity readiness and operational capacity.[863]

As a first step, Toka assessed current cybersecurity readiness and the challenges in Chile. Building on the process that developed the Cybersecurity Policy, Toka started by looking to identify key government stakeholders who had a good understanding of the cybersecurity domain.[864] Through this cadre of professional, interested and capable government stakeholders,

---

[857] Bank Info Security, 'Vietnamese Bank blocks $1 Million SWIFT Heist', 2016, https://www.bankinfosecurity.com/vietnamese-bank-blocks-1-million-online-heist-a-9105; Business Times, 'Symantec says Swift heist linked to Philippines attack', 2016, Sony hack, https://www.businesstimes.com.sg/banking-finance/symantec-says-swift-heist-linked-to-philippines-attack-sony-hack.

[858] Bank Info Security, 'Banks with Bad Cybersecurity Could Face SWIFT Justice', 2016, https://www.bankinfosecurity.com/blogs/banks-bad-cybersecurity-could-face-swift-justice-p-2145?highlight=true.

[859] Bloomberg, 'Toka Selected by Chile and Inter-American Development Bank to Access and Support Chile's National Cybersecurity Readiness', 2020, https://www.bloomberg.com/press-releases/2020-05-19/toka-selected-by-chile-and-inter-american-development-bank-to-assess-and-support-chile-s-national-cybersecurity-readiness.

[860] TRPC Interview (3 August 2020 and 18 August 2020) Nir Peleg, Vice President, Technology & Global Services, Toka.

[861] Compilation of Regulations ('the RAN'), in chapters 20-8 on Information on Operational Incidents and Database of Cybersecurity Incidents and 1-13 on the Classification of Management and Solvency. Hipervinculos (2018) Forced landing: an overview of Chilean legislation on financial cybersecurity, https://www.hipervinculos.cl/en/forced-landing-an-overview-of-chilean-legislation-on-financial-cybersecurity/#new_tab?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration.

[862] Hipervinculos, 'Forced landing: an overview of Chilean legislation on financial cybersecurity', 2018, https://www.hipervinculos.cl/en/forced-landing-an-overview-of-chilean-legislation-on-financial-cybersecurity/#new_tab?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration.

[863] Bloomberg, 'Toka Selected by Chile and Inter-American Development Bank to Access and Support Chile's National Cybersecurity Readiness', 2020, https://www.bloomberg.com/press-releases/2020-05-19/toka-selected-by-chile-and-inter-american-development-bank-to-assess-and-support-chile-s-national-cybersecurity-readiness.

[864] TRPC Interview (3 August 2020) Nir Peleg, Vice President, Technology & Global Services, Toka.

the process initially sought to educate key government decision makers on the scope of the challenges and the need for both a clear strategy and a sustained effort to build government cybersecurity capacity. It was essential from Toka's perspective that decisions that require significant changes and adaptations at an economy-wide level, such as establishing a new governance model, updating the laws and capacity building require a top-down approach. This approach would enable a leading cyber transformation process that will eventually lead Chile to be a lean-forward cyber resilient regional leader.[865]

Toka highlighted in particular the necessity of the cybersecurity law in mobilizing government resources to fully execute any strategy the government envisioned. The government has thus more aggressively pursued drafting a new bill—though progress has stalled due to internal discussion and priorities and the forthcoming Chilean Plebiscite.

The lead ministry working with Toka, bearing responsibility for establishing a new governance framework, is the Ministry of the Interior and Public Security (MIPS), with the Ministries of Finance (MOF) and Defence (MOD) also engaged.[866] MIPS is the coordinating ministry for cybersecurity, while the MOF and MOD are consulting for more specific applications to do with financial crimes and advanced persistent threats, respectively.

Involved to a lesser degree are representatives from critical infrastructure sectors, Chile's Central Bank, and the Chilean Senate and House of Representatives.[867] The Chilean Central Bank's involvement is directly related to the government's increased focus on cybersecurity in the finance industry in light of the 2018 incident, while the Senate and House are involved in knowledge-sharing efforts designed to get lawmakers up to speed on cybersecurity issues.

Once there is clarity around governance, efforts will turn to practical capacity building. Beyond bringing decision makers on board, as has been done, there is need for a framework of common language to communicate information about cybersecurity across the government and industry. There remains work to be done to implement and assimilate a common language framework for cyber information sharing and crisis management. The framework should be derived from leading international standards, best practices and platforms. This is especially important for communication among critical sectors as well as between these sectors and the public sector (e.g., regulators, CSIRT).[868]

Again noting the importance of laws in establishing frameworks and generating momentum for wider systemic change, Chile has been advised to amend laws to enable information sharing about incidents between commercial enterprises and government agencies. Communication of

[865] TRPC Interview (3 August 2020) Nir Peleg, Vice President, Technology & Global Services, Toka.
[866] TRPC Interview (3 August 2020) Nir Peleg, Vice President, Technology & Global Services, Toka.
[867] Jones Day, 'Global Privacy & Data Security Update Vol.9', 2018, https://www.jonesday.com/en/insights/2018/10/jones-day-global-privacy--data-security-update--vo?RSS=true&utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration.
[868] TRPC Interview (19 August 2020) Nir Peleg, Vice President, Technology & Global Services, Toka.

incidents may be constrained by current banking, consumer and competition law or privacy and data protection laws, and exceptions for information sharing will be essential to preventing future incidents.[869] Receptivity to such approaches has been positive, though, progress has again been stalled by domestic political dynamics.

Looking ahead, with a cybersecurity law in place, government capacity established, and laws reformed as needed, Chile will be situated to consider the greater cybersecurity ecosystem, for the private sector and academia. For example, to maintain adequate capacity within government agencies and across the private sector, academia must develop curriculums to produce students skilled in cybersecurity. Furthermore, businesses beyond the critical infrastructure sectors will need to identify risks and introduce cybersecurity measures to address those risks.

Box 5.14: Brunei Darussalam's Cooperative Agreement with Microsoft

Consulting to government is one approach in which the private sector brings expertise to help governments address cybersecurity. In other cases, such as Brunei Darussalam, major private sector companies work directly with government to enhance the government's ability to address cyberthreats. In Brunei Darussalam, ITPSS Sdn Bhd is a private cybersecurity company who has been providing cybersecurity capacity and expertise to the government and others since its founding in 2003.[870] In 2010, Microsoft and ITPSS entered a security cooperative agreement to establish a joint Security Cooperation Program (SCP) to provide a structure for ITPSS and Microsoft to engage with the government of Brunei Darussalam to address cyberthreats to domestic security.[871] ITPSS operates the Brunei Computer Emergency Response Team (BruCERT) under the auspices of the government's IT Protective Security Sdn Bhd in collaboration with the Internal Security Department as an interim cyber security center. Microsoft provides threat information to ITPSS to help the government secure critical infrastructure and sensitive data, such as geographic data related to the oil and gas industries.[872] The cooperative agreement was renewed in 2014 and continues to be in effect.[873]

Brunei Darussalam continues on its journey of improving government capacity to address cybersecurity. In January 2020, Ministry of Transport and Infocommunications (MTIC) announced the formation of the government's new cybersecurity agency, Cyber Security Brunei (CSB).[874] CSB is in its infancy and the SCP will assist in developing and organizing

[869] TRPC Interview (3 August 2020) Nir Peleg, Vice President, Technology & Global Services, Toka.
[870] IT Protective Security Services Sdn Bhd (ITPSS), https://itpss.com/
[871] Microsoft, 'Security Cooperation Program to protect Brunei from cyber threats', 2014, https://news.microsoft.com/apac/2014/02/19/msftitpss/
[872] TRPC Interview (13 August 2020) Afif Mohamed Ali, Country Managing Director, Brunei Darussalam, Microsoft
[873] TRPC Interview (13 August 2020) Afif Mohamed Ali, Country Managing Director, Brunei Darussalam, Microsoft
[874] ITPSS, 'National Cyber Security Agency to be Formed, Says MTIC Minister', 2020, https://www.itpss.com/News/2020/10012020.html

capacity to take on the growing cybersecurity role. CSB will underpin the recently announced Digital Economy Masterplan 2025, which supports the objectives of Brunei Darussalam's Wawasan 2035 (Vision 2035), to improve the quality of life, provide for a highly educated and skilled workforce and a dynamic, sustainable economy.[875] As the government expands capacity to address cybersecurity, it is expected that the public sector will continue a collaborative role as it does in even the most developed economies.

Conclusion

There are generally two possible reasons a government will seek to establish a cybersecurity framework: (i) either a government's leadership recognizes the need to address cybersecurity, for example, to lay the foundations for a digital-ready society or digitalized economy, or (ii) the government finds itself with an urgent need to respond to an incident. As in Chile initially, the government recognized the potential risks and the need to be prepared for threats as they developed their digital agenda for the economy. Yet it wasn't until a triggering event—the theft from Banco de Chile—that the government sought to aggressively address the challenges. As the Toka consultant observed, it is best to be proactive and prepared; to set priorities, develop the appropriate governance model and practical capacities to meet the most immediate needs first.[876] It is one thing to proclaim in a document the need to be cyber-ready, it is another thing entirely to have the leadership, the laws and the resources to meet the need for cybersecurity.[877] The greatest risks are to critical infrastructure and government, and the question is not if, but when there will be an attack.[878] In almost all circumstances, the private sector can contribute to the ability of an economy to address the cybersecurity. The question for each economy's government is what type of assistance and cooperation best suits their needs.

Japan

Japan has set its social agenda to achieve 'Society 5.0,' defined as a "human-centered society that balances economic advancement with the resolution of social problems by a system that highly integrates cyberspace and physical space."[879] This transformation is intended to address the challenges to economic growth presented by having the largest aging population among

[875] The Scoop, 'Gov't Releases First Digital Economy Masterplan', 2020, https://thescoop.co/2020/06/05/govt-releases-first-digital-economy-masterplan/, see also Digital Government strategy 2015-2020, http://www.digitalstrategy.gov.bn/Themed/index.aspx.

[876] TRPC Interview (3 August 2020) Nir Peleg, Vice President, Technology & Global Services, Toka.

[877] Jones Day, 'Global Privacy & Data Security Update Vol.9', 2018, https://www.jonesday.com/en/insights/2018/10/jones-day-global-privacy--data-security-update--vo?RSS=true&utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration.

[878] Jones Day, 'Global Privacy & Data Security Update Vol.9', 2018, https://www.jonesday.com/en/insights/2018/10/jones-day-global-privacy--data-security-update--vo?RSS=true&utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration.

[879] Cabinet Office, 'Society 5.0', https://www8.cao.go.jp/cstp/english/society5_0/index.html.

world economies.[880] Japan has been on a rapid journey building its cybersecurity to underpin this objective. Compounded with the urgency of the pending Tokyo Olympics, both government and industry are working hard to address cybersecurity needs and challenges.[881] Japan began by developing laws specific to addressing cybersecurity to fill gaps in the computer crime laws or criminal code and consolidate legal authorities. Further, because cybersecurity is a rapidly evolving area both in terms of threats and solutions, requires relatively specialized skills, and has impact on all sectors, it is of utmost importance to build government and private sector capacity.[882]

Cybersecurity Laws Fill the Gaps of Traditional Criminal Laws

For many years, governments relied on laws addressing criminal conduct implicating computers. To address evolving threats, governments are criminalizing cyberattacks with more specificity.[883] New cybersecurity laws are more expansive in scope and precise in language, addressing malicious activities that may not previously have fallen under criminal law. The challenge is complex, but governments are stepping up by developing new enforcement mechanisms.

In Japan, illegal access to electronic data is criminalized under the 1999 Act on the Prohibition of Unauthorized Computer Access (UCAL), along with other forms of hacking, phishing and malware propagation. [884] Other forms of data falsification, misuse or destruction are criminalized under Japan's Penal Code Act of No. 45 of 1907.[885] Theft of trade secrets and IP through illegal means such as cyberattacks is penalized under Japan's Unfair Competition Prevention Act.[886]

However, between 2011 and 2013, cyberattacks on major Japanese defense contractor Mitsubishi Heavy Industries resulted in the possible theft of nuclear power plant, submarine and missile designs.[887] In May 2013, login credentials of 22 million Yahoo! Japan (which is co-owned by network provider Softbank) users were leaked.[888]

---

[880] TRPC Interview (26 August 2020) MNC in Japan.
[881] TRPC Interview (26 August 2020) MNC in Japan.
[882] TRPC Interview (27 August 2020) Telecoms Company.
[883] Cyber Experts, 'Cybersecurity Laws – A Complete Overview', 2020, https://cyberexperts.com/cybersecurity-laws/
[884] Japanese Law Translation, 'Act on Prohibition of Unauthorized Computer Access [Act No.128 of Aug 13 1999]', 2020, http://www.japaneselawtranslation.go.jp/law/detail/?re=02&dn=1&x=0&y=0&co=1&ia=03&ja=04&yo=&gn=&sy=&ht=&no=&bu=&ta=&ky=computer+access&page=79.
[885] UNODC, Penal Code [Act No. 45 of 1907], 2006, https://www.unodc.org/res/cld/document/penal-code-japan_html/Japan_Penal_Code_1907_As_Amended_2006.pdf.
[886] Japanese Law translation, 'Unfair Competition Prevention Act [Act No.47 of May 19 1993]', 2020, http://www.japaneselawtranslation.go.jp/law/detail/?re=02&dn=1&x=59&y=14&co=1&ia=03&ja=04&yo=&gn=&sy=&ht=&no=&bu=&ta=&ky=unfair+competition+prevention+act&page=22.
[887] Info Security, 'Major cyberattack on Mitsubishi involving nuclear power plant data', 2011, https://www.infosecurity-magazine.com/news/major-cyberattack-on-mitsubishi-involving-nuclear/ and Yahoo Finance , 'Japan its own enemy in cybersecurity', 2016, https://au.finance.yahoo.com/news/japan-own-enemy-cybersecurity-010124267.html.
[888] Dark Reading, 'Yahoo Japan Data Breach: 22M Accounts Exposed', 2013, https://www.darkreading.com/attacks-and-breaches/yahoo-japan-data-breach-22m-accounts-exposed/d/d-id/1110035.

These incidents resulted in Japan recognizing the need for a whole-of-economy approach to cybersecurity in the face of growing domestic and international cyberthreats and the growth of Internet-related industries. It thus passed the Basic Act in 2014, establishing a framework for developing and enforcing cybersecurity across both the public and private sectors. In the introductory preamble to the 2015 Cybersecurity Strategy, the rationale for the Basic Act is to address emerging threats to national safety and security, business operators and governmental bodies which might provide critical infrastructure, as well as maintaining the free flow of information in light of the escalation in persistence of cyber threats.[889] A key feature of the Act is that in which the government establishes a cross-government ministry to address the cybersecurity within government and enforce the law across society.[890]

Box 5.15: Japan's 2014 Basic Act on Cybersecurity

The Basic Act provides a framework for collaboration among government agencies on cybersecurity. The key provisions recognize the need for both top-down national level policy development as well as regional and sectoral engagement—especially in the case of providers of critical infrastructure. The creation of a coordinating body charged with formulating overall strategy also reflects a recognition of the need for intradepartmental communication, though the ultimate lack of enforcement capabilities within the Act limits overall effective implementation.

- Articles 4-5: Allocates responsibility for overall policy formation on comprehensive cybersecurity policies to the national government, while also calling on local governments to formulate and implement local cybersecurity requirements—in alignment with the economy-wide laws.
- Article 12: Requires that providers of critical infrastructure and cyberspace-related businesses develop adequate knowledge and capacity regarding cybersecurity under a government developed Cybersecurity Strategy.
- Article 24: Creates an enforcement agency, the Cybersecurity Strategic Headquarters (CSH), directly answerable to the Cabinet. The CSH is charged with the preparation of the Cybersecurity Strategy and setting standards for, and promoting adoption of, cybersecurity measures to be taken by government agencies.

Source:

- Japanese Law Translation (2015) The Basic Act on Cybersecurity [Act No. 104 of November 12, 2014], http://www.japaneselawtranslation.go.jp/law/detail/?printID=&re=02&vm=02&id=2760&lvm=01

To meet the needs to secure the planned Olympics anticipated for Japan in 2020, the government recognized the need to orchestrate public- and private-sector collaboration on

[889] NISC, 'Cybersecurity Strategy 2015', 2015, https://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf.
[890] TRPC Interview (27 August 2020) Telecoms Company.

cybersecurity.[891] Of particular concern was the increased logistical burden Japan's critical infrastructure would face in light of the influx of tourism anticipated during this period, as well as the precise cross-industry coordination necessary to allow for the smooth security operation and broadcast of the events.[892] Concerns were raised regarding the need to address vulnerabilities created by gaps in existing information-sharing regimes.

To accommodate this, amendments were passed to the Basic Act in 2018 to provide for the creation of a cybersecurity council comprised of representatives from government, critical infrastructure service providers, academia and industry.[893] The council's purpose is the facilitation of information transmission across participating agencies. It was also recognized by government that to instill confidence it was important to work with the international cybersecurity community.[894]

The Cybersecurity Strategy first published in 2015 has been updated in 2018 to reflect technological and economic developments such as the increasing interconnectedness of cyberspace and 'real space' in industries such as transport, e-government, healthcare and manufacturing, due to the proliferation of automation and the Internet of Things (IoT).[895] The government plans to update the Strategy every three years and amendments to the 2015 Strategy were opened for public consultation prior to their implementation.[896] Specific input from companies, individuals and other entities regarding proposed amendments were integrated where deemed appropriate in the government's review of comments.[897]

Japan also introduced tax incentives to spur investment in cybersecurity and IoT.[898] Entities which acquire cybersecurity-related assets can claim tax credits worth 3 percent of the cost of acquiring the assets, and may access additional special depreciation of 30 percent of acquisition costs. These incentives are available across all industries and sectors.

