

How APEC can address restrictions on cross-border data flows

Joshua P. Meltzer

Senior Fellow, Global Economy and Development, Brookings Institution

This report was commissioned by the APEC Business Advisory Council (ABAC) and ABAC Malaysia¹.

¹ This report was delivered to ABAC in July 2020 under the guidance of ABAC Chair Dato Rohana Tan Sri Mahmood and ABAC Digital Innovation Working Group Co-Chair Robert Milliner. The opinions expressed in this report are those of the author. They do not purport to reflect the views of ABAC or ABAC Malaysia.

Executive Summary

Within APEC, cross-border data flows are transforming international trade, creating new opportunities for participation in the global economy. Use of data and digital technologies such as AI should also drive increased productivity and economic growth.² APEC has already recognized the importance of the digital economy, including in the 2017 APEC Leaders Declaration which called on APEC to work together to release the potential of the internet and the digital economy. APEC has developed an Internet and Digital Economy Roadmap and APEC Cross-Border E-commerce Facilitation Framework and in 2018, APEC established the Digital Economy Steering Group.

Despite the elevation of digital issues within APEC, cross-border data flows are increasingly being restricted within the APEC region. Data flow restrictions in APEC have grown from one such regulation in 1988 to seventy-three in 2020. There has been a particularly large increase in the number of regulations over 2013-2019, from twenty-three regulations restricting cross-border data flows in 2013 to seventy-one such regulations in 2019, an increase of over 300 percent.

In APEC, the restrictions on cross-border data flows are in pursuit of a range of regulatory goals, in particular privacy, security, competition (which covers restrictions aimed at helping a domestic industry), internet access and control and financial regulation and law enforcement. Privacy is by far the main reason for data flow restrictions in APEC, counting for over 40 percent of regulation. Internet access and control is the second most salient reason for restricting data flows, accounting for 22 percent, followed closely by financial regulation at 20 percent, security at 11 percent and competition at 2 percent.

Restricting data flows to achieve a range of regulatory goals has a couple of key underlying drivers. One is the regulatory concern that allowing data to be transferred to a third country will undermine domestic regulatory standards. This is a key rationale for restrictions on transfers of personal data and is at play for various security focused regulations. Another regulatory concern driving data restrictions is that without data being localized, regulators won't have access to the information needed to do their job. This leads to many of the regulations requiring the financial sector to localize data. A third driver is the impact of access to information on political and social stability, and competition.

APEC regulations affecting cross-border data flows are also of different levels of restrictiveness. However, growth in data flow restrictions have been most pronounced in regulation that are medium and most restrictive. Looking at the last 20 years, least restrictive data flow regulations – almost all of them privacy laws – have increased from one in 2000 to fourteen in 2020. In contrast, over this period, regulations with medium levels of data flow restrictiveness have gone from zero in 2000 to thirty-one in 2020, and the most restrictive cross-border data flow

² Erik Brynjolfsson et al., "Artificial Intelligence and the Modern Productivity Paradox: A Clash of Expectations and Statistics", NBER Working Paper no. 24001, October 2017 (revised December 2017), p. 10

regulations have increased from four in 2000 to twenty-eight in 2020. To put it another way, in 2020, twenty percent of data flow restrictions were least restrictive, forty-two percent were of medium restrictiveness and thirty-eight percent were most restrictive.

While almost all APEC economies have regulations restricting cross-border data flows, there are four APEC economies that account for the largest number and the most restrictive regulations: China, Indonesia, Russia and Vietnam. Korea also has a high number of medium-restrictive regulations.

The focus of APEC on the opportunities of data for trade and economic growth requires addressing the growth in restrictions on cross-border data flows. The following outlines a work program for APEC aimed at addressing the underlying drivers of such data flow restrictions.

- First, APEC should update the Bogor goals to include the free flow of data. Already 14 APEC economies have made a commitment in FTAs to cross-border data flows. APEC should aim to include such a commitment in all future FTAs and as part of an eventual FTAAP. To support this goal, APEC should develop a work program in two key areas.

Building trust in cross-border data flows

- The first work program should aim to support domestic implementation of regulation that can build trust in cross-border data flows, addressing the regulatory drivers to restrict data flows where it undermines achievement of domestic regulatory goals. Initially, the focus should be on privacy, consumer protection and cybersecurity.
- As part of this agenda, APEC should aim to minimize regulatory heterogeneity amongst APEC economies by doing two things. The first is developing APEC-wide international standards that can be a basis for domestic regulation, as has been done in the privacy, space where the APEC Privacy Framework is a baseline for APEC economy privacy laws. Second, APEC needs to expand its existing work on aligning domestic regulation with international standards to include standards and domestic regulation affecting cross-border data flows.
- APEC can also make progress minimizing data flow restrictions by expanding its work on good regulatory practice to include cross-border data flows. This should include working with regulators on achieving the following:
 - Conducting a regulatory impact assessment for all new regulation that includes the impact on cross-border data flows.
 - Enhance transparency, consultation and reason-giving within APEC with respect to data flows. This could include publishing in advance regulations affecting data flows, explaining the rationale for the regulation, agreeing to consider alternatives,

providing all interested parties with opportunities to comment on proposed regulations and publishing reasons for the final approach taken.

- Assessing whether there are ways of achieving the regulatory goal in a way that is least restrictive on cross-border data flows.
- Expanding existing work in APEC on developing and improving coordination mechanisms across government agencies to also account for data

Expand international regulatory cooperation to develop interoperability mechanisms

- This second work stream is aimed at regulatory cooperation and development of interoperability mechanisms that can enable cross-border data flows. With the APEC Cross-Border Privacy Rules (CBPRs), APEC has already made significant progress on developing an interoperability mechanism that allows personal data to flow across borders notwithstanding different privacy laws amongst APEC economies. Given the ongoing importance of privacy as a driver of cross-border data flow restrictions, APEC should update CBPR, in part to address the impact of EU adequacy findings under GDPR on the ability of business to use CBPR. This could involve updating the Privacy Framework to minimize differences with GDPR and increasing the bindingness of CBPR. FTAs amongst APEC economies could include commitments to having privacy regulation based on the Privacy Framework and to complying with CBPR for transfers of personal data.
- Building on experience with CBPR, APEC should consider developing an interoperability mechanism to address restrictions on data flows caused by security and consumer protection. Progress here will be facilitated by progress with the first work stream as APEC economies implement domestic regulation based on international standards or regulate in ways that minimizes unnecessary regulatory heterogeneity within APEC. Interoperability mechanisms can follow the CBPR model, building mechanisms for oversight and enforcement to