Further, in 2018, the Telecommunications Business Act (TBA) which is the telecommunications industry law that protects the privacy of telecommunications, was amended to allow carriers to share with other carriers information on sources of cyber-attacks

[891] Gov Insider, 'Japan sets up cybersecurity council to secure the 2020 Olympics', 2019, https://govinsider.asia/connected-gov/japan-sets-up-cybersecurity-council-to-secure-the-2020-olympics /.
[892] TRPC Interview (26 August 2020) MNC in Japan.
[893] Gov Insider, 'Japan sets up cybersecurity council to secure the 2020 Olympics', 2019, https://govinsider.asia/connected-gov/japan-sets-up-cybersecurity-council-to-secure-the-2020-olympics /.
[894] Gov Insider, 'Japan sets up cybersecurity council to secure the 2020 Olympics', 2019, https://govinsider.asia/connected-gov/japan-sets-up-cybersecurity-council-to-secure-the-2020-olympics /.
[895] NISC Japan, 'Summary of the Japan's Cybersecurity Strategy', 2018, https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-shousaigaiyou-en.pdf.
[896] TRPC Interview (26 August 2020) MNC in Japan.
[897] One trust Data Guidance, 'Japan: NISC Releases draft cybersecurity strategy for public consultation', 2018, https://www.dataguidance.com/news/japan-nisc-releases-draft-cybersecurity-strategy-public-consultation; NISC, Cybersecurity Strategy Headquarters Meeting Summaries, 2018, https://www.nisc.go.jp/conference/cs/index.html#cs19.
[898] PwC, 'IT Investment Incentive for "Connected Industries', 2018, https://www.pwc.com/jp/en/taxnews/pdf/jtu-20180821-en-138.pdf.

through a mechanism utilizing the ICT Information Sharing and Analysis Center Japan. This is a step toward overcoming the cultural reluctance to share information about attacks for fear of blame.[899]

Capacity Building and Addressing Cultural Challenges

Japan initially addressed the widely acknowledged vulnerability of its private sector to cyber-threats through law and public policy. Yet a 2016 report by Japan's Ministry of Economy, Trade and Industry (METI) identified a shortage of IT professionals (capable engineers, cyber experts, and security manager) at 132,060, which was expected to increase to 193,010 in 2020.[900] It was apparent there was a capacity and skills issue for Japan's government and industry to which industry had to respond, most importantly, in the field of cybersecurity.[901] Japan's National Center for Incident Readiness and Strategy for Cybersecurity (NISC) guides all central government agencies in establishing and implementing cyber security policies and measures. NISC announced its National Strategy for Cyber Security 2018 which identifies an urgent need for reinforcing cybersecurity measures in all levels of Japanese society and in all aspects of technological development.[902]

Public reportage suggested that data breaches went unaddressed due to the cultural tendency of employees to fear punishment for harming the reputation of their employer.[903] Further, Japan's business culture presented challenges to ensuring that workers understood and stayed current on cybersecurity threats, risks and solutions. Japanese workers generally enjoy lifetime employment, rotating jobs every 2-3 years. Many Chief Information Security Officers (CISOs) are thus dual-hat and lack backgrounds in cybersecurity. Only 28 percent of IT professionals work in-house in Japan, whereas 65 percent do so in the US and 54 percent in the UK.[904] Most Japanese companies outsource their IT and cybersecurity functions to system integrators.[905] Industry recognized that cybersecurity for Japan would depend on an improved cybersecurity ecosystem involving all industries, and businesses large and small.[906] To support these efforts, the government has offered subsidies to companies for cybersecurity reskilling.[907]

---

[899] The Japan Times, 'Japan gropes for cybersecurity solution as victims suffer in silence', 2017, https://www.japantimes.co.jp/news/2017/01/15/national/japan-gropes-cyberattack-solution-victims-suffer-silence/.

[900] United States International Trade Administration, Japan-Cybersecurity, https://www.export.gov/apex/article2?id=Japan-Cyber-Security.

[901] TRPC Interview (26 August 2020) MNC in Japan.

[902] Japan's National Center for Incident Readiness and Strategy for Cybersecurity (NISC), 'National Strategy for Cyber Security', 2018 https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf.

[903] Yahoo, 'Japan its own enemy in cybersecurity', 2016, https://au.finance.yahoo.com/news/japan-own-enemy-cybersecurity-010124267.html.

[904] Eurasia Review, 'Cybersecurity Framework: Addressing Japan's Manpower Crunch-Analysis', 2020, https://www.eurasiareview.com/30012020-cybersecurity-framework-addressing-japans-manpower-crunch-analysis/.

[905] NIST, 'Success Story: Japanese Cross-Sector Forum', 2018, https://www.nist.gov/cyberframework/success-stories/japanese-cross-sector-forum.

[906] TRPC Interview (27 August 2020) Telecoms Company.

[907] TRPC Interview (27 August 2020) Telecoms Company. See also, Ministry of Education, Culture, Sports, Science and Technology (MEXT) budget plan at https://www.mext.go.jp/en/unesco/mext_00002.html.

Although the structure of IT resourcing in Japan differs from the United States significantly, the IPA published a Japanese translation of the United States' National Institute of Standards and Technology (NIST) Cybersecurity Framework in 2014 to enable Japanese companies to adopt the framework for themselves.[908]

With the awareness of the urgency to address capacity issues, many companies stepped up to work with academic institutions, as well as within their companies, to develop cybersecurity professional training and broader cybersecurity education and re- and up-skilling development programs.[909] Japan's federation of businesses, the Keidanren, characterized the challenge as being a problem for all industries, not only the information technology sector.[910] With the view that industry should focus on supply chain, and understand that the chain is only as strong as its weakest link, in 2015, NTT, NEC Corporation and Hitachi, Ltd. established the Cross-Sector Forum (CSF) to spark the creation of an ecosystem to educate, recruit, retain, and train cybersecurity professionals in collaboration with academia and government.[911] The objective was to build cybersecurity capacity for all sectors, a pool of experts that could fill cybersecurity roles, to improve the knowledge of the respective industry's workers through upskilling, and improve top management understanding of cybersecurity needs for their businesses.[912] The CSF worked with the NIST Cybersecurity Framework, along with NIST's National Initiative for Cybersecurity Education (NICE)[913] Framework to identify and catalog the skills that would be required and worked with experts in education and skilling to build cybersecurity capacity in Japan. The program, initially founded by three technology companies, grew to include over 40 major critical infrastructure companies from the energy, chemical, financial, manufacturing, media, and transportation sectors.[914] These companies are working to upskill their workers and with academic institutions, provide the broader society cybersecurity curriculum.[915] To support these efforts, the government offered subsidies to companies for the reskilling and to students pursuing an academic career in cybersecurity.[916]

As noted, the imminent 2020 Tokyo Olympics created urgency to improve cybersecurity.[917] The CSF sought to address capacity challenges as a first step towards improving Japan's overall cybersecurity readiness, harnessing the NIST Cybersecurity Framework and NICE to identify the roles and job-types needed.[918] The CSF then worked with academia and government to

[908] IPA, 'Framework for Improving Critical Infrastructure Cybersecurity', 2018, https://www.ipa.go.jp/files/000071204.pdf and Eurasia Review, 'Cybersecurity Framework: Addressing Japan's Manpower Crunch-Analysis', 2020, https://www.eurasiareview.com/30012020-cybersecurity-framework-addressing-japans-manpower-crunch-analysis/.
[909] TRPC Interview (26 August 2020) MNC in Japan.
[910] TRPC Interview (27 August 2020) Telecoms Company.
[911] TRPC Interview (27 August 2020) Telecoms Company.
[912] TRPC Interview (27 August 2020) Telecoms Company.
[913] NIST - National Initiative for Cybersecurity Education (NICE), https://www.nist.gov/itl/applied-cybersecurity/nice.
[914] TRPC Interview (27 August 2020) Telecoms Company.
[915] TRPC Interview (27 August 2020) Telecoms Company.
[916] TRPC Interview (27 August 2020) Telecoms Company.
[917] TRPC Interview (26 August 2020) MNC in Japan.
[918] Eurasia Review, 'Cybersecurity Framework: Addressing Japan's Manpower Crunch-Analysis', 2020, https://www.eurasiareview.com/30012020-cybersecurity-framework-addressing-japans-manpower-crunch-analysis/.

develop university cybersecurity programs and curricula. This focus on capacity building is being recognized internationally as the CSF has shared its experiences in developing Japan's talent.[919]

As successful as these programs are at moving people into more advanced educational opportunities, and ultimately into the cybersecurity workforce, the enormous and growing talent gap continues to undermine enterprises' ability to defend against rapidly evolving cybersecurity threats.[920] It has been recognized that the private sector cannot meet the challenge alone.[921] Industry, governments and academia must step up efforts to develop and scale up efforts to proliferate curricula, skills development and the hiring of cybersecurity talent.

Conclusion

Japan has taken an aggressive approach to rapidly improve the economy's cybersecurity, both to advance Society 5.0 and particularly in light of the planning for the Tokyo Olympics in 2020.[922] Government first established the appropriate laws and a framework for cooperation and strategy leadership among stakeholders and subsequently addressing capacity and cultural issues. Although government and industry are moving rapidly to develop their cybersecurity capacity, challenges remain, as evidenced by significant high-profile incidents in the past two years. From this experience, it is clear that capacity building is more challenging than developing laws and policies, and yet, is fundamental to ensuring a more secure cyber environment. In light of the rapidly evolving, global and pervasive nature of modern cyber threats, ideally all businesses need to have some cybersecurity expertise, and all employees—indeed, all citizens—need to become more aware of cyber-hygiene, the measures taken by individuals to protect themselves and their organizations from cyberthreats.

As governments consider restarting economies across the globe after the COVID-19 pandemic, many unemployed people are now able to reskill, while those moving into the workforce for the first time must be able to move into new types of positions.[923] An opportunity exists to use economic recovery efforts to address longer-term needs for cybersecurity skills and capacity.

---

[919] Eurasia Review, 'Cybersecurity Framework: Addressing Japan's Manpower Crunch-Analysis', 2020, https://www.eurasiareview.com/30012020-cybersecurity-framework-addressing-japans-manpower-crunch-analysis/ https://www.sipri.org/sites/default/files/2018-04/integrating_cybersecurity_0.pdf, see also, https://www.eurasiareview.com/30012020-cybersecurity-framework-addressing-japans-manpower-crunch-analysis/.

[920] TRPC Interview (27 August 2020) Telecoms Company.

[921] The New York Times, 'The Pandemic Has Accelerated Demands for a More Skilled Force Work Force', 2020, https://www.nytimes.com/2020/07/13/business/coronavirus-retraining-workers.html.

[922] TRPC Interview (27 August 2020) Telecoms Company.

[923] Several more detailed definitions are available at, Singapore CSA (2029), Internet of Things Security Landscape Study, https://www.csa.gov.sg/news/publications/iot-security-landscape, (This document, the IoT Security Landscape, was jointly commissioned by the Cyber Security Agency of Singapore and the Ministry of Economic Affairs and Climate Policy of the Netherlands. The report provides an in-depth review of the IoT cybersecurity landscape in 2019, and provides several important recommendations, including the need for more uniform adoption of standards for IoT and harmonization of standards (supported by global research); the need for labels and certifications to inform consumers of security risks; for smaller economies, collaboration on government procurement requirements for IoT services; specialized liability laws for IoT, with

United States

In the United States, the private sector works closely with the public sector in very practical approaches to cybersecurity. From the earliest efforts to respond to threats by coordinating across sectors through Computer Emergency Response Teams (CERTs), to developing the standards-based NIST Cybersecurity Framework for critical infrastructure (which has become far more widely accepted as a global gold-standard cybersecurity framework), and biannual cybersecurity exercises called 'Cyber Storm," involving stakeholders from across the economy modeling and addressing the most current threats. These programs illustrate the leadership the private sector exhibits in driving cybersecurity measures and strategies in the US.

Industry Leadership: CERTs, NIST and Industry Led Voluntary Cybersecurity

In the US, the private sector and the federal government typically have worked in an effective partnership, in some cases, more formally, such as the National Cybersecurity and Communications Integration Center (NCCIC), which incorporates the US Computer Emergency Response Team (CERT), and in some cases, informally, such as consultations on standards and practices developed with the National Institute for Science and Technology (NIST).

Box 5.16: CERT Establishment

Well before government was addressing the issues of cybersecurity for non-government systems, industry was developing the capacity to protect their own networks, software and hardware. Indeed, when the Internet was devised, security wasn't even a consideration as the academics developing the network all trusted each other.[924]

It was not until 1988, when a graduate student at Cornell University, Robert Morris, unleashed the first computer worm, crippling 10 percent (6,000) of the computers on the Internet, brought together experts from around the world to collaborate to respond to the infiltration.[925] Within weeks, the first Computer Emergency Response Team (CERT) was established, headed by Carnagie-Mellon University computer scientists.[926]

companies adopting supply chain risk management to aid allocation of liability; and most importantly, the industry should act as a global community when learning from incidents. This requires an open culture of sharing and mutual learning, and the understanding that security is a joint responsibility. It is recommended to set up a global initiative – involving government, academia and industry -- to address gaps in standards and practices, lack of alignment and information sharing across supply chains, and lack of foundational IoT device security.)

[924] Cybersecurity Insiders, 'A Brief History of Cybersecurity', 2019, https://www.cybersecurity-insiders.com/a-brief-history-of-cybersecurity/.

[925] ITU, 'Introduction to Computer Security incident Response Team (CSIRT)', 2016, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Session%202%20-1115-1230-v09-10-2016.pdf.

[926] Carnegie-Mellon trademarked the acronym to ensure those using it are actually part of the specific network of specialists that work across the globe in close collaboration to address cyber threats.

Today, most economies have at least one CERT, which works in close coordination with others around the world. CERTs are comprised of stakeholders from a wide range of public- and private-sector enterprises, including government, the information technology sector, energy, financial services, telecommunications and other critical infrastructure. Carnegie-Mellon encouraged the use of the term Computer Security Incident Readiness Teams (CSIRTs) more broadly to distinguish the unique coordination among CERTs.[927] CERTs and CSIRTs today represent a well-integrated, collaborative approach between government and the private sector to fully prepare enterprises, and economies, or threats and respond to malicious incidents rapidly.[928]

From early days, the private sector and academia led in addressing cybersecurity. In 1995, Netscape developed Secure Socket Layer (SSL), the first secure network protocol to run on the Internet, followed by the development of an entire industry around antivirus software. From these efforts, standards or common methods to address cybersecurity have advanced. In the United States, it wasn't until the Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1996 there was any federal law setting out standard methods to protect personal information.[929] In 1999, the Financial Services Modernization Act of 1999 (also known as the Gramm-Leach-Bliley Act (GLBA)), introduced Safeguard Rules to protect banking customers' information.[930]

In 2002, Federal Information Security Management Act (FISMA) was enacted as part of the law creating the United States Department of Homeland Security after the 9/11 attack. Within FISMA, NIST was given authority to develop a framework of standards, guidelines and methods to address government cybersecurity.

[927] Software Engineer Institute, Authorized Users of the CERT Mark, https://www.sei.cmu.edu/education-outreach/computer-security-incident-response-teams/authorized-users/.

[928] US-CERT, 'Incident Management', 2015, https://us-cert.cisa.gov/bsi/articles/best-practices/incident-management/incident-management.

[929] Cyber Experts, 'Cybersecurity Laws – A Complete Overview', 2020, https://cyberexperts.com/cybersecurity-laws/

[930] Cyber Experts, 'Cybersecurity Laws – A Complete Overview', 2020, https://cyberexperts.com/cybersecurity-laws/

Box 5.17: NIST Technical Standards

NIST's traditional role as a standards setting body has it working closely with industry to develop technical standards for the United States. In the realm of computer security and cybersecurity, NIST leads the development and promulgation of Federal Information Processing Standards (FIPS) that are "compulsory and binding" for federal computer systems. An example of a FIPS standard is the Standards for Security Categorization of Federal Information and Information Systems, FIPS 199, published in 2004 and FIPS 197, Advanced Encryption Standard (AES), published in 2001. There are also several Digital Signature Standards, a series of FIPS 186 documents.[931] One objective for FIPS was to enable the use of commercial off the shelf solutions in government applications to improve standardization and harmonization across government and with private sector practice.[932]

NIST also publishes Special Publications, which provide standards and practices guidance to both government and the private sector on numerous topics and are widely respected, including sector specific cybersecurity recommendations, such as:[933]

- SP800 series which addresses computer and information security;
- SP1800 series which addresses cybersecurity practices; and
- SP500 series related to computer systems cybersecurity and privacy.

Beginning in 2012, the United States federal government began to explore the need for new laws to protect critical infrastructure from cyber threats.[934] The idea of federal legislation was very controversial, as were the specifics of proposed legislation.[935] There were several different formulations being considered, but a central feature was regulatory authority, rather than an entirely voluntary approach.[936] To respond to the need for more immediate federal action, the President of the United States issued Executive Order 13636 (EO) in 2013. The EO initiated a federal effort to pursue a voluntary approach with substantial private sector input (it was not until later people realized that the voluntary approach was sufficient and there was no need for a regulatory backstop).[937] The objective was to improve the private- and public-sector sharing of cybersecurity threat information, and develop a framework for reducing risks to critical

[931] NIST, 'Computer Security Resource Center – FIPS Series', 2020, https://csrc.nist.gov/publications/fips.
[932] TRPC Interview (26 August 2020) Adam Sedgewick, Senior Information Technology Policy Advisor and Amy Mahn, International Policy Specialist, NIST.
[933] NIST, 'Computer Security Resource Center – SP Series', 2020, https://csrc.nist.gov/publications/sp.
[934] TRPC Interview (26 August 2020) Katie Ignaszewski, Cybersecurity Policy, IBM.
[935] TRPC Interview (26 August 2020) Katie Ignaszewski, Cybersecurity Policy, IBM (the bill, S. 2105 (112th Congress), was introduced but did not receive a vote, see https://www.congress.gov/bill/112th-congress/senate-bill/2105.
[936] TRPC Interview (26 August 2020) Adam Sedgewick, Senior Information Technology Policy Advisor and Amy Mahn, International Policy Specialist, NIST.
[937] TRPC Interview (26 August 2020) Adam Sedgewick, Senior Information Technology Policy Advisor and Amy Mahn, International Policy Specialist, NIST.

infrastructure based on successful current practices.[938] Under this EO, NIST was tasked with the development of a "Cybersecurity Framework" for the protection of critical infrastructure.[939] Within weeks, NIST began its public consultation process, issuing its first Request for Information (RFI), highlighting the key objective to draw from industry experience, a public call for information on standards and best practices in cybersecurity, to start the dialog with industry and academia and to begin to collect lessons learned and identifying standards and practices that were being used with success that potentially could be generalized into a framework.[940] Industry has past experience with NIST and knew it to be a skilled, neutral convenor and a 'safe place' to discuss the challenges of cybersecurity risks.[941] The objective was to create a consensus document within a year.[942] The general framing of the process for this 'development' stage of the Framework was to seek industry consensus on a voluntary cybersecurity framework that would align standards and best practices in industry to be applicable to any enterprise of any scale.[943] The Framework would be a 'living document,' to be revised as circumstances evolved, to address issues not initially addressed or as new learning developed.[944]

Working with the timeframe objective of a one-year process, NIST initially hosted five workshops, first, an online workshop to socialize the need for a framework and solicit interest, and subsequently, a three-day workshop at Carnegie-Mellon University in Pennsylvania (and webcast, to provide for greater participation) to encourage debate and discussion and collect information.[945] There was enthusiastic, committed participation from all stakeholders in private sector, academia and the relevant government agencies.[946] From these workshops and the

---

[938] The White House, Foreign Policy, 'Cybersecurity - Executive Order 13636', https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/eo-13636 see also, NIST – Cybersecurity Framework, History and Creation of the Framework, https://www.nist.gov/cyberframework/online-learning/history-and-creation-framework (In the US, the President can initiate executive branch actions through an Executive Order (EO).)

[939] NIST - Industry Impacts; Cybersecurity Framework, https://www.nist.gov/industry-impacts/cybersecurity-framework.

[940] TRPC Interview (26 August 2020), Adam Sedgewick, Senior Information Technology Policy Advisor and Amy Mahn, International Policy Specialist, NIST. (It was well understood that basing the framework on industry standards and practices would better enable enterprises to adopt cybersecurity measures in such a way there was harmonization across enterprises and sectors that was flexible enough to respond to trends in technology. This approach was considered to be more effective to meet the cybersecurity objectives than were the government to develop and impose its own standards.)

[941] TRPC Interview (26 August 2020), Katie Ignaszewski, Cybersecurity Policy, IBM and TRPC Interview (26 August 2020), Adam Sedgewick, Senior Information Technology Policy Advisor and Amy Mahn, International Policy Specialist, NIST. For example, NIST's public-private partnership work on encryption standards for the Internet has achieved global adoption and is widely regarded as one of the most impactful workstreams for NIST in this area.

[942] TRPC Interview (26 August 2020), Adam Sedgewick, Senior Information Technology Policy Advisor and Amy Mahn, International Policy Specialist, NIST.

[943] TRPC Interview (26 August 2020), Adam Sedgewick, Senior Information Technology Policy Advisor and Amy Mahn, International Policy Specialist, NIST.

[944] TRPC Interview (26 August 2020), Adam Sedgewick, Senior Information Technology Policy Advisor and Amy Mahn, International Policy Specialist, NIST.

[945] NIST, 'NIST – History and Creation of the Framework', Last accessed 6 October 2020, https://www.nist.gov/cyberframework/online-learning/history-and-creation-framework and TRPC Interview (26 August 2020), Adam Sedgewick, Senior Information Technology Policy Advisor and Amy Mahn, International Policy Specialist, NIST. (An alternative development model, to establish working group, would have taken more time, possibly a year simply to create the working group).

[946] TRPC Interview (26 August /2020), Katie Ignaszewski, Cybersecurity Policy, IBM.

responses to the RFI, a preliminary draft was released in anticipation of the third major workshop, which was held at the University of San Diego in California.[947] A discussion draft substantially expanding on the preliminary draft was circulated the following month, followed by another workshop, this time in the University of Texas in Dallas, Texas, in which breakout sessions enabled smaller groups of attendees to focus on specific aspects of the discussion draft. NIST received feedback that included the need for additional clarification around the general structure of the Framework and a recommendation to focus on cybersecurity outcomes.[948] A further 200 written responses to the draft were received as a result of a 45-day public RFI process. The fifth workshop was held at North Carolina State University in Raleigh, North Carolina where small and medium sized businesses and critical infrastructure representatives considered the applicability of the draft Framework.[949]

On February 12, 2014, the first version of the Cybersecurity Framework was published, one year from the issuance of EO 13636. Considered a 'living document', in 2017, the process was resumed with another RFI and several workshops which resulted in the Cybersecurity Framework v.1.1 being released on April 16, 2018.[950] Following an initial roadmap developed with the initial Framework, the revision included some topics, such as supply chain cybersecurity, that had been tabled in the first drafting.[951] The expectation is that there will be revisions to the roadmap periodically, and updates to the Framework likely on a three year cycle.[952] If there is anything disruptive, the timeframe would not hinder revisions, but NIST is careful to consider avoiding disruption to the use of the Framework.[953] With the initial efforts of creating the Framework behind them, much of the effort is focused on how the Framework is being used, as use will inform revisions.[954]

While the primary intent was to provide an industry-led voluntary risk-based framework for owners and operators of United States critical infrastructure (e.g., energy, communications, banking and defense), NIST has actively promoted its use to extend to all public- and private-sector enterprises across the globe. The Framework is considered by many the gold standard, as was, and continues to be the transparent and inclusive process for its development and

[947] NIST, 'NIST – History and Creation of the Framework', Last accessed 6 October 2020, https://www.nist.gov/cyberframework/online-learning/history-and-creation-framework.
[948] NIST, 'NIST – History and Creation of the Framework', Last accessed 6 October 2020, https://www.nist.gov/cyberframework/online-learning/history-and-creation-framework.
[949] NIST, 'NIST – History and Creation of the Framework', Last accessed 6 October 2020, https://www.nist.gov/cyberframework/online-learning/history-and-creation-framework.
[950] NIST, 'NIST - Cybersecurity Framework; Evolution of the Framework', Last accessed 6 October 2020, https://www.nist.gov/cyberframework/evolution.
[951] TRPC Interview (26 August 2020) Katie Ignaszewski, Cybersecurity Policy, IBM. and TRPC Interview (26 August 2020) Adam Sedgewick, Senior Information Technology Policy Advisor and Amy Mahn, International Policy Specialist, NIST .
[952] TRPC Interview (26 August 2020), Katie Ignaszewski, Cybersecurity Policy, IBM.
[953] TRPC Interview (26 August 2020) Adam Sedgewick, Senior Information Technology Policy Advisor and Amy Mahn, International Policy Specialist, NIST.
[954] TRPC Interview (26 August 2020) Adam Sedgewick, Senior Information Technology Policy Advisor and Amy Mahn, International Policy Specialist, NIST.

revisions.[955] For leading information technology companies, the Framework has been a useful tool to assist commercial partners and customers to improve cybersecurity and as an advocacy tool to encourage attention to address cybersecurity.[956]

The process through which the Cybersecurity Framework was developed was more recently applied to the development of the NIST Privacy Framework which was initiated in 2018. The Privacy Framework also follows the structure of the Cybersecurity Framework to facilitate the use of both together.[957]

Box 5.18: NIST Cybersecurity Framework

The NIST Cybersecurity Framework integrates industry standards and best practices to help government and private-sector enterprises of any scale to prevent, detect, respond to, and recover from, cybersecurity threats. The NIST Framework addresses security contemplating three areas for controls: confidentiality, integrity and availability of data. Under the NIST Framework there are five main functions that an organization should address:

- Identification (understanding current potential risks and risk tolerance);
- Protection (developing appropriate controls to protect critical operations and data given the risks and risk tolerance);
- Detection (establishing the controls to detect cybersecurity risk events in a timely manner);
- Response (establishing the controls that enable swift action against a detected cybersecurity risk); and
- Recovery (a comprehensive plan and ability to ensure business continuity and return quickly and to normal operations once a cybersecurity risk has been addressed).

For each of these five functions, there are several relatively high-level categories of objectives. Under each category are subcategories which address specific areas for which controls should be considered. Controls are typically based on accepted international standards and are applied in alignment with the risk profile for the particular data. With the objective of enabling the use of commercial off the shelf solutions for better standardization and harmonization, within each subcategory is a set of technical references, typically standards such as those published as ISO/IEC (e.g., ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27017) or NIST (e.g., FIPs) or related to COBIT 5 (Control Objectives for Information and Related Technologies, a data governance framework developed by Information Systems Audit and Control Association (ISACA) most recently updated in 2012).[958] Controls fall into three applications, for technology, processes and personnel. As well, the Framework provides a strategy to operationalize the data management and

[955] TRPC Interview (26 August 2020), Katie Ignaszewski, Cybersecurity Policy, IBM.
[956] TRPC Interview (26 August 2020), Katie Ignaszewski, Cybersecurity Policy, IBM.
[957] NIST, 'Privacy Framework 1.0', January 2020, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf.
[958] TRPC Interview (26 August 2020), Adam Sedgewick, Senior Information Technology Policy Advisor and Amy Mahn, International Policy Specialist, NIST.

cybersecurity controls. The NIST Framework is among the most comprehensive, adaptable approaches to cybersecurity.

Sources:

- NIST, 'Cybersecurity Framework', Last accessed 6 October 2020, https://www.nist.gov/industry-impacts/cybersecurity-framework.
- ISO, 'ISO/IEC 27001 Information Security Management', https://www.iso.org/isoiec-27001-information-security.html
- NIST, 'Federal Information Processing Standards Publications', Last accessed 6 October 2020, https://www.nist.gov/itl/publications-0/federal-information-processing-standards-fips;
- ISACA, 'Frameworks standards and models', Last accessed 6 October 2020, https://www.isaca.org/resources/frameworks-standards-and-models

Cybersecurity Exercises

Cybersecurity exercises (i.e., wargames) are an important way of assessing cybersecurity readiness and ensuring that in the case of genuine cyber-attacks, technical staff and public servants are well-drilled and as prepared as they can be to respond to new and changing scenarios. Given the importance of institutional adaptability in the face of an evolving threat landscape, cybersecurity exercise parameters cannot remain static and should always account for new trends or threat profiles. The continuing digitalization of different sectors—such as due to the spread of IoT devices in manufacturing or autonomous vehicles—may necessitate wider participation.

The United States Department of Homeland Security, Cybersecurity & Infrastructure Security Agency (CISA), is tasked with protecting the United States infrastructure from cyber threats. CISA works across the spectrum of society, providing information to, and working with, agencies of the federal government; state, local, tribal and territorial government; private industry; academia; NGO and non-profit; and general public stakeholders.[959] CISA provides extensive cybersecurity information related to working from home, protecting critical infrastructure, smaller towns, soft targets and crowded places, and the electoral system.[960] Like NIST, the private sector was often invited to engage with CISA and found these engagements very constructive.[961] CISA has hosted a biennial series of cybersecurity exercises since 2006, called Cyber Storm.[962] Each Cyber Storm involves businesses from across the economy and government at all levels, state, local and federal. Each successive event has been built on lessons learned from real-world incidents from the intervening years to ensure that participants face scenarios that reflect actual real-world conditions and potential cyber-threats. The most recent Cyber Storm, which was held in 2018, had a narrower sectoral focus on the

[959] CISA, 'Service Catalog', https://www.cisa.gov/publication/cisa-services-catalog.
[960] CISA Hometown Security, https://www.cisa.gov/.
[961] TRPC Interview (26 August 2020), Katie Ignaszewski, Cybersecurity Policy, IBM.
[962] CISA, 'Cyber Storm: Securing Cyber Space', 2019, https://www.cisa.gov/cyber-storm-securing-cyber-space.

manufacturing and transport sectors.[963] Notably, one of the exercise's primary stated goals was evaluating the effectiveness of the United States National Cyber Incident Response Plan (NCIRP) in guiding responses, which demonstrates a commitment to field-testing response protocols, and helps to predict their relevance in real-world threat scenarios. There is a planned Cyber Storm exercise for 2020.[964]

Evolving Threat Landscape: IoT Security

The threat landscape is evolving rapidly with the evolution of artificial intelligence, 5G, and the innovations around connected devices, what is colloquially called the Internet of Things (IoT). [965] More and more, e-commerce entails the use or sale of new, connected devices. Ordinary objects are being connected to each other and to business networks. Some of these devices transmit and receive highly sensitive data or data which if corrupted, could cause serious harm or if disclosed maliciously could reveal personal information or business confidential information. Imagine a connected home refrigerator which is enrolled with an online marketplace in which it can reorder milk when the refrigerator detects the supply is low. The refrigerator may hold your market account, food preferences (and possibly medication) information, credit card details, as well as your address for delivery.

IoT is improving home and business efficiencies, enabling finer automated control to improve the operation of homes, buildings, transportation, and eventually, entire cities (to give a sense of scale of the cybersecurity challenge, 'smart cities' are comprised of a vast array of connected devices) and improving efficiency and productivity across all sectors, most notably in healthcare, logistics and supply chain management, agriculture and manufacturing. But there are risks. The more devices that are connected to a network, the greater the opportunity for cybercriminals to attack that network. Each new device is a new vulnerability. Currently, the focus for developers prioritizes time-to-market and profitability over security. This must change. To stimulate that change in priority, California enacted a new law to require security be incorporated into all IoT sold in the state.

A. California IoT Security Law

In 2018, there was estimated to be approximately seven billion connected devices globally.[966] In 2016, domain name service (DNS) provider Dyn, was assaulted by a sequence of distributed denial-of-service (DDOS) attacks perpetrated using a botnet operating through a multitude of IoT devices such as surveillance cameras, residential gateways, and baby monitors, that had

[963] CISA, 'Cyber Storm VI: National Cyber Exercise', 2020, https://www.cisa.gov/cyber-storm-vi.
[964] CISA, 'Cyber Storm 2020', 2020, https://www.cisa.gov/cyber-storm-2020.
[965] In addition to the risks that IoT presents, in Corporate Security Predictions 2020, https://securelist.com/corporate-security-predictions-2020/95387/, Kaspersky researchers described an ever-more complex and challenging threat environment.
[966] ABA Journal, 'California imposes new regulations on 'internet of things' devices', 2018, https://www.abajournal.com/news/article/new_california_imposes_regulations_on_the_internet_of_things.

been infected with malware.[967] The incident temporarily shut down websites including AirBnb, Amazon, CNN, Netflix, PayPal, Reddit, Spotify and Twitter in the northeast of the US and other regions. This incident was a wakeup call to governments across the United States. Companies that moved early into IoT did not consider the security threats, and it was up to government to compel that to change.[968]

In the United States, California is often on the cutting edge of consumer protection law. In January 2020, California's 2018 IoT Security Law came into effect.[969] This first-of-its-kind law mandates that all IoT devices sold in the state must have "reasonable cybersecurity measures appropriate to the nature and function of the device, appropriate to the information it may collect… and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure, as specified."[970]

One weakness of consumer IoT is that manufacturers commonly do not include password protection, or they use default login credentials common to all devices of their manufacture, making them easy to exploit. One of the features of the California law is to address this issue, requiring either a preprogrammed unique password, or the user to generate a unique password before being able to use the device.[971] To address this weakness, the California laws specifies certain access and authentication requirements, such as how passwords are to be implemented.

B. Security-by-design

The California law also requires developers to implement reasonable cybersecurity measures appropriate to the nature and function of the devices. One approach to achieve this objective—and the general objective of improving IoT cybersecurity—is the concept of security-by-design, to encourage developers to consider security issues as they are developing new products.

Although IoT is not yet contemplated in the NIST Cybersecurity Framework, there is consideration to adding it, as well as 5G—two new technologies expected to have a major impact on cybersecurity, but currently, given the risk-based approach of the Framework, IoT is not an additional type of risk that needs to be addressed separately.[972] That said, NIST is

[967] The Guardian, 'DDoS attack that disrupted internet was largest of its kind in history experts say', 2016, https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet, see also, Sucuri Blog,2019, 'The Largest DDoS Attacks & What You Can Learn From Them', 2019, https://blog.sucuri.net/2019/08/largest-ddos-attack.html.

[968] BFV, 'Internet of Things: California Passes Legislation on Connected Devices', 2018, https://www.bfvlaw.com/internet-of-things-california-passes-legislation-on-connected-devices/.

[969] California Legislative Information, 'Senate Bill No.327 Information Privacy: Connected Devices', Chapter 886, 2018, https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327.

[970] California Legislative Information, 'Senate Bill No.327 Information Privacy: Connected Devices', Chapter 886, 2018, https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327.

[971] ABA Journal, 'California imposes new regulations on 'internet of things' devices', 2018, https://www.abajournal.com/news/article/new_california_imposes_regulations_on_the_internet_of_things.

[972] TRPC Interview (26 August 2020), Katie Ignaszewski, Cybersecurity Policy, IBM.

working with the private sector in the US to improve IoT cybersecurity.[973] One project brings cybersecurity to connected medical devices. Wireless, connected healthcare devices can pose a threat both to the user of the device, the patient, and can become a vulnerability to the hospital network to which they communicate. NIST is working with industry to reduce these risks using standards-based commercially available technologies and industry best practices. Medical infusion pumps, once free-standing and communicating only with the patient and the care provider, are life-saving devices that now are wirelessly connected to hospital networks, improving the use of the device and management of care.[974] NIST made recommendations to manufacturers on how to improve the cybersecurity of these devices by adding a digital certificate to the data flow, which only allows the device to communicate with specific servers.[975] This and other recommendations with regard to this type of device, are illustrative to the healthcare sector as to approaches to address cybersecurity for all devices in their highly sensitive environment.

Conclusion

In the United States, the private sector has immediacy, capacity and agility with regard to cybersecurity. As well, some of the most sensitive infrastructure are in the control and management of the private sector. With regard to e-commerce, the commerce, trade and financial services cybersecurity operations are very sophisticated and capable. The government has a significant role in addressing cybersecurity for public-sector assets, and as well, convening efforts to work across private-sector industries and in public-private sector collaborations. Close collaboration between the private sector and public sector has led to a robust cybersecurity capacity. CERTs provide a forum for defensive collective action to identify and address specific threats. The NIST Cybersecurity Framework guides enterprises to understand their cybersecurity threats, vulnerabilities and potential impacts and enable them to develop the means to reduce risk with measures, based on international standards and industry best practices, they customize to the enterprise's needs.[976] The Framework also guides response to cybersecurity incidents, prompting an affected enterprise to analyze causes and consider lessons learned.

The Framework, and the process for its development and continuing improvements is a model for such public-private cybersecurity collaboration. Recognizing the fluidity of the cybersecurity environment, the Framework is considered a living document, which will be regularly reviewed and periodically updated as circumstances demand. And through real-time exercises, the Cyber Storm approach gives all stakeholders the opportunity to test and refine their readiness to address severe threat scenarios.

---

[973] NIST, 'NIST - Internet of Things (IOT) What Is The Internet Of Things (IOT) And How Can We Secure It?', https://www.nist.gov/topics/internet-things-iot.

[974] NCCOE-NIST, 'Securing Wireless Infusion Pumps', https://www.nccoe.nist.gov/projects/use-cases/medical-devices.

[975] NCCOE-NIST, 'Securing Wireless Infusion Pumps', https://www.nccoe.nist.gov/projects/use-cases/medical-devices.

[976] TRPC Interview (26 August 2020) Adam Sedgewick, Senior Information Technology Policy Advisor and Amy Mahn, International Policy Specialist, NIST.

Key Lessons

The scale and purpose of many cyberattacks threaten e-commerce from several perspectives. First, there is a real and direct threat to consumers' financial security and sensitive personal information with the risk of identity theft. In addition, threats serve to undermine trust in the online environment, an incident in one sector may impact all businesses in that sector. Similarly, threats undermine the adoption of new and rapidly evolving technologies such as IoT (including AVs and robotics). Finally, for businesses threats to trade secret, IP, customer data and other sensitive business information risk competitive advantage, financial losses and reputational harm. Finally, in recent years, attacks on political institutions threaten to undermine the political system and a government's ability to govern.

E-commerce is comprised of many small and medium-sized businesses. Some are developers of apps or other online services or products, others are small enterprises running their business on a large marketplace platform. Depending on their product or service and position in the e-commerce ecosystem, they will need cybersecurity capabilities to match the risks associated with the data they control. It is important too that businesses, large and small, and governments in every economy take a cooperative, collaborative approach to cybersecurity. The threats know no geographic or political bounds, and the defenses should not either. Therefore, adopting widely accepted international industry standards and best practices, and maintaining and updating these regularly and frequently (in accordance with best practices) will ensure greater agility and the most current methods and technologies applicable to cybersecurity needs. Effective cyber defense demands resources across the economy, from government and the private sector. In many ways cyberattacks (viruses or malware for example) can be similar to pandemics, and a failure of a rapid, coordinated response can have dire consequences.

1. Economies **must attain the leadership and support from the highest level of government to focus on cybersecurity, with leadership and resources allocated at all levels in both the public and private sector.** Capacity must be developed to address day-to-day threats as well as the need for more specialist research to identify and prepare for more highly sophisticated threats. Every agency of government needs dedicated high-level leadership and resources with the skills and capacity to address the rapidly evolving cybersecurity threat landscape. Every employee must be responsible for cyber-awareness.
2. Developing economies may not have the resources to maintain even basic cybersecurity. Therefore, they should **collaborate with and receive support from the private sector**.
3. **All economies need to coordinate on cybersecurity** which knows no geographic or political boundaries. Indeed, in the same way small businesses are more vulnerable than larger businesses, and therefore are more likely to be targeted, less developed economies are often the target as a path to access assets in more developed economies.
4. In the area of cybersecurity, **industry can lead**—as these stakeholders have the most current and sophisticated understanding of threats and the resources allocated to address risks and respond to attacks with speed and agility -- through years of experience, best

practices and technical standards, as well as elaborate cybersecurity frameworks which have been developed and continue to be revised as the threat landscape rapidly evolves. Yet, **government has a role in coordinating efforts and responses to threats, encouraging the adoption of industry best practices, international standards and commercial off the shelf solutions across their economy and globally**, and as appropriate, ensuring compliance through certification or accountability.

5. Recognizing the constant and substantial growth in cybersecurity risks and threats, every enterprise with an online connection needs to address cybersecurity, which means there is a growing demand for cybersecurity talent. Therefore, uptake for digital services including e-commerce, will be affected if those talent needs are not met. **Governments, academia and the private sector in each APEC member economy should work together to develop and deliver curricula for the education, workforce skills development and the hiring of cybersecurity talent**. As we invest in restarting economies across the globe after the COVID-19 pandemic, many people now out of work are capable of reskilling, or those moving into the workforce for the first time need to be able to move into new types of positions, including all aspects of cybersecurity. **COVID-19 recovery investment should also address these long-term workforce challenges.**
6. **Government policy should encourage IoT safety and security from the starting point of design**. IoT development has focused on time-to-market and cost savings, laws can elevate cybersecurity requirements for IoT across industries. Cybersecurity should be designed into every device from the early stages of development, rather than added on after a product is fully developed. In order to encourage this, laws should require certain standards for cybersecurity are implemented and security and privacy objectives are met.

5.5 FOCUS AREA E: INFRASTRUCTURE RELATED ASPECTS

OVERVIEW

These case studies examine the role of infrastructure in the facilitation and promotion of e-commerce, especially among MSMEs, and why overcoming the digital divide is instrumental in achieving this. Two of Asia Pacific's most networked economies are taken as examples: Korea and Chinese Taipei. In addition, the case of Mexico is included, as an upper middle-income economy that introduced telecommunications reforms from 2012 onwards. From these case studies, lessons can be learned, in particular regarding the opening up of markets to allow for competitive entry of other suppliers of traditional telecommunication services, as well as new technologies, to enable a range of digital services that underpin e-commerce.

Furthermore, the importance of infrastructure is determined by the modes of access to e-commerce, typically by computers and smartphones. Wireless and fixed-line (and fixed wireless) networks are required to support these devices, as well as online payment systems. On the one hand, wireless networks are typically mobile cellular networks and Wi-Fi

networks.[977] On the other hand, fixed line networks, either narrowband copper or broadband fiber are not only used in their own right as modes of access, usually by a computer, but are of paramount importance as a backhaul for cellular networks needing to connect to mobile switching centers, or to routers on the economy-wide broadband network. The economy-wide broadband network is a backbone that runs the length of an economy connecting to provincial and distant local routers, to submarine cable landing stations and to satellite earth stations for international traffic. A fixed broadband infrastructure is needed to make the mobile wireless networks effective, and the wireless networks in particular are needed to make e-commerce accessible to the general public, either as vendors or as consumers. While most traffic to and from e-commerce sites requires only narrow bandwidths[978], when the narrowband data traffic is aggregated from the tens of thousands of local vendors and/or buyers, the backhaul and backbone networks need to be broadband.[979] But in many developing economies, remote and rural areas, and MSMEs located there, Internet access is still irregular or not available as broadband infrastructure has not been rolled out. These problems have been addressed by economies like Korea and Chinese Taipei while others like Mexico and Peru continue to explore the potential of advances in satellite and 5G telecommunications technologies.

Key Issues

The basic infrastructure of broadband networks, which by today's digital standards means fixed line, wireless and mobile networks, Internet Exchange Points (IXPs), Content Delivery Networks (CDNs) and cloud computing networks through a cluster of data centers are essential foundations of a digital economy and an economy that can trade competitively in world markets.[980] These case studies therefore focus upon the policies that are most certain to induce sustainable investment in such networks, and will then examine the policy shifts towards a digital economy.

- **Broadband:** State of the market with respect to competition, supply and demand; public and private investment; wholesale and retail networks; fixed backbone and international capacity and mobile networks. The case of both Korea and Chinese Taipei highlight the necessity of investing in broadband Internet infrastructure.
- **Other telecommunications infrastructure issues**: Regulatory policies that impact market entry and competition in wholesale and retail markets; and policies towards facilities sharing and universal service. The case study of Mexico highlights the significance of an independent regulator in ensuring competition.

[977] Although specialist wireless networks exist to serve very high-density confined spaces, such as shopping malls, or to provide local coverage for remote and low-density areas such as rural villages.
[978] Although uploading video requires higher bandwidths.
[979] There are numerous glossaries of telecom terminologies, for example, https://standards.tiaonline.org/resources/telecom-glossary.
[980] OECD Going Digital — Making the transformation work for growth and well-being; Digital Infrastructure, https://www.oecd.org/going-digital/topics/digital-infrastructure/.

- **Digital economy**: Development of a digital economy needs to go hand-in-hand with suitably revised laws and regulations enabling the adoption of cloud computing and data usage. Korea and Chinese Taipei's approaches to establishing and promoting essential cloud infrastructure are also examined.

CASE STUDIES

Korea

This case study of Korea illustrates how the drive for universal broadband coverage, in order to ensure international competitiveness, has underpinned consistent and long-term policy-making over the last few decades. This was achieved through close cooperation between the government and private sector investing in a modern broadband Internet infrastructure for all in a digitalized economy; a focus upon adopting international standards to gain traction in global markets; and holistic and innovative policy approaches. However, in order to ensure continued and sustained digital economy and e-commerce growth, Korea will need to address limited use of digital technologies by businesses, including the use of cloud computing technologies.

Universal Service Drives Broadband Infrastructure Roll Out

Korea is a world leader in broadband coverage and speeds. Data from the Ministry of Science and ICT (MSIT) demonstrates that by 2018, 100 percent Internet penetration rates for households and businesses employing 10 or more staff, together with 90 percent Internet usage rates for individuals had been achieved.[981] As smartphones replace computers the proportion of households with computers after 2012 starts to fall, but not for businesses.

Korea's universal broadband coverage is the outcome of consistent investment in telecommunications networks and equipment over a number of decades, and has been driven by a strong imperative to close the digital divide and build a more inclusive society. In providing this foundational infrastructure—which now supports and spurs on digital economy and e-commerce growth—Korea undertook a number of steps, including:

- Raising the total domestic investment in telecommunications from 3 percent in the 1970s, to 7 percent in the 1980s;[982]
- Moving from copper to broadband fiber since the 1990s, resulting in becoming the world leader in broadband penetration since the early 2000s;

[981] MSIT (2020) 2019 Year Book of Information Society Statistics, http://english.msip.go.kr/cms/english/pl/policies2/__icsFiles/afieldfile/2020/02/14/2019%20Yearbook%20of%20Information%20Society%20Statistics.pdf.

[982] ITU, 'ITU (March 2003) Broadband Korea: Internet Case Study', http://www.itu.int/ITU-D/ict/cs/korea/material/CS_KOR.pdf.

- Universal telephone service started in 2000, with facilities-based operators providing local telephone service, public telephone service, island communications service and maritime cellular phone service or sharing the costs of such services;
- Focusing on educating communities in the use of broadband Internet through, for example, Cyber Korea 21 in 1999 and the expansion of the Korea Agency for Digital Opportunity and promotion (KADO) in 2003;[983]
- Introducing competition in fixed market in 1999, and in wireless market in 2002;
- Aiming to close the digital divide, with the Comprehensive Plan requiring Korea Telecom (KT) provide broadband Internet service (defined as 1Mbps) to all farming and fishing villages, commencing in 2002;[984] and
- Establishing universal public Wi-Fi in 2012, and providing high-speed (100Mbps) broadband universal service anywhere in Korea upon demand from 2020.[985]

The economic growth as a result of the initial increase in domestic investment in telecommunications, which transformed "Korea into an IT powerhouse," motivated Korea to further invest in broadband and the Internet in order "to recreate a similar success story."[986]

Box 5.19: Universal Service

Universal service basically means service-on-demand, i.e., networks should cover the entire population and services should be affordable. For many developing economies this remains aspirational. But what universal service means in practical terms has changed over the decades, for two reasons. First, owing to technological change the nature of the service has changed, notably from analogue to digital, then to Internet, then to broadband and then to high speed broadband; second, the growing role played by telecommunications in the economy and society has turned always-on connectivity into a way of life.

Today, universal service essentially means access to broadband networks, increasingly mobile broadband networks, and at speeds that allow fast downloads and uploads to the Internet. Broadband has itself changed its meaning from 144Kbps until the 1980s, to 1Mbps by the later 1990s, then to 10Mbps, and today even 1Gbps is not unusual in developed economies. As the speeds get ever faster there is no one meaning attached to broadband, but for regulatory purposes different economies use different benchmarks.

Achieving universal service has also changed. Before the digital and Internet revolutions, the Public Switched Telephone Network (PSTN) was often operated by a monopoly carrier, and regulators obliged the carrier to cross-subsidize unprofitable service to uneconomic areas

983 Digital Preservation Europe, 'KADO - Korea Agency for Digital Opportunity and Promotion, South Korea', https://www.digitalpreservationeurope.info/registries/competence-centres/list/?id=137.

984 Cepal, 'The Strategy for Building Information Society in Korea', 2003 https://www.cepal.org/noticias/noticias/3/12743/kijoolee2.pdf.

985 Korea Herald, 'S. Korea starts universal super high-speed internet service for the entire country', 2020, http://www.koreaherald.com/view.php?ud=20200105000109.

986 TRPC Interview (26 August 2020) Ray Jo, Microsoft, Korea.

from the profits made in other markets. When mobile networks became widespread, new entrants were able to challenge the incumbent fixed line operator with more flexible and cheaper services. Where regulations allowed facilities sharing, licensed new operators, controlled the charges for interconnection with the dominant carrier, and allocated spectrum at little or no cost for underserved areas, opportunities were created for new entrants to serve underserved areas. However, even in these cases, some level of state subsidy is often required.

Today, when broadband Internet is considered necessary for the digital economy, the issue of universal service has become an issue of the digital divide. It should be noted that bridging the digital divide is a challenge for all economies and it exists not only between urban and rural areas, but also within urban areas, including disadvantaged and low-income communities. The first question is what *the digital divide is*, to which the answer is: it depends. If broadband is not ubiquitous then that is the digital divide, usually measured today in terms of what proportion of the population has access to a 3G+ network and a smartphone. In more developed economies, if access to fast broadband Internet is not universal, then that can be construed as the digital divide, especially as it impacts upon access to media-rich content for consumers and as it impacts upon high bandwidth applications by small and medium-sized businesses. It should also be noted that 5G will not close the digital divide, on the contrary initially it will almost certainly increase it. 5G represents the highest contemporary bandwidths for general usage but will be primarily deployed initially for enterprise and smart city applications—which will be concentrated in urban areas of developed economies.

In order to understand Korea's pre-eminence in broadband, a number of important factors need to be considered, including:

- First, in 1995 Korea signed telecommunication commitments to the WTO, enabling market liberalization;
- Second, concerted effort focused upon its strategic industrial needs enabled Korea to switch from domestic to international standards enabling the economy to be on a competitive international footing;
- Third, Korea utilized an integrated approach to closing the digital divide, by adopting a whole-of-government approach, and tapping into a broader ecosystem of research institutes; and
- Currently, adoption of innovative policy approaches, including use of TV White Spaces, ensures Korea is able to plug any further coverage gaps.

A. WTO membership ensures market liberalization

Korea opened up all sectors of value-added services in January 1994, a year before signing telecommunication commitments to the WTO,[987] and increased foreign equity participation on facilities-based operators from 33 percent in 1997, to 49 percent from 2001 onwards. Korea allowed leased line resale in 1995 and increased foreign equity participation from 49 percent to 100 percent as from 2001.[988]

Prior to 1995, Korean telecommunications networks were very much the product of state-support for large private-sector corporations or 'chaebols'.[989] By joining the WTO, Korea was recognizing that allowing new entry into the market was the route towards putting the economy on a strong competitive footing in international markets. To bolster this, Korea undertook a steady progression of policy and regulatory steps prior to and after WTO membership—further promoting investment and competition in the telecommunication market, and laying the basis for rolling out the necessary infrastructure networks—including:[990]

- Spinning off telecom operations from the policy ministry, incorporating and then privatizing Korea Telecom;
- Creating a stand-alone telecoms regulator to oversee what eventually became a competitive market—in 2001, two additional economy-wide licenses and dozens of local licenses were issued;
- Subjecting the market to the oversight of the Korea Fair Trade Commission (KFTC) which was created following the Monopoly Regulation and Fair-Trade Act of 1980; and
- Abandoning the duopoly model of service operators (Korea Telecoms and Korea Mobile) in 1999, leading to the liberalization of the market in 2001.

B. Industrial strategy, and adoption of international standards

In strategic policy-making, historical continuity is important because it creates the building blocks for future development; but it also requires an ability to recognize new technological and social trends and adjust accordingly. One of Korea's strengths is that it has a proven record of learning from the past and making necessary adjustments.[991] This was certainly the case when Korea adapted domestic telecommunication equipment standards, such as the design of wireless devices and their use of radio frequencies, to ensure greater alignment with international standards and maintain international competitiveness.

---

[987] WTO, 'Republic of Korea and the WTO' https://www.wto.org/english/thewto_e/countries_e/korea_republic_e.htm

[988] WTO, Telecommunications commitments and exemptions, 1997, https://www.wto.org/english/tratop_e/serv_e/telecom_e/telecom_highlights_commit_exempt_e.htm#country.

[989] ITU (2003) Broadband Korea: Internet Case Study, http://www.itu.int/ITU-D/ict/cs/korea/material/CS_KOR.pdf.

[990] ITU (2003) Broadband Korea: Internet Case Study, http://www.itu.int/ITU-D/ict/cs/korea/material/CS_KOR.pdf.

[991] Gwanglae Kim (2016) 'The Shape and Implications of Korea's Telecommunications Industry: Crisis, Opportunity and Challenge', https://telsoc.org/sites/default/files/tja/pdf/75-776-1-pb.pdf.

Initially, in the 1980s—as a result of Korea's economic surplus being redirected into industrial, scientific and technological development since the 1950s[992]—Korea developed its own TDX electronic switch (a Korean equivalent to the world standard Asynchronous Transfer Mode (ATM)) that was capable of handling both analogue and digital traffic. The focus on self-sufficiency had advantages and disadvantages for Korea, for example:

- On the one hand it saved the cost of imported technology while allowing Korea to develop an expertise of its own and push ahead with investment in a telecoms infrastructure through a combination of private and public investment, including government loans to what became— after privatization—Korea Telecom.
- On the other hand, for a while it led Korea into a reliance upon home-grown technologies that were less cost effective than more globally successful technologies from Europe and the United States.

Although Korea's WiBro standard aligned with international standards (e.g., IEEE 802.16 WiMax,[993] and ITU-R 3G/4G recommendation), international adoption was limited, with LTE[994] succeeding with global deployment.[995]

As in Japan (see Box 5.20) so in Korea the large industrial conglomerations known as chaebols were the early investors in telecoms and developed their own technology standards. While this limited the economy's ability to penetrate global markets, it did not detract from Korea's concerted push for universal coverage of telecommunications which was achieved by the 1990s. This was an analogue copper fixed line network, which was followed by another push towards fiber cables and broadband upgrades.

A policy shift came later, in the 2000s, when Korea turned to the adoption of international standards, such as the 3GPP standards for UMTS (Universal Mobile Telecommunications Service)[996] and eventually, through companies such as Samsung and LG Electronics, became a world leader in cellular handsets. This achievement was only possible by the policy shift and was driven by an awareness that capturing a global market required Korea to develop and place itself at the center of a global value chain (GVC), which it could achieve by leveraging its homegrown expertise with designs and applications, such as high quality cameras for smartphones that had international appeal.

---

[992] EFF, 'Why Is South Korea a Global Broadband Leader?', 2020, https://www.eff.org/deeplinks/2020/02/why-south-korea-global-broadband-leader.

[993] IEEE (2009) The IEEE 802.16 Standards and the WiMAX Technology, https://ieeexplore.ieee.org/document/8538829

[994] Kim, D et. (2014), Comparison of WiBro and TD-LTE through the social network analysis, https://ieeexplore.ieee.org/document/6858479.

[995] John Ure (2008; ed), Telecommunications Development in Asia, HKU Press, Chapter 10, https://hkupress.hku.hk/pro/868.php.

[996] For example, Korea stands is part of the 3GPP standards for 5G technologies. See: Business Korea, 2016 '3GPP Adopts 5G Network Standards Proposed by '5G Global Group' Including SK Telecom', 2016, http://www.businesskorea.co.kr/news/articleView.html?idxno=16610.

Box 5.20: Japan - Liberalization and International Standards

Japan faced a similar dilemma. Japan's economy has been dominated by two sets of conglomerate business structures, the *zaibatsu* which are horizontally-organized and the *keiretsu* business networks that include vertically-integrated companies with multiple network relationships across the economy.[997] One of the consequences has been a tendency for Japanese companies to source their manufactured designs and components from other Japanese companies. An example was Nippon Telegraph and Telephone Corporation (NTT), that manufactured telecom equipment, sourced from its own network of local suppliers, and was Japan's dominant operator. This arrangement was common globally among dominant private or state-owned telecom enterprises (SOTE) until the 1980s and beyond.

In the field of telecoms this resulted in technologies like NTT's DoCoMo iMode which was a radical development pioneering mobile phone access to the Internet. Japan also made significant development in CDMA cellular technologies. However, these products which used standards and designs specific to the Japanese market, did not sell well in markets beyond Japan.

At the same time, Japan came under increasing pressure from the signatories to the WTO to relax non-tariff barriers to trade in the form of restrictions on IT and telecom products entering the Japanese market. As a result of this pressure, and at a time when Japan was facing growing competition internationally, especially from China, policy changes were introduced. Among these was the privatization of NTT, the eventual liberalization of the telecom and Internet markets, and a move towards international standards for fixed and mobile broadband infrastructure.[998] As a result, like Korea and Chinese Taipei, Japan in now a world leader in broadband infrastructure.

C. Policy enrichment through whole-of-government approach, and use of research institutes

In order to adequately and comprehensively address the digital divide, Korea adopted an integrated approach, that was not just limited to the telecommunications sector. This whole-of-government approach has ensured that Korea has become the benchmark in terms of closing the digital divide. Examples of these holistic strategic policies include:[999]

- An early recognition of the digital divide as it affected rural areas by giving responsibility to the Ministry of Food, Agriculture, Forestry and Fisheries (MFAFF) to

[997] FinLaw, 'Zaibatsu and "Keiretsu"- Understanding Japanese Enterprise Groups', 2017, https://corporate.findlaw.com/corporate-governance/zaibatsu-and-keiretsu-amp-150-understanding-japanese.html.

[998] John Ure, 'Telecommunications Development in Asia', HKU Press, Chapter 90, 2008, https://hkupress.hku.hk/pro/868.php.

[999] John Ure, 'Telecommunications Development in Asia', HKU Press, Chapter 10, 2008, https://hkupress.hku.hk/pro/868.php.

offer ICT training through the Rural Development Administrations (RDAs) illustrates Korea's perception of the digital divide first and foremost as a development issue;

- Public and private investment in broadband, notably in (i) a domestic broadband backbone and (ii) a competitive market in wireless broadband, mostly cellular, but also using other technologies, such as low-powered wide-area networks (LPWAN) and TVWS;[1000]
- Government adoption of Internet for e-government and for schools and clinics, including subsidies for ICT skills training and for computers;
- Capital subsidies for public access to Internet kiosks and municipal centers;
- Digital laws and plans, such as the Digital Signature Act 1999[1001] and the General Plan for Promoting E-Commerce 2000[1002]; and
- A truly comprehensive digital skills education and training program for all sectors of society, from career civil servants to old age pensioners, from prison inmates to youth centers.[1003] By 2010, an OECD report judged Korea as number one in digital literacy world rankings.[1004]

Further, successful policy outcomes often rest upon the sustainability of the institutions involved in policymaking. Being a relatively small, albeit advanced economy compared with some of its competitors, Korea—at an early stage—created an ecosystem of agencies and research institutes to advise on economic and industrial strategies. During the earlier period the focus was on technology with the setting up of:

- 1966: Korea Institute of Science & Technology;
- 1971: Korea Advanced Institute of Science & Technology; and
- 1976: Electronics and Telecommunications Research Institute.

Later the focus switched to economic and social development issues with the creation of the Korea Information Society Development Institute (KISDI), [1005] the Korea Development Institute (KDI)[1006] and others.[1007] The thinking was clearly designed to focus on immediate domestic priorities. This has provided Korea with a consistency in long-term policymaking even as governments changed, something that is often lacking in other economies.

[1000] John Ure (2008; ed), Telecommunications Development in Asia, HKU Press, Chapter 10, https://hkupress.hku.hk/pro/868.php.

[1001] Korea Legislation Research Institute-KLRI, 'Digital Signature Act Chapter I General Provisions [Act No. 14577. Mar 4 2017]', 2017, https://elaw.klri.re.kr/eng_service/lawView.do?hseq=42625&lang=ENG.

[1002] Choong Yong Ahn (2019), E-commerce & ICT Development in South Korea: Prospects & Challenges, https://www.jef.or.jp/journal/pdf/223rd_Cover_Story_04.pdf.

[1003] The World Bank, 'Bringing Government into the 21st Century – Korean Digital Governance Experience', 2016, http://documents1.worldbank.org/curated/en/934391468011726182/pdf/106581-REVISED.pdf.

[1004] The Korea Herald, 'Koreans top in digital literacy: OECD data', 2011, http://www.koreaherald.com/view.php?ud=20110629000573.

[1005] KISDI, KISDI History – Overview, https://www.kisdi.re.kr/kisdi/jsp/fp/eng/about/KE_32000.jsp.

[1006] KDI, http://www.kdi.re.kr/kdi_eng/main/main.jsp.

[1007] GW Libraries, Korean Studies: Organizations, https://libguides.gwu.edu/korea/organizations.

Box 5.21: Chile and Peru in Closing the Digital Divide

According to rounded World Bank data, the proportion of the population using the Internet in 2018 in Chile (2017) 82 percent and in Peru 55 percent. Ten years earlier (2008), the figures were 37 percent and 31 percent so while Chile has made significant progress, Peru remains with half the population using the Internet.[1008] Both economies are signatories to the WTO with Chile, which has a highly competitive domestic market, [1009] committed to opening its international sector to foreign competition and Peru its entire market.[1010] The reasons why the digital divide remains so much higher in these economies involve partly:

- Periods of political instability (including a period of military rule in Chile and a guerrilla war in Peru);
- Inherent geographical challenges (such as the sparsely populated area of Patagonia of southern Chile and the Andes Mountains of Peru);
- The development status of the two economies (with Chile the more developed of the two), and the incidence of poverty in both economies which is exacerbated by highly unequal levels of income distribution[1011,1012]; and
- Economic factors such as the collapse of commodity prices.

Chile's improvement can be partly put down to also reaching out for an integrated approach. Chile was motivated to re-establish civilian rule and social development following the end of military rule in 1990. There was a "realization that education would play an important role in domestic performance." [1013] For example, the ICT in Education initiative of the Chilean Educational Reform known as 'Enlaces'[1014] was created from the National Network of Universities (REUNA) to provide training for citizens under the National Campaign for Digital Training. Although not particularly well-resourced, Chile is a good example of making the most of what it has through a strong motivation to upgrade its teachers and students in preparation for a digital future, a lesson other developing economies would do well to follow.

[1008] The World Bank, 'Individuals using the Internet (% of population)', Last accessed August 2020, https://data.worldbank.org/indicator/IT.NET.USER.ZS.

[1009] Business Wire, 'Chile Telecoms Infrastructure, Operators, Regulations Statistics and Analyses 2019 - ResearchAndMarkets.com', August 2019, https://www.businesswire.com/news/home/20190809005208/en/Chile-Telecoms-Infrastructure-Operators-Regulations-Statistics-Analyses.

[1010] WTO, 'Telecommunications Services: commitments & exemptions', 1997 https://www.wto.org/english/tratop_e/serv_e/telecom_e/telecom_highlights_commit_exempt_e.htm#country.

[1011] The Borgen Project, 'Truth About Poverty in Chile', 2017, https://borgenproject.org/tag/poverty-in-chile/.

[1012] Reuters, 'Peru poverty rate rises for first time in 16 years: government', 2018, https://www.reuters.com/article/us-peru-poverty/peru-poverty-rate-rises-for-first-time-in-16-years-government-idUSKBN1HV2L2.

[1013] ResearchGate, 'Strategies for Bridging the Internet Digital Divide in Peru: A Benchmarking of South Korea and Chile, 2016, https://www.researchgate.net/publication/308994735_Strategies_for_Bridging_the_Internet_Digital_Divide_in_Peru_A_Benchmarking_of_South_Korea_and_Chile.

[1014] Enrique Hinostroza, Pedro Hepp, Ernesto Laval, 'Enlaces: The Chilean ICT Experience in Education', http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.109.102&rep=rep1&type=pdf.

Peru is trying to follow a similar path by promoting Internet access as far as resources permit and by liberalizing the telecoms sector. In 2013, mobile network operators were required to sell space to mobile virtual network providers (MVNOs) and, in 2014, customers were able to keep their phone numbers when migrating service providers.[1015] Soon after the Ministry of Transportation and Communications along with the regulator Supervisory Agency for Private Investment in Telecommunications (OSIPTEL), was under pressure to allow facilities sharing of mobile cell-site towers.[1016] OSIPTEL has already issued a license to low-cost new entrant from Viet Nam, Viettel Mobile in 2012. By 2015, there were seven mobile operators in the market.[1017] With the advent of newer technology, there is even the possibility of Peru leapfrogging into an era of broadband Internet. Using a 4G OpenRan technology a new model for telecoms development is being trialed by a PPP between Telefónica del Perú, Facebook, the IADB and Central Bank of Latin America (CAF) called 'Internet para Todos' (Internet for All – IPT) which aims to connect people with no access in more than 30,000 rural locations in Peru.[1018] By December 2019, Peru announced more than a million people across 7,400 communities in coastal, mountainous and jungle-covered parts of the economy has been connected by the initiative.[1019]

D. Innovative policy approaches, including TVWS, help to close the digital divide

In 2016, a drive towards universal high-speed broadband was launched, accompanied by a drive to plug the gaps where signals and fiber were not available. This effort, particularly for the benefit of MSMEs[1020] and isolated groups, ranges from big cities, such as the Smart Seoul Network project which aims to achieve 100 percent coverage for citizens and visitors,[1021] to coverage of villages in rural areas and fishing communities.

Among the regulatory steps taken by Korea to achieve universal service and access to the Internet is the introduction of spectrum-free usage of the unused or under-used TV white spaces in UHF transmissions, otherwise known as TVWS technology, to provide coverage in remote landscapes. The use of spectrum-free licensing is gaining in popularity globally to provide

[1015] Peru Reports, 'Low-cost providers shake up Peru's telecommunications industry', 2015, https://perureports.com/low-cost-providers-shake-up-perus-telecommunications-industry/1593/.
[1016] Tower Exchange, 'MNOs call on towercos to provide power in Peru', 2017, https://www.towerxchange.com/mnos-call-on-towercos-to-provide-power-in-peru/.
[1017] Peru Reports, 'Low-cost providers shake up Peru's telecommunications industry', 2015, https://perureports.com/low-cost-providers-shake-up-perus-telecommunications-industry/1593/.
[1018] CAF, 'Internet for All" to benefit 6 million Peruvians with 4G mobile internet and close digital divide by 2021', 2019, https://www.caf.com/en/currently/news/2019/06/internet-for-all-to-benefit-6-million-peruvians-with-4g-mobile-internet-and-close-digital-divide-by-2021/.
[1019] Mobile World Live, 'IpT Peru scheme expands OpenRAN sites', 2020, https://www.mobileworldlive.com/featured-content/top-three/ipt-peru-scheme-expands-openran-sites/.
[1020] R.D. Atkinson, 'The Real Korean Innovation Challenge: Services And Small Businesses in Korea's Economy 30 Korea Economic Institute of America and the Korea Institute for International Economic Policy', 2015, http://keia.org/sites/default/files/publications/kei_koreaseconomy_2014_2-23-16_final.pdf.
[1021] Korea Times, 'Seoul to become free WiFi city', 2019, https://www.koreatimes.co.kr/www/nation/2019/10/281_276745.html.

universal coverage in remote areas and to provide emergency communications where networks are down due to natural disasters. As analogue TV shifts towards digital TV transmission, swathes of frequencies in the VHF and UHF wavebands are becoming available, and the long-distance propagation of such frequencies are ideal for large but sparsely populated areas. One company with this spectrum free license is Innonet (see Box 5.22).

Box 5.22: Innonet and the use of spectrum-free licensing

The use of TVWS globally is restricted to the unused broadcast frequencies in the VHF and UHF bands, the key point being that the low power of these transmissions will not interfere with adjacent radio and TV broadcasts yet the frequencies themselves are suitable for long-range coverage of areas of low population using non-line-of-sight (NLos) technology that works well even in poor atmospheric conditions. So long as there are fiber backhaul networks available to connect the traffic from the TVWS access points in remote areas to the economy-wide networks—in the case of Innonet, they are required to be within 1Km or beyond 10Km—this can be an effective and low-cost way to provide Internet coverage and to provide emergency back-up when mobile networks are down, for example, as a result of an earthquake or typhoon. The regulator decided against the need for a license given no interference of signals, and in general a regulator can waive fees to promote coverage to underserved areas. However, when radio and TV migrate to digital transmissions, these frequencies are likely to be re-allocated to mobile networks.

According to Innonet the reasons behind the decision to permit the use of TVWS stem first, from a commitment to democratize access to the Internet through a drive to provide public Wi-Fi throughout poorly served areas; second, from a need to provide low-cost connectivity for IoT by introducing innovative licensing; third, the use of a regulatory sandbox to experiment with unlicensed use of spectrum and the need to avoid radio interference. Given that TVWS costs far less to provide than LTE cellular network access it is ideal for low rates of usage in remote areas, for example, for use on a smart farm. Korea was in fact the first economy to experiment with a TVWS plan.[1022] There are now 48 local governments using TVWS operated by companies like Innonet.

Innonet is a TVWS operator, and in an interview Dr Hosang Yoo, CEO[1023] explained Innonet had been awarded five Korean Certifications (KC-certification) to provide wireless services in remote areas. The UHF band, being low frequency, offers very good propagation over wide areas even at low power to avoid interference with broadcast signals. Dr Yoo is hoping to apply for certificates overseas, for example to the FCC in the US, to expand the market of Innonet.

[1022] The Unwired People, 'YV white spaces (finally) open in Korea', 2012, https://theunwiredpeople.com/2012/01/19/tv-white-spaces-finally-open-in-korea/

[1023] TRPC Interview (5 July 2020) Hosang Yoo, CEO and Founder, Innonet

Source:

- ET News, 'Innonet Conducts Tests to Experiment TV White Space Wi-Fi Service', 2020, http://english.etnews.com/20200622200002

Roll Out of 5G Replicates Telecoms Success

Korea has become a role model for other economies not only in its achievement of technological prowess, which may not be easily replicated in its scope, but in the importance of the principle of being highly focused upon what can be achieved. For example, because Korea had already become a world leader in broadband by 2019, it has also taken the global lead in installing 5G cellular networks.[1024]

This is the driver in Korea, as elsewhere, for 5G development: a means to preserve and enhance the economy's international competitiveness, but also to lay the foundations for the next phase of the Information Society, or Industry 5.0. If Industry 4.0 is about Internet-linked automated industrial systems (the Internet of Everything or IoE) Industry 5.0 is about new ways in which human society seamlessly interacts with these systems.[1025]

Korea's model for 5G follows its previous telecom investment models with government working closely with the operators as part of the digital transformation of the economy, including:

- In 2015, the Korean Strategic 5G Promotion Committee, comprised of members from both public and private sectors, drafted the 5G+ Strategy, which unequivocally aspires to spawn development in key industries that will generate new services and produce USD 152 billion in gross national output and export volume of USD 73 billion by 2026. A crucial element of the strategy was to prioritize the allocation and assignment of spectrum by auction.[1026]
- New infrastructure sharing polices are also lowering the costs of 5G, despite initial opposition from the incumbent operator.[1027]
- Following a meeting with the MSIT in July 2020, SK Telecom, KT and LG Uplus have agreed to invest a total of KRW 25.7 trillion (USD22 billion) through to 2022 to boost 5G infrastructure.
- The MSIT has also declared its support for 5G as part of a 'Digital New Deal' including tax credits and tax reductions to help achieve an increase in coverage of the economy

[1024] EFF, 'Why Is South Korea a Global Broadband Leader?', 2020, https://www.eff.org/deeplinks/2020/02/why-south-korea-global-broadband-leader.
[1025] Master Control, 'Industry 5.0: Top 3 Things You Need to Know', July 2020, https://www.mastercontrol.com/gxp-lifeline/3-things-you-need-to-know-about-industry-5.0/.
[1026] World Bank Blogs, '5G in Korea: lessons for the developing world', February 2020, https://blogs.worldbank.org/eastasiapacific/5g-korea-lessons-developing-world.
[1027] EFF, 'Why Is South Korea a Global Broadband Leader?', March2020, https://www.eff.org/deeplinks/2020/02/why-south-korea-global-broadband-leader.

from 14 percent to 70 percent by 2025.[1028] The MSIT pointed out that the technologies most closely associated with Industry 4.0—such as artificial intelligence (AI), Internet of Things (IoT), sensor networks and Big Data analytical tools—will all use 5G.

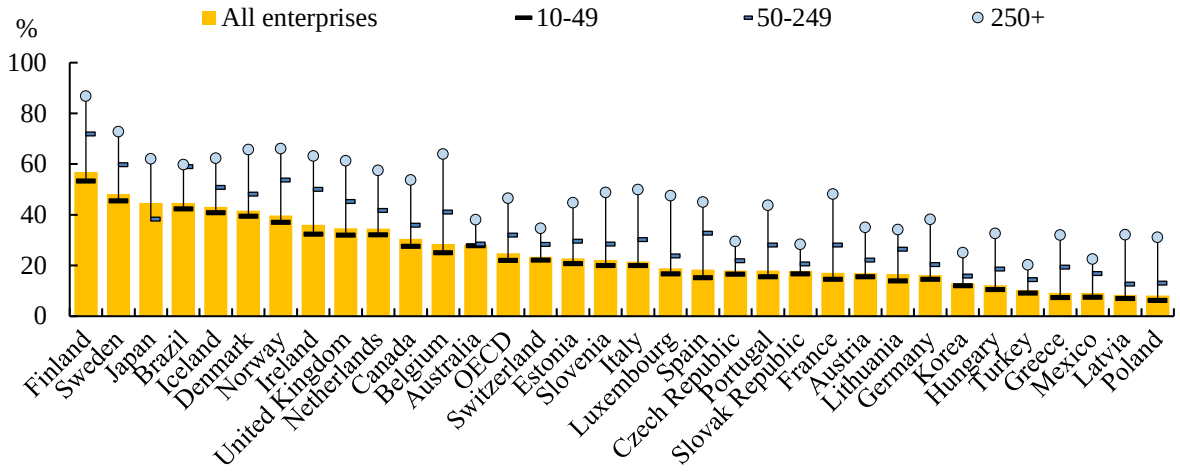
Advanced IT Infrastructure Lags Due to Lack of Digital Usage and Skills

In contrast to Korea's global leadership in broadband infrastructure and development of hardware, Korea lags in its more advanced IT infrastructure, such as the infrastructure for high-performance computing, blockchain and autonomous driving,[1029] and the uptake of these digital technologies, which will inevitably result in a drag on the adoption of digital applications—crucial for continued and sustained inclusive digital economy growth.[1030]

Korea is thirteen places below the OECD average in the uptake of digital technologies by enterprises (see Figure 5.4) especially lagging is uptake by SMEs, but even large firms fall behind. Further, there is a gap in digital skills in the workforce compounded by a mismatch where "around 63% percent of Korean workers are not well matched to their job",[1031] with many staff in IT departments lacking necessary training. MSIT (formerly MSIP)'s 2017 'Mid-to Long-Term Master Plan in Preparation for the Intelligent Information Society Managing the Fourth Industrial Revolution' notes these private sector concerns regarding the underdevelopment of the IT infrastructure and shortage of experts in the field.[1032] Further, the 2019 National Strategy for AI, which has a focus on software and AI research and teaching in schools and universities, is pointed to as it will "not only to create new jobs but also help those who want to switch jobs."[1033]

[1028] RCRWireless News, 'South Korean operators to invest $22 billion in 5G networks by 2022', July 2020, https://www.rcrwireless.com/20200716/5g/south-korean-operators-invest-22-billion-5g-networks-2022.
[1029] TRPC Interview (26 August 2020) Ray Jo, Microsoft, Korea.
[1030] OECD, 'Digitalisation: An Enabling Force for the Next Production Revolution in Korea', 2017, https://www.oecd.org/publications/digitalisation-an-enabling-force-for-the-next-production-revolution-in-korea-9789264285545-en.htm.
[1031] OECD, 'Digitalisation: An Enabling Force for the Next Production Revolution in Korea', 2017 https://www.oecd.org/publications/digitalisation-an-enabling-force-for-the-next-production-revolution-in-korea-9789264285545-en.htm.
[1032] MSIP, 'Mid- to Long-Term Master Plan in Preparation for the Intelligent Information Society Managing the Fourth Industrial Revolution', 2017, http://english.msip.go.kr/cms/english/pl/policies2/__icsFiles/afieldfile/2017/07/20/Master%20Plan%20for%20the%20intelligent%20information%20society.pdf.
[1033] TRPC Interview (26 August 2020) Ray Jo, Microsoft, Korea.

Figure 5.4: Korean firms lag significantly in the uptake of key digital technologies



Source: Adapted from the OECD (2017) Digital Economy Outlook 2017.

Although Korea was the first economy to adopt a 'Cloud First Policy' in 2015—through the Act on the Development of Cloud Computing and Protection of its Users (the Cloud Computing Act)[1034]—and operates certain restrictions (such as: i) limiting government cloud procurement to Korean companies; ii) until 2020 restricting financial institutions' use of cloud where sensitive personal data is involved, such as information pertaining to bank accounts; and iii) a localization requirement that such data cannot be stored or transferred outside of Korea), the limited advanced IT infrastructure and insufficient numbers of trained professional engineers in Korea has left a vacuum to be filled by foreign investors.[1035] Among the first to build their own cloud facilities were the chaebols, with many foreign players such as Amazon Web Services (AWS)—who has been present in the economy since 2012—IBM, and Microsoft, initially leasing data centers to provide services. With Google set to enter the market in 2020, this leaves around 30 percent of the market to local CSPs.

In an interview with the director of the Asia Pacific Centre for ICT, he made the point that the main hindrance to further accelerating the cloud computing infrastructure had been "security concerns, the public sector's policy for network segregation between internal and external networks, and each industry level regulations. These factors also considered affecting negatively on the related industries and ecosystem."[1036] Given that Korea is highly dependent upon investment by the private sector in the cloud infrastructure and technologies, and with a

[1034] Ministry of Science and Technology Information and Communication (Internet Promotion Division), English Law provided by Korea Legislative Research Institute, Act on the Development of Cloud Computer and Protection of its Users, [Act No.13234, 27 March 2015, Enforcement Date 28 September 2015]', http://www.law.go.kr/lsInfoP.do?lsiSeq=169562&lsId=012266&chrClsCd=010202&urlMode=engLsInfoR&viewCls=engLsInfoR#0000.

[1035] The Korea Times, 'Korea has long way to go in cloud computing', 2019, https://www.koreatimes.co.kr/www/tech/2019/04/133_267386.html.

[1036] TRPC Interview (24 August 2020) Mr Kiyoung Ko, Director, APCICT.

forecast 16 new data centers due to be built during 2020,[1037] Korea is taking steps to improve and attract investment into a new digital infrastructure, including:

- In June 2020, MSIT announced steps to strengthen both the cloud infrastructure and to utilize data from the digital economy for the promotion of AI as part of the Digital New Deal to revitalize the economy following COVID-19,[1038] by setting goals for domestic cloud transformation, promoting public sector cloud use, as well as strengthening the domestic cloud industry ecosystem, particularly SMEs, through the use of AI, IoT, and blockchain.
- Steps are being taken to update the Digital Services Contract procurement system,[1039] together with a 'SME Support Project cloud fund' providing KRW 3-20 million (USD 2,526-16,841) per company to help businesses transition to the cloud, and the promotion of a 'cloud flagship business' to increase the quality and expansion of cloud services, all ensuring a local cloud industry ecosystem that enables that domestic cloud companies to actively participate in the public and private cloud transformation journey.
- Further, the opening up of the banking and financial services sector (with the Financial Services Commission (FSC) starting January 2021, loosening restrictions on the financial services sector storing personal data in the cloud) and enablement and use of data (with the amendment to the Network Act and Personal Information Protection Act to allow anonymized personal data to be more widely used in areas such as healthcare, finance and digital government)[1040] create and incentivize opportunities for players.[1041]

Conclusion

Korea has placed much emphasis upon universal access to Internet services and in closing the digital divide, illustrates the importance of consistent long-term planning, and creating the right advisory and policy instruments according to the level of development. The experience of Korea is also an example of policies carefully calibrated to foster the use of new technologies, such as broadband mobile Internet, TVWS, and cloud computing. Korea has shown a balance between prudence with concerns for security issues on the one hand (e.g., caution about the financial services market storing sensitive personal data in the cloud), with services innovation. Given Korea's commitments to the WTO on the telecommunications side, and a recent cautious opening of the banking and financial services use of cloud, Korea remains attractive for international enterprise investment and provides a platform for cross-border digital trade that stands to benefit MSMEs, as well as larger businesses. However, on the IT side, especially with

[1037] W.Media, 'Why South Korea is a perfect place to set up a data center', 2020, https://w.media/news/why-south-korea-perfect-place-data-center/.

[1038] MSIT, 'Data Economy and Cloud Industry in preparation for the AI Era', June 2020, https://www.msit.go.kr/web/msipContents/contentsView.do?cateId=_policycom2&artId=2940227.

[1039] MSIT, 'Establishment of specialized contract system to drive the growth of the digital service industry', June 2020, https://www.msit.go.kr/web/msipContents/contentsView.do?cateId=_policycom2&artId=2938310.

[1040] W.Media, 'Why South Korea is a perfect place to set up a data center', 2020, https://w.media/news/why-south-korea-perfect-place-data-center/.

[1041] Korean Tech Today, 'Korean Tech Companies Leverage On Banks For Their Cloud Computing Services', 2019, https://www.koreatechtoday.com/korean-tech-companies-leverage-on-banks-for-their-cloud-computing-services/.

restrictions such as government cloud procurement regulations, Korea remains not entirely open to foreign investments.

Mexico

This case study of Mexico highlights efforts to achieve both universal services and to close the digital divide as the economy becomes digital through: (i) initial and revitalised telecoms reform; (ii) establishing independent regulators to promote and ensure competition; (iii) policy approaches to ensure competition and coverage, including addressing interconnection charges between the dominant broadband carrier and its competitors—which in turn led to the regulator applying economic principles to asymmetric regulation—enhanced connectivity mandates, and public-private partnerships (PPP).

Mexico's Need for Broadband Infrastructure, and Competition

Broadband coverage and Internet usage are essential if Mexico is to develop a digital economy. By the time of the reforms of 2012 (outlined below), Mexico was among the lowest rankings of the OECD index for Internet penetration rates, with just 26 percent of households with Internet access. In the richer regions such as Sonora, Baja California, Nueva Leon, and in Mexico City, one in four households had Internet access, but in poorer provinces such as Oaxaca, Chiapas and Guerrero, the average was one in ten.[1042]

In order to address its growing need for broadband infrastructure and connectivity for all, Mexico has taken a number of steps including:

- First, WTO membership spurred initial telecoms reform, with the 2012 General Election resulting in further reforms being made;
- Second, the establishment of independent regulators as part of the 2012 reforms addressed market restraints and promoted competition (for example, by addressing interconnection charges);
- Third, doubling down on its connectivity for all mandate through the Broadband for All program, through public-private partnerships (PPP), and through the National Development Plan 2019-2024 (PND).

A. WTO commitments and telecoms reform

Mexico's WTO commitments accelerated and reinforced the need for telecoms reform—which was initially achieved by: i) raising the ceiling on foreign investment in telecommunications service providers from 40 percent to 49 percent; ii) opening up all telecom retail services; and enabling the ceiling of 49 percent on mobile service providers to be raised "subject to prior

[1042] Juan Manuel Mecinas Montiel, 'Mexican Law Review - The Digital Divide In Mexico: A Mirror Of Poverty', Vol. IX, No. 1, 2016, https://revistas.juridicas.unam.mx/index.php/mexican-law-review/article/view/10432.

authorization"[1043]—but it was not until the 2012 General Election that a landmark shift towards a more open and competitive telecommunications environment occurred. The use of Internet during the election debates, and the President commitment to an inclusive digital agenda resulted in: [1044]

- Launching of the National Digital Strategy (NDS) in 2013, a plan for the following five years to promote digitalization in government; in the economy-at-large; in education; in the health sector; and to encourage civic innovation and citizens' participation.[1045]
- Establishment of the Federal Telecommunications and Broadcasting Law and the Federal Institute of Telecommunications (IFT) in 2014.[1046]
- A National Development Plan 2019-2024 (PND) was introduced as Mexico's fourth plan for transformation with a strong focus upon infrastructure, including to further build and maintain a Federal Government telecommunications infrastructure.[1047]

This reform program, which is driven by the election promise of achieving universal service, is underpinned by Mexico becoming the first economy in the world to make Internet access a constitutional right, with the government seen as the main provider.[1048]

B. Establishment of independent regulators to address competition

In Mexico, over 60 percent of the telecom markets—fixed and mobile—are dominated by América Móvil, which owns fixed-line operator Telmex and mobile operator Telcel. To address this, Mexico appointed independent regulators with the authority to promote competition:

- The enactment of the 2014 Federal Telecommunications and Broadcasting Law began the process of making new entry into the markets easier and established the IFT as a regulator with strong independent powers, including those to ensure competition in the sector.
    - In an interview, the IFT highlighted that the Law empowers IFT to apply asymmetric regulation to the dominant carrier (e.g., América Móvil), designated as the *Agente Económico Preponderante en Telecomunicaciones* (AEPT), related to "the unbundling of the local loop, interconnection, network

[1043] WTO, 'Mexico', 1997, https://www.wto.org/english/tratop_e/serv_e/telecom_e/telecom_highlights_commit_exempt_e.htm#country.

[1044] OECD, 'Reforming telecommunications in Mexico', 2017, https://www.oecd.org/about/impact/reforming-telecommunications-in-mexico.htm.

[1045] OECD, 'Digital Platforms and Competition in Mexico 2018', 2018, http://oe.cd/dpc.

[1046] Juan Manuel Mecinas Montiel, 'Mexican Law Review - The Digital Divide In Mexico: A Mirror Of Poverty', Vol. IX, No. 1, 2016, https://revistas.juridicas.unam.mx/index.php/mexican-law-review/article/view/10432. https://www.reesearchgate.net/publication/309465699_The_digital_divide_in_mexico_a_mirror_of_poverty.

[1047] The National Law Review, 'Mexico's 2019-2024 National Development Plan', August 2019, https://www.natlawreview.com/article/mexico-s-2019-2024-national-development-plan.

[1048] The Conversation, 'Mexico wants internet access for all. Getting everyone online could reduce poverty too', November 2018, https://theconversation.com/mexico-wants-internet-access-for-all-getting-everyone-online-could-reduce-poverty-too-104206.

infrastructure sharing, dedicated links, roaming and capacity commercialization to Virtual Mobile Operators (VMO)."[1049]

- Further, under the Law, the Secretariat of Communications and Transport (SCT) has responsibility to pursue the goals of universal service with an obligation to publish annually its progress.

- The Federal Competition Commission (COFECE) which was created to implement the 2013 Federal Economic Competition Law (LFCE) has been designated the authority to promote competition in the digital economy, similar to the IFT's role in telecoms. Its mission is to promote competition for the benefit of society and for "the well-being of families" and to follow a Code of Ethics and Conduct for objectivity and transparency in line with the 2014-2017 Strategic Plan.[1050]

However, the digital economy raises a raft of new issues, such as data security and data privacy, the use of Big Data, new market structures such as platform businesses which can easily dominate e-commerce markets, consumer protection, the introduction of new technologies, and these issues overlap between traditional telecommunication markets such as mobile broadband Internet (which would normally fall under the authority of the IFT), and the emerging markets for digital products and services (many of which are cross-border markets and as digital markets they could be seen as falling under the authority of COFECE). For example, in 2019 the First Collegiate Court Specialized in Economic Competition, Broadcasting and Telecommunications was called upon to rule which regulator had jurisdiction over a merger review of Uber, a ride-sharing digital platform, and a local company, Cornershop. It ruled COFECE should take responsibility. To avoid further confusion, the IFT proposed to establish a Technical Policy Committee for the Digital Environment to coordinate with other regulatory bodies including COFECE.[1051]

C. Approaches taken to ensure competition

The roles and responsibilities of the IFT and the SCT, including a number of initiatives that they have undertaken, are in pursuit of ensuring universal service and promoting competition. For example:

- The IFT issues licenses and sets the price floor for frequency auctions. The IFT has ruled in favor of net neutrality and the obligation of carriers to protect consumer data (but also to store it for up to 24 months and make it available to authorities within 48 hours).
- The SCT establishes concessions to be administered along with licenses by the IFT. Carriers that hold more than one concession can apply to consolidate them into a single renewable 30-year concession. Resellers of telecom services, including Mobile Virtual

[1049] TRPC Interview (7-10 September 2020) Ms. Jimena Sierre Navarrete, Director of International Affairs, on behalf of Mr. Juan Carlos Hermandez Wocker and Ms. Citalli Invonne Garcia Gonzales, IFT.
[1050] COFECE, 'Home Page', https://www.cofece.mx/en/about-cofece/.
[1051] ILO, 'Institutional cooperation to address competition challenges of digital economy', December 2019, https://www.internationallawoffice.com/Newsletters/Competition-Antitrust/Mexico/SAI-Law-Economics/Institutional-cooperation-to-address-competition-challenges-of-digital-economy.

Network Operators (MVNOs) need only obtain a 10-year license from the IFT, but fixed and mobile operators need to secure an SCT concession.

- The SCT is also responsible for telecom and broadcast radio policies and content issues, along with satellite resources where satellite landing stations are only required to have a license, whereas previously they required a concession.
- There are no restrictions on foreign investments where they are confined to telecoms, but a 49 percent ownership ceiling on broadcasting stations reducible to the levels pertaining in the investors' jurisdiction of domicile.[1052]

The aims of these policies is to match the expectations of domestic and foreign investors, and above all to improve economy-wide connectivity, promote effective competition and protect consumer rights.[1053]

Interconnection charges between networks are an added cost that disadvantage smaller competitors (see Box 5.23). With government intent on lowering the cost of entry into the market, the Federal Telecommunications and Broadcasting Law introduced a provision to reduce interconnection charges to zero between the carrier designated as 'predominant'[1054] and other carriers. As regulator, the IFT took steps to implement the new law, however in 2017, the Supreme Court declared these zero rated provisions unconstitutional.[1055] While asymmetric pricing was specifically allowed for under the Law, the Supreme Court upheld the view that the Law designated decision-making directly to the IFT rather than Congress (who drafted the Law),[1056] and the IFT therefore either needed to make its own case or to introduce changes to the Law.[1057] This offered the IFT an opportunity to use economic principles to determine an interconnection charge based upon long run incremental costs (LRIC)[1058] which would preserve the incentive of the incumbent carrier to invest in its network while simultaneously lowering the interconnection charges.[1059] The charges were subsequently revised

[1052] Lexology – Baker McKenzie, 'Telecoms in Mexico', 2018, https://www.lexology.com/library/detail.aspx?g=092404d3-a2ed-409f-b590-744008c64d9e.

[1053] OECD, 'Digital Platforms and Competition in Mexico 2018', 2018, http://oe.cd/dpc.

[1054] While the Mexican Anti-Trust Law designates dominance to companies in specific markets, the sector-specific regulations require a designation of pre-dominance. Ibid.

[1055] Baker McKenzie, 'The Federal Institute of Telecommunications Issues the Interconnection Rates Applicable for 2019', 2018, https://www.bakermckenzie.com/en/insight/publications/2018/12/interconnection-rates-applicable-for-2019.

[1056] Reuters, 'Mexico regulator says America Movil can charge competitors for calls', 2017, https://www.reuters.com/article/us-mexico-telecoms/mexico-regulator-says-america-movil-can-charge-competitors-for-calls-idUSKBN1D300U.

[1057] Bnamericas, 'Court rules in favor of Telcel in zero interconnection rate dispute', 2017 https://www.bnamericas.com/en/news/court-rules-in-favor-of-telcel-in-zero-interconnection-rate-dispute.

[1058] LRIC measures only the additional costs to the incumbent that are incurred by investing in parts of the network that are to be opened to competitors, preventing the cumbent from inflating interconnection charges by passing on costs incurred by other parts of the network.

[1059] TRPC Interview (31 August 2020) Mtra. Adriana Labardini Inzunza, Former IFT Commissioner.

downwards,[1060] and further downwards in 2018, applicable from 2019.[1061] In fact, under the influence of the reforms, the costs of the OECD's 'low usage basket' (100 calls and 500 Megabytes of data) fell by 65 percent in Mexico between 2012 and 2016 while users increased by 50 million.[1062] The IFT's drive to increase the level of competition seems to have been effective.

One of the important achievements of the IFT was to rely upon economic methodology in regulatory decisions. The use of economics that takes into account the effects of regulation on investment, on business incentives and on end-user affordability is important and needs to figure in trade-related considerations. Among the economic tools used by the IFT to measure the degree to which markets are dominated by just one or a few firms—a proxy for the degree of effective competition—is the Herfindahl-Hirschman Index (HHI) which in 2019 for mobile telecoms was 4,558, well above the threshold of 2,500 that is considered the upper limit for a competitive market. In the fixed line market it was 3,547. Internet access was little better at 3,396.[1063] Only in the subscription TV market is there a different dominant player, Televisa, because the 1990 Concession to América Móvil is limited to telecoms and the Internet.[1064] The OECD report for 2017[1065] recommended that the pay TV market be opened to competition from América Móvil and others, clearly with an eye upon the future digitalisation of TV transmission by satellite or terrestrial broadcast, cable or streaming. As Mexico strives to overcome its digital divide in terms of access, it also has to turn attention to the universal availability of services and applications over the infrastructure.

The steps taken by IFT do appear to have reduced the dominance of the AEPT. Based on data provided by the IFT,[1066] while the company is still in the market pole position, América Móvil's share of the mobile broadband market fell from 82 percent to 70 percent 2013-2019, and in the fixed broadband market from 73 percent to 51 percent over the same period. In the total mobile market for example, its share of subscribers in 2019 was 62 percent, down from 69 percent in 2013. Notable also is the difficulty MVNOs have in creating a market for themselves at only 1.7 percent market share, and only slightly higher in the mobile broadband market at 2.1 percent.

[1060] Reuters, 'Mexico regulator says America Movil can charge competitors for calls', 2017, https://www.reuters.com/article/us-mexico-telecoms/mexico-regulator-says-america-movil-can-charge-competitors-for-calls-idUSKBN1D300U.

[1061] Bnamericas, 'Mexico publishes new telecom interconnection tariffs for 2019', 2018, https://www.bnamericas.com/en/news/mexico-publishes-new-telecom-interconnection-tariffs-for-2019.

[1062] OECD, 'Digital Platforms and Competition in Mexico 2018', 2018, http://oe.cd/dpc.

[1063] Data provided by Mtra. Adriana Labardini Inzunza, The HHI $=S1^2+S2^2+S3^2+\ldots Sn^2$ where S = market share of firm 1, 2,3 … N. The market shares of each firm are squared and added. Anything below 2,500 is considered competitive to some degree. However it is important to carefully define the market. In a platform economy this can become very difficult because many services are available at no cost so an alternative measure is required.

[1064] Media Ownership Monitor: Mexico, 'Carlos Slim Helú', March 2019, https://mexico.mom-rsf.org/en/owner/individual-owners/detail/owner/owner/show/carlos-slim-helu-1/.

[1065] OECD, 'Reforming telecommunications in Mexico', 2017, https://www.oecd.org/about/impact/reforming-telecommunications-in-mexico.htm.

[1066] TRPC Interview (7-10 September 2020) Ms. Jimena Sierre Navarrete, Director of International Affairs, on behalf of Mr. Juan Carlos Hermandez Wocker and Ms. Citalli Invonne Garcia Gonzales, IFT.

As outlined above, Telmex and Telcel (being two markets conjoined as a sector) are considered in the terminology of the IFT to be pre-dominant,[1067] and as fast broadband Internet replaces earlier generations of telecoms, and flat-rate pricing for Internet access replaces timed calls, it is arguable that interconnection charges between these networks and their competitors will become a thing of the past.

Box 5.23: Interconnection

If a network has N subscribers, then the maximum possible number of connections between any two subscribers in the network is (N-1) N or N^2-N. For example, a network with 1,000 subscribers would have 1,000,000 – 1,000 = 999,000 connections. The addition of one more subscriber (1,001) would create 1,001,000 possible connections, a difference of 2,000 over the previous level. The larger the network the greater the margin of new connections for every new subscriber. This is known as network economics, a form of economies of scale, where size adds cumulative potential revenues. It is easy for a telecoms network that enjoys strong economies of scale to reach an unassailable position as a monopoly, what is often referred to as a natural monopoly because its monopoly power does not necessarily rely upon having an exclusive license or favorable treatment by a government, although historically the two have often gone together.

To create a more open competitive market it is crucial that the new entrants can access the subscribers of the larger network to give them a choice to switch networks or to subscribe to at least some of their services. This requires the right to interconnect. Dominant carriers usually oppose mandatory interconnection and will raise objections ranging from technical difficulties to loss of control over the network in which they have invested. Regulators will demand interconnection if they want to open the market. This sometimes goes under the name of equal access by which all bona fides carriers (usually licensed) can interconnect, but there are a host of issues to be overcome, including at which points of the network the interconnection takes place, as this can affect the interconnection charges (if there are any) – for example, for a long distance call if the interconnection is at the caller end then the connecting network has to cover the cost of the long distance as well as the far end call deliver – and the quality of the interconnection, for example should it just involve low bandwidths or include high-speed bandwidths. The opportunities for dominant carriers to make interconnection difficult are almost endless and often a disputes resolution process is required unless the regulator is prepared to impose a determination.

The advent of broadband Internet has changed just about everything in the telecommunications markets. While owning a broadband network remains an important source of business for the carriers, not least because there is a substantial growth in the backhaul of mobile traffic and IPTV services can be marketed over broadband, access to the

[1067] While the Mexican Anti-Trust Law designates dominance to companies in specific markets, the sector-specific regulations require a designation of pre-dominance, http://www.oecd.org/daf/competition/digital-platforms-and-competition-in-mexico-2018.htm.

Internet effectively by-passes the need for much of the network interconnections. The Internet by definition interconnects everyone on it, unless there are local restrictions imposed by regulators. But in IT networks the same network economics principles apply, for example, if banks interconnect their ATM networks it means customers can send and receive funds to and from any other customer of any other bank. The same holds true for online payments networks. The important *additional* point is that the applications that allow funds and files to be transferred between networks can only work if the networks involved are also inter-operable. They need APIs (application protocol interfaces) that work with each other.

D. Connectivity mandate furthered with Broadband for All program, PPP, and PND

While reforms have improved coverage, they have not improved Mexico's OECD rankings among 28 economies. In broadband mobile penetration rates Mexico remains fifth from bottom, and third from bottom for fixed broadband penetration rates and Internet speeds.[1068] In absolute terms and according to World Bank figures for 2018, over 95 percent of the population have broadband mobile phones, 15 percent fixed broadband, over 60 percent using the Internet.[1069] On the contrary, according to OECD data, broadband mobile subscriptions per 100 population have increased from 16 in 2012 to over 77 by 2019.[1070]

Further improvements in Internet and broadband coverage across Mexico is hindered by the problem that serving most of the rural and more remote areas is uneconomic for the private carriers, and all the retail carriers are private. Besides América Móvil, other economy-wide carriers are AT&T Mexico and ALTÁN Redes (part owned by JP Morgan) operating the 4G Red Compartida network, together with twelve MVNOs.

It has proved very difficult for MVNOs to survive, and by 2018 while there were reportedly over 15 different service providers, they were mostly local and with less than 2 percent of the mobile market between them.[1071] While there is no universal rule as to the optimum number of mobile network operators—as opposed to MVNOs—who can profitably survive in a market, and there are plenty of exceptions, the wisdom of the industry often suggests three. For example, this was a frequent number among OECD economies in 2015.[1072]

[1068] OECD, 'Broadband Portal', 2019, https://www.oecd.org/sti/broadband/broadband-statistics/.
[1069] The World Bank, 'Mobile cellular subscriptions (per 100 people) – Mexico', 2018, https://data.worldbank.org/indicator/IT.CEL.SETS.P2?locations=MX.
[1070] OECD, 'Broadband Portal', 2019, https://www.oecd.org/sti/broadband/broadband-statistics/ .
[1071] Bnamericas, MVNOs in Mexico: How have they performed in 2020?, 2020, https://www.bnamericas.com/en/features/mvnos-in-mexico-how-have-they-performed-in-2020.
[1072] OECD, 'Working Party on Communications Infrastructures and Services Policy - Wireless Market Structures and Network Sharing', 2015, https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP(2014)2/FINAL&docLanguage=En.

An economic analysis carried out in 2019 concluded that there was no strong business case for investment in a new mobile broadband operator given the capital and maintenance costs of building a network, but a pure MVNO gaining at least 1 percent market share could operate profitably, and a hybrid MVNO leasing 80 percent of its network capacity and building the remaining 20 percent would require a market share of 4.5 percent to be profitable.[1073] Another economic analysis examines Mexico's digital divide by segmenting the economy into zones A, B and C where zone A which covers around 83 percent of the population would be profitable to serve if the supply was forthcoming, zone B covers 9.2 percent of the population and the supply of broadband Internet would be viable if appropriate incentives were available to private networks but the level of demand may need to be encouraged with lower prices, and zone C covers the remaining 7.3 percent of the population who are low income and live in difficult locations where only government subsidy could provide services.[1074]

To address this Mexico has put in place further policy measures to address its connectivity mandate, including:

- SCT launching the Digital Connectivity: Broadband for All program in 2017;
- Red Compartida wholesale public-private partnership (PPP) commencing in 2017; and
- The PND setting out a guiding principle of "leave no one behind, leave no one outside" and further outlining a target to raise the penetration of broadband Internet connectivity from under 70 percent to 100 percent.[1075]

The Digital Connectivity: Broadband for All program complies with the sixth article of the Constitution that guarantees the right of access to information technologies, services and the right to digital inclusion.[1076] The program aims to promote access to an affordable broadband infrastructure, including a shared trunked broadband data network run by Telecommunications de Mexico, or CFE Telecomunicaciones e Internet para Todos—CFE Telecommunications and Internet for All—as a subsidiary of the Comisión Federal de Electricidad (CFE, Federal Electricity Commission). CFE Telecommunications will "create subsidiaries and participate in partnerships and alliances" as President López Obrador aims to expand internet reach from 87 percent in 2019 to 95 percent when his presidential term ends in 2024.[1077] In 2019, the CFE

[1073] Promtel, 'Proposals For Investment Projects For The Provision Of Mobile Broadband Services', 2019, https://www.gob.mx/cms/uploads/attachment/file/439680/Resumen_Ejecutivo_estudio_de_inversi_n.pdf.

[1074] Martin Cave, Rubén Guerrero, Elisa Mariscal, 'Bridging Mexico's digital divide: an inside-out/outside-in view of competition and regulation', 2018, http://ceeg.mx/publicaciones/ESTUDIO_2_2018-Bridging_Mexicos_digital_divide_Final_2018_12_20.pdf.

[1075] SCT, 'Programme of SCT 2020-2024', 2019, https://www.gob.mx/cms/uploads/attachment/file/565614/Programa_Sectorial_de_Comunicaciones_y_Transportes_2020-2024.pdf.

[1076] Gobierno de Mexico, 'Digital Connectivity Program: Broadband for All', 2017, https://www.gob.mx/telecomm/articulos/programa-de-conectividad-digital-banda-ancha-para-todos-96391?idiom=es.

[1077] CapacityMedia, 'Mexico to set up national 'Internet for All' company to expand rural coverage', 2019, https://www.capacitymedia.com/articles/3824047/mexico-to-set-up-national-internet-for-all-company-to-expand-rural-coverage.

awarded a license to Red Troncal to build a Mexico optical fiber backbone and CFE Telecommunications will lease the fiber to offer and deliver non-profit telecoms services.[1078]

Further, as part of the Broadband for All program, the IFT will allow network sharing between mobile broadband networks. In addition, free broadband Internet will be made available to schools, health centers, libraries and other public places and spaces. Analogue TV will give way to Digital TV, thus freeing up spectrum for expansion of mobile broadband using lower frequencies which can more effectively serve rural areas, a satellite program will be expanded, which again can help serve rural or remote areas, for example through Vsat technology,[1079] and a campaign has been launched to spread digital literacy and science and technology courses, such as robotics. The 2014 Law also added restrictions on the incumbent preventing it from using its broadband investment to offer linear TV services. This has benefitted the national broadcaster Televisa as companies prepare for the digital age and the coming of streamed services and Over-the-Top (OTT) programming.

In addition, the use of PPP models for infrastructure projects is relevant for all APEC economy considerations, and Red Compartida is a particularly interesting wholesale public-private partnership (PPP) network between América Móvil on the private side and the Telecommunications Investment Promotion Agency (PROMTEL) on the public side. It started in 2017 as a USD7 billion privately funded project, and aims to cover at least 92.2 percent of the population in Mexico with the most advanced mobile services.[1080] Specifically, it aims to cover at least 70 percent of the population by January 24, 2022 and 92.2 percent by January 24, 2024.[1081] The network, which began operations in 2018, offers retail carriers wholesale opportunities to apply most recent technologies, such as 4GLTE or 5G. The wholesale network operates on the 700 MHz band wave which gives extensive coverage in the least populated areas.[1082]

Red Compartida's current reach is a little over 50 percent[1083] and while it has signed Shared Network agreements with 48 service providers, including 17 offering broadband and telephony services to end users,[1084] it has been unable to date to attract MVNOs to use its network with

[1078] Lexology, 'Internet for everyone?', June 2019, https://www.lexology.com/library/detail.aspx?g=4e7cbc05-81d5-4e53-be73-4910d458225f.
[1079] PR Newswire, 'Viasat Helps Bridge the Digital Divide in Mexico with Affordable, Fast Satellite-Enabled 'Community Wi-Fi' Service', April 2018, https://www.prnewswire.com/news-releases/viasat-helps-bridge-the-digital-divide-in-mexico-with-affordable-fast-satellite-enabled-community-wi-fi-service-300626101.html.
[1080] ITU, 'Red Compartida', 2017,, https://www.itu.int/net4/wsis/archive/stocktaking/Project/Details?projectId=1514835212.
[1081] TRPC Interview (7-10 September 2020) Ms. Jimena Sierre Navarrete, Director of International Affairs, on behalf of Mr. Juan Carlos Hermandez Wocker and Ms. Citalli Invonne Garcia Gonzales, IFT.
[1082] The Law Reviews, 'The Technology, Media and Telecommunications Review – Edition 10; Mexico', 2019, https://thelawreviews.co.uk/edition/the-technology-media-and-telecommunications-review-edition-10/1211265/mexico.
[1083] TRPC Interview (31 August 2020) Mtra. Adriana Labardini Inzunza, Former IFT Commissioner.
[1084] TRPC Interview (7-10 September 2020) Ms. Jimena Sierre Navarrete, Director of International Affairs, on behalf of Mr. Juan Carlos Hermandez Wocker and Ms. Citalli Invonne Garcia Gonzales, IFT.

the exception of a fixed-wireless network.[1085] For example, in 2019, Telefonica's mobile network entered an MVNO agreement with AT&T, not Red Compartida.[1086] Reports in 2020 suggest Telefonica may withdraw completely from the Mexico market,[1087] which is perhaps a sign of slow revenue growth in a market dominated by a duopoly.

IFT Commissioners pointed out that the prices of telecom services even at higher speeds has fallen by nearly 29 percent from June 2013 to December 2019, and "taking into account Mexico has had an inflation of 29.8 percent" this means "a difference higher than 50 percent between telecom and other products in the Mexican market."[1088] All these indicate that Mexico is moving in the right direction.

Conclusion

The post-2012 General Election reforms—including the establishment of a proactive independent regulator—have had a significant impact in terms of driving up coverage and reducing costs, especially of broadband mobile. As the IFT Commissioners put it: "The Constitutional Reform Decree has in this sense, propelled the penetration of telecommunication services along with wider broadband Internet service coverage for Mexicans."[1089] Nevertheless, Mexico remains far below the OECD average for broadband Internet. Legal and jurisdictional issues arise quite frequently in Mexico (such as the case of interconnection), and while these are part of due process, ways need to be found to reduce the procedural delays when it comes to socially important issues such as policies to promote investment in universal services for rural and remote communities. A commitment to achieve universal service also needs the use of economic regulatory tools that preserve incentives to invest, especially in times of economic uncertainty. The preservation of an independent regulator is also very important for effective policy implementation. The connectivity mandate should be progressed through SCT's Digital Connectivity: Broadband for All program, alongside further PPPs.

Chinese Taipei

The case study of Chinese Taipei highlights the need for both: i) strong international telecoms connectivity with the rest of the world due to the economy's high reliance upon international

[1085] However, the IFT commissioners do "expect that the Shared Network project, along with existing regulation, will have visible effects on competition by encouraging the entry of new operators…" TRPC Interview (7-10 September 2020) Ms. Jimena Sierre Navarrete, Director of International Affairs, on behalf of Mr. Juan Carlos Hermandez Wocker and Ms. Citalli Invonne Garcia Gonzales, IFT.

[1086] Reuters, 'Telefonica teams up with AT&T in Mexico in new bid to take fight to Slim', November 2019, https://www.reuters.com/article/us-mexico-telefonica/telefonica-teams-up-with-att-in-mexico-in-new-bid-to-take-fight-to-slim-idUSKBN1XV2CM.

[1087] BuddeCom, 'Telefónica makes moves to exit the Mexican telecom market', February 2020, https://www.globenewswire.com/news-release/2020/02/10/1982231/0/en/Telef%C3%B3nica-makes-moves-to-exit-the-Mexican-telecom-market.html.

[1088] TRPC Interview (7-10 September 2020) Ms. Jimena Sierre Navarrete, Director of International Affairs, on behalf of Mr. Juan Carlos Hermandez Wocker and Ms. Citalli Invonne Garcia Gonzales, IFT.

[1089] TRPC Interview (7-10 September 2020) Ms. Jimena Sierre Navarrete, Director of International Affairs, on behalf of Mr. Juan Carlos Hermandez Wocker and Ms. Citalli Invonne Garcia Gonzales, IFT.

IT supply chains; and ii) domestic universal broadband access to support SMEs, which make up the majority of businesses.

Imperative of Telecommunications Infrastructure

Creating a universally accessible and affordable domestic telecommunications infrastructure to support the growing need to use the Internet has become a strategic objective in its own right for Chinese Taipei. Due to the economy's high reliance upon international IT supply chains, the government makes it a priority to assist SMEs in developing their domestic B2B and B2C e-commerce capacity, which includes extending broadband Internet to rural and remote areas where both SMEs and communities living in mountainous regions can benefit.

This overarching objective has noticeably driven policy and regulatory reform in Chinese Taipei, including:

- Initial introduction of competition reforms in 1988, which led to the opening up of fixed and mobile markets,[1090] laid the foundation for WTO membership, and further encouraged the establishment of the National Communications Commission (NCC), an independent regulator;[1091]
- Setting out a real commitment to a fair and more equal and inclusive society within the Digital Nation & Innovation Economic Development Plan (DIGI+) 2017-2025;[1092] and
- Currently, has shifted the focus towards service quality and innovation, including a focus on developing cloud infrastructure.

A. WTO and an Open Market

Since 1949, Chinese Taipei has been under constant pressure to open and maintain trading relations with as many other economies as possible. Membership of the WTO was a natural step for the economy, and followed many years of introducing competition reforms in the market, starting with the liberalization of the customer premises market in 1988 and leading to the 1996 Telecommunications Act[1093] which set the stage for the incorporation and eventual privatization of Chunghwa Telecom (CT) and the subsequent opening up of the fixed and mobile markets.[1094] In accordance with the WTO's Reference on Regulatory Reform, Chinese

[1090] John Ure, 'Telecommunications Development in Asia', HKU Press, Chapter 12, 2008, https://hkupress.hku.hk/pro/868.php.

[1091] China, 'The National Communications Commission Organization Act', Last amended 28 December 2011 https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=P0000008.

[1092] DIGI+ 2017-2025 Vision, https://digi.taiwan.gov.tw/#vision.

[1093] There is no online version of the original Act but for the 2013 revised Act see Law and Regulations Database, Telecommunications Act: China, 'Telecommunications Act', Last amended 11 December 2013, https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=K0060001.

[1094] John Ure, 'Telecommunications Development in Asia', HKU Press, Chapter 12, 2008, https://hkupress.hku.hk/pro/868.php.

Taipei in 2006 created the National Communications Commission (NCC) as an independent regulator.[1095] This progressive opening up of the telecoms markets is set out in Table 5.1.

Chinese Taipei committed to open all its telecom markets, with the proviso agreed in 2001 that "Investment in telecommunications services will be limited to 20 percent per person but can reach 60 percent if the investment is part of a joint-venture with an individual from Chinese Taipei. Other than the investment requirements, there are no restrictions on supplying value-added telecommunication services."[1096] The privatization of CT also allowed these terms to apply to the dominant fixed-line carrier.

Table 5.1: Sequence of Telecommunications reforms in Chinese Taipei, pre-1996–2008

Reform Initiative	Pre 1996	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008
Paging service liberalised														
Basic telecommunications legislation														
2G mobile market licensed														
Fixed-line market liberalised														
3G mobile market liberalised														
Acceded to the WTO														
Incumbent operator privatised														
Converged regulator (telecommunication + broadcasting) established														
Wireless broadband access (Wimax) licensed														

Note: The basic legislation, the Telecommunications Act, established the pro-competition regulatory regime; the Organizational Act, the independent regulator; and the Incorporation Act, the incumbent operator.

Source: APEC PSU (2011), Chapter 19: Telecommunications in Chinese Taipei, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiPvu-riJDrAhUdyDgGHQVPDjUQFjAAegQIARAB&url=https%3A%2F%2Fwww.apec.org%2F-%2Fmedia%2FAPEC%2FPublications%2F2011%2F1%2FThe-Impacts-and-Benefits-of-Structural-Reforms-in-Transport-Energy-and-Telecommunications-Sectors%2FTOC%2FTelecommunications-in-Chinese-Taipei.pdf&usg=AOvVaw37G-bZZaMeSfNU1y5P1f69.

[1095] China, 'The National Communications Commission Organization Act', Last amended 28 December 2011, https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=P0000008.

[1096] WTO, 'WTO successfully concludes negotiations on entry of the Separate Customs Territory of Taiwan Penghu, Kinmen and Matsu (Chinese Taipei)', 2001, https://www.wto.org/english/news_e/pres01_e/pr244_e.htm.

B. Further policy and regulatory reform results in commitment to closing the digital divide

Despite the structural and licensing reforms, complementary investments in broadband were at first not so forthcoming. The levy of interconnection charges between the big three Internet Service Providers (ISPs) dampened usage demand for Internet services, such that by 2012 the NCC issued a statement acknowledging Internet-access services in Chinese Taipei "have degenerated into long-term market failure, and that as a result of poor efficiency in internet exchange centers, the development of broadband networks has been stagnant." [1097] To reverse the situation the NCC abolished the Internet interconnection charges between three telco companies, thereby freeing up demand for Internet-based services. Currently there are five Internet Exchange Points,[1098] and five competing mobile broadband service providers, and at least one report suggests Chinese Taipei excels in 4G and in video content delivery. Only in terms of Mbps do the operators lag slightly behind other Asian economies, such as 20-30Mbps rather than 40Mbps.[1099] 5G licenses have been issued to each of the operators, and two new entrants, TStar and Asia Pacific Telecom.[1100] By 2020 the determination of the NCC to see market competition between well-resourced local carriers has resulted in island-wide coverage of broadband Internet as Table 5.2 illustrates.[1101] The NCC stated that the process was very much aided by the good working relationship between the NCC and the operators.[1102] Although no direct subsidies are provided, and the operators are willing to make island-wide investments, under the DIGI+ programme a scheme of matching funds is available for broadband to rural areas using funds from the 5G spectrum auction.

Table 5.2: Broadband Internet Coverage

Service	Penetration (2018)
Broadband mobile (3G + 4G) coverage	100% of population
Broadband fixed line coverage	24% population
Internet coverage	89% of households
Internet usage	86% population
Tariffs[a] for mobile broadband as % GNI	0.28 prepaid and 0.31 post-paid

Note: '[a]' refers to the numbering being based upon 30 outgoing calls per month plus 100 SMS.
Source: NCC - Telecommunications indicators 2016-2018, https://www.ncc.gov.tw/english/files/20010/802_200106_1.pdf.

[1097] ILO, 'NCC decided on free internet interconnections', 2012, https://www.internationallawoffice.com/Newsletters/Tech-Data-Telecoms-Media/Taiwan/Shay-Partners/NCC-decided-on-free-internet-interconnections.
[1098] TeleGeography (2020) Internet Exchange Map, https://www.internetexchangemap.com/#/building/22675.
[1099] Open Signal, 'Taiwan-Mobile Network Experience Report June 2019', 2019, https://www.opensignal.com/reports/2019/06/taiwan/mobile-network-experience.
[1100] Taipei Times, 'Taiwan Star, Asia Pacific Telecom obtain 5G licenses', 2020, https://www.taipeitimes.com/News/biz/archives/2020/07/30/2003740785.
[1101] NCC, 'NCC - Telecommunications indicators 2016-2018', Last accessed 6 October 2020, https://www.ncc.gov.tw/english/files/20010/802_200106_1.pdf.
[1102] TRPC Interview (28 August 2020) Dr. Yeali S. Sun, NCC Commissioner.

As explained by the NCC Department of Planning, "Chinese Taipei has been actively investing in the construction of network infrastructures with a view to enhancing ubiquity of the broadband internet. Currently, almost 100 percent of the households can obtain access to 100 Mbps high-speed broadband network. In addition, in recent years, Chinese Taipei has consistently ranked in the top 20 of world digital competitiveness ranking by the IMD."[1103]

The commitment to a fair and more equal and inclusive society was clearly spelt out in the Digital Nation & Innovation Economic Development Plan (DIGI+) 2017-2025 which "aims to enhance digital infrastructure, re-construct a service-based digital government, and realize a fair and active internet society with equal digital rights" as components of becoming a Smart Island.[1104] The promotion of 5G is very much part of DIGI+ and seen as a precursor to Industry 4.0 development throughout the economy. According to the NCC, the early applications of 5G will likely be by enterprise. [1105] The 5G spectrum auctions raised TWD100 billion (USD3 billion) which will go towards a matching funds scheme for rural broadband development, where the last mile will frequently consist of WiFi. DIGI+ also outlines a programme to raise digital literacy at all levels of education from primary school to post-graduate studies including adding an infrastructure of networked computers. The Ministry of Education also runs Digital Opportunity Centres in areas where many families do not have access to computers.[1106] The digital themes were further expounded in the NCC's Communications Policy White Paper, issued February 2020.[1107] The paper goes beyond the development of high-speed broadband access to a host of digital applications and services that is building upon it, including for example the role of OTT services which range from messaging services to platform businesses to digital content and media services.

Importantly, in July 2020, the Telecommunications Management Act came into effect.[1108] The new Act which replaces the 1958 Act and its subsequent amendments, removes the regulatory siloes between telecom networks and broadcast and streamed services, and shifts the focus from how to create the infrastructure to how it is to be used to provide innovative services, from basic communications to advanced data analytics, from information services to social media and entertainment. Indeed, Article 1 of the new Act indicated that it was enacted to ensure the sound development of the telecommunications industry, to encourage innovative services, to facilitate fair market competition, safe and reliable telecommunications infrastructure, to ensure the reasonable use and efficiency of resources, to improve technological development and interconnection applications, and to protect the rights and interests of consumers.

[1103] TRPC Interview (13 August 2020) Ms. Li Pei-fen, Department of Planning, NCC.

[1104] DIGI+ 2017-2025 Vision, https://digi.taiwan.gov.tw/#vision.

[1105] China, 'Telecommunications Management Act', 2019, https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=K0060111.

[1106] MOFA, 'Taiwan Digital Opportunity Center (TDOC) Project', 2016, https://nspp.mofa.gov.tw/nsppe/news.php?post=104415.

[1107] NCC (2020) Communications Policy White Paper, https://www.ncc.gov.tw/chinese/files/20032/5237_42741_200320_1.pdf.

[1108] Law and Regulations Database (June 2019), Telecommunications Management Act, https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=K0060111.

C. Continued reliance on international connectivity has encouraged innovation policy shift

As outlined above, the high level of dependency upon cross-border B2B transactions gives strategic importance to Chinese Taipei's international telecommunications and cloud infrastructure. By early 2020, there were 15 submarine cables serving the island, and seven landing stations. Besides the domestic carriers CT and FarEasTone Telecom, several international consortia own and operate the cables. Both Facebook and Google have significant investments in several of them, including those connecting directly to the United States which adds social media and multi-media capacity to the domestic market. Google also owns two hyperscale data centers on the island.[1109] However, unlike other Asia 'tiger' economies, most of the world's leading IT companies were slow to invest in data centers in Chinese Taipei and as result many SMEs rely upon CSPs who lease space rather than run their own data centers.[1110] Chinese Taipei recognized it was falling behind in cloud computing and in 2010 launched the Cloud Computing Application and Development Project. The motivation behind this project was to increase Chinese Taipei's "market share of hardware solutions in cloud computing data centres and their added value."[1111] The projects consists of two components: [1112]

- First, to help domestic companies participate in government projects, to link the cloud computing industry to government service applications, to integrate services across government departments, and to link government resources and services to business and citizens; and
- Second, to stimulate the adoption of cloud across industry.

The results have been positive in two respects. First, it has stirred an interest in the adoption of cloud and therefore investment in cloud. Second, the relaxation of regulations has made the cloud environment much more friendly to investors. For example, AWS, IBM and Microsoft, have each invested in AI and IoT research labs, and Google committed in 2019 to invest TWD 26 billion (USD 851 million) in expending its data centers.[1113] Microsoft has also partnered with local carriers to offer AZURE services.[1114]

Conclusion

Recognizing the strategic importance of the international market and international telecommunications to the island's economy, Chinese Taipei reformed its telecoms sector from

[1109] Submarine Cable Networks, 'Cable Landing Stations', 2020, https://www.submarinenetworks.com/stations/asia/taiwan

[1110] GoodFirms, 'Top Cloud Computing Companies in Taiwan', https://www.goodfirms.co/cloud-computing-companies/taiwan.

[1111] TRPC Interview (27 August 2020) Dr. Tzi-Cker Chiueh, Vice President & Gen. Director of Information and Communications Research Laboratories (ICL), ITRI.

[1112] Sheng-Chi Chen, 'An Experience of Taiwan Policy Development To Accelerate Cloud Migration', 2014, https://pdfs.semanticscholar.org/d65c/40165967d10b54ef59d3828d735ad80c3565.pdf.

[1113] Nikkei, 'Google boosts Taiwan data center plans with $850m investment', 2019 https://asia.nikkei.com/Business/Technology/Google-boosts-Taiwan-data-center-plans-with-850m-investment.

[1114] DigiTimes, 'Microsoft launches Azure ExpressRoute service in Taiwan', 2019, https://www.digitimes.com/news/a20190327PD200.html.

the 1990s, hence creating the conditions to apply for WTO membership, including the establishment of NCC, an independent regulator. When market liberalization was not enough to ensure investment in broadband, the NCC moved to abolish Internet interconnection charges which lowered usage costs and set the scene for a shift from a traditional telecom market to much more competitive and innovative broadband Internet market that has attracted investments from companies such as Facebook and Google, and encouraged a shift in focus towards innovation with the launch of the Cloud Computing Application and Development Project.

Key Lessons

Both Korea and Chinese Taipei have created world class high-speed broadband infrastructures to support Internet access, in turn supporting and sustaining digital economy growth and e-commerce participation. On the other hand, Mexico has created an independent regulator with pro-active powers to create a more open and competitive telecoms market with a focus upon bringing broadband Internet to everyone. These learnings can inform other economy approaches, including taking into account the following considerations:

1. **Consistent long-term planning** (such as reforming of traditional telecoms markets, and the creation of independent regulators) will ensure both fair and free competition. This planning should be **supported by close collaboration between the public and private sectors**, including the setting up of specialist research institutes with input from both academia and industry to bolster long-term consistency.
2. **Creating an independent regulator** with real powers to open the markets to competitive entry, for example by reducing the interconnection charges the dominant carrier can impose on competitors.
3. **Investment in infrastructure with competitive universal access in mind**—especially to remote locations—and adjusting licensing laws and regulations accordingly (such as facilities sharing).
4. **Encouraging the development and adoption of cloud computing** which enables third parties to offer e-commerce platforms to SMEs, is especially important for overseas markets, and for the application of data analytics. Likewise, keeping a non-protectionist approach to government procurement and taking a precautionary but measured approach to data storage issues.

6 FINAL REMARKS

This study has been designed to contribute to the current WTO negotiations on e-commerce as well as the capacity building activities that may arise from it. A primary component is a review of publicly available submissions issued by WTO members since 2018, where WTO members elaborated their negotiating approach as well as the elements they believe should be included and discussed in the exploratory work and eventual agreement on e-commerce.[1115] Although it should be acknowledged that these public submissions may not be reflective of all the elements that would be in the eventual agreement, particularly given the acceleration of e-commerce activities driven by Covid-19, these submissions help provide clarity on the aspects that WTO members collectively view as critical in facilitating e-commerce.

Categorizing these elements into 6 focus areas, namely: A (electronic transactions framework); B (openness and cross-border related issues); C (consumer protection and privacy issues); D (cybersecurity/network security); E (infrastructure-related aspects); and F (market access), and using them as a basis of assessment, this study finds that there are variations in the state of economies' laws, regulations and initiatives.

Pertaining to Focus Area A (Electronic Transactions Framework), on the call in many submissions that it is important to allow contracts to be concluded electronically and to ensure that e-contracts have the same legal effect as their paper counterparts, analysis has shown that while e-contracts are widely recognized in APEC economies as valid and enforceable, they have not been found to be entirely sufficient for all forms of legal instruments. Regarding the call in several submissions that electronic payment regulations should be flexible and in line with the rapid advancement of technology and business models, it has been observed that some APEC economies have adopted a broad definition of electronic payment, while others have opted for a narrower definition. On recognizing e-invoicing standards that enhance efficiency, accuracy and reliability of e-commerce transactions, analysis found that in addition to several APEC economies having mandated or encouraged such adoption through their laws, economies have also participated in multilateral frameworks to promote interoperability.

With respect to Focus Area B (Openness and Cross-Border Issues), specifically on the call by several submissions that data-related measures are least trade restrictive and at the same time, fulfil valid public policy objectives, analysis shows that many APEC economies have established conditions under which data exports of personal data can occur and/or are allowed. Additionally, some economies are part of the international/regional frameworks that regulate or facilitate cross-border data transfers including the APEC CBPR System. At the same time, some APEC economies have introduced requirements regarding the location of computing facilities as well as data retention and storage requirements. Regarding the call by some submissions that there should be competition-related regulations to ensure that online platforms do not abuse their market position, analysis observed that although most APEC economies

[1115] The reader should note that there is a set of submissions that are not public. This study does not include the analysis of these submissions.

have competition laws in place, only a handful of economies have undertaken specific efforts to adapt competition laws to the digital environment, particularly addressing competition issues associated with online platforms. Pertaining to issues related to intermediary liability, analysis found that most APEC economies have a conditional liability regime and definition of an intermediary varies considerably across economies.

On Focus Area C (Consumer Protection and Privacy Issues), regarding the call in some submissions that members put in place regulations to protect online customers from fraudulent and deceptive commercial activities, analysis indicated that while consumer protection laws in APEC economies broadly cover e-commerce transactions, only a few have made specific references to e-commerce or have legislations devoted to it. Pertaining to the call by some submissions that members adopt measures to protect consumers from SPAM, analysis noted that many APEC economies have enacted laws to deal with it. However, variations can be observed in areas such as how consent is defined and what constitutes as SPAM. On the call in several submissions for a balanced approach towards data-related regulations and which noted members' right to regulate for valid public policy objectives, analysis found that most APEC economies have introduced laws on data privacy and protection, but they differ in terms of what is defined as personal information as well as the principles under which personal data can be processed.

Pertaining to Focus Area D (Cybersecurity/Network Security), on the call of some submissions that members strengthen their capabilities to prevent and respond to cybersecurity incidents, analysis noted that different APEC economies have cybercrime legal frameworks embedded in their criminal laws. Additionally, a large number of APEC economies have also developed strategies to protect themselves against cyber threats. At the same time, it was observed that not many APEC economies have cybersecurity laws to deal with a larger set of issues including the protection of Critical National Information Infrastructure.

On Focus Area E (Infrastructure related aspects), regarding the call in several submissions that members continue work on promoting connectivity and bridging the digital divide, analysis found that most APEC economies have adopted full market entry liberalization for their GATS commitments on telecommunication services. Many have also made more commitments through free trade agreements. Pertaining to the Telecommunications Reference Paper, although all APEC economies had adopted it, some have adopted a modified/reduced version, while others have adopted additional commitments.

With regards to Focus Area F (Market Access), specifically on improving access to ICT-related goods, analysis noted that most APEC economies have joined the WTO Information Technology Agreement (ITA). At the same time, it was noted that few APEC economies have put in place regulations pertaining to encryption and other aspects such as those requiring licensing of electronic/IT products, which could have an inadvertent impact on market access. Moreover, although most APEC economies do not tie market access to the provision of product proprietary information, there are still economies that do so. On services, while most or all

APEC economies have made commitments in their GATS schedules and/or through their trade agreements, there continues to be variation in the extent of liberalization at the MFN level.

Given the above, it can be surmised that capacity building activities are needed across all focus areas to assist economies in realizing the elements identified in the eventual agreement. Generally, the capacity building activities that APEC can consider undertaking could benefit two groups of economies, namely: 1) economies that do not yet have the necessary laws, regulations and initiatives pertaining to specific elements/aspects to develop one (e.g., e-invoicing, competition policies related to online platforms, cybersecurity laws); and 2) economies that already have existing laws, regulations and initiatives so that they can fine-tune them to better facilitate e-commerce.

In terms of the area/theme that these capacity building activities could cover, one area/theme worth exploring would be encouraging the adoption of international standards, practices, guidelines and recommendations in economies' laws and regulations. As an illustration, for economies looking to develop or fine-tune laws and regulations pertaining to electronic signatures, it may be beneficial to have capacity building activities built around the Model Law on Electronic Commerce (MLEC) and the Model Law on Electronic Signatures (MLES) developed by UNCITRAL. For economies exploring the development of laws and regulations pertaining to open data, capacity building activities aimed at introducing international frameworks related to it could be useful (e.g., Open Government Partnership, Open Data Charter). Similarly, for economies considering the development of domestic cybercrime laws and regulations, capacity building activities built around international instruments such as the Budapest Convention on Cybercrime would be helpful.

A related area/theme would be to improve mutual recognition and interoperability among the laws, regulations and initiatives that economies have put in place. For instance, considering that various APEC economies have created single windows within their own economies, it is arguably more sensible to work on enhancing interoperability among existing systems, as opposed to building from scratch a common system for all participating economies. Similarly, although economies have built flexibilities for cross-border data flows within their domestic laws, variation in specific requirements among these laws continue to entail significant costs for firms operating in multiple jurisdictions. One solution to minimize this is through advocating the adoption of some form of mutual recognition (e.g., APEC CBPR), whereby a firm fulfilling the data privacy regulations of one economy is regarded as meeting those of other economies which are part of the mutual recognition system.

Another area/theme to be considered is on strengthening international cooperation with regards to specific aspects of e-commerce. As an illustration, the increase in cross-border e-commerce is likely to lead to an increase in transactions-related issues between buyers and sellers located in different economies. This will likely result in challenges for local consumer protection laws. Therefore, it would be advisable to better understand how international cooperation can be enhanced to tackle issues such as cross-border consumer protection efficiently. Likewise, considering that cybercrimes and cybersecurity incidents are likely to be transnational in nature,

it would be worthwhile to have capacity building activities focusing on how international cooperation in such areas (e.g., cross-border access of information by law enforcement agencies) can be further augmented.

The rapid developments driven by digitalization has made it imperative that economies are responsive and many have risen to the challenge by instituting new approaches to regulations, including the use of technology to facilitate process. For example, economies have introduced fintech regulatory sandboxes to encourage the development and adoption of newer technologies in the payment sector. Such sandboxes generally allow for time-bound testing of innovations under the oversight of regulators. Economies are implementing middle-ground approaches to data-related regulations which on one hand, would promote the growth of data-utilizing businesses such as those in the e-commerce sector, while on the other hand, would enable governments to achieve public policy objectives, such as data security and privacy. Economies are also exploring innovative approaches to address digital divide, including the use of TVWS technology to provide wireless services in remote areas. It would be helpful to have capacity building activities focusing on these new approaches to regulations.

Although it is important to ensure that economies have the necessary framework to facilitate e-commerce, equally important if not more is to ascertain that these laws, regulations and initiatives are practical, reasonable and therefore, can be operationalized efficiently. For example, as the series of case studies has shown, it is critical that in the process of developing them, economies endeavor to engage with various stakeholders and balance their varied interest. Once they are in place, one option economies can undertake to encourage adoption and raise awareness is through educational outreach. During implementation, economies also need to ensure that measures are continuously monitored so that they can be evaluated and improved upon. Capacity building activities aimed at sharing some of these valuable experiences could go a long way in supporting economies' efforts in developing or fine-tuning their e-commerce-related policies and initiatives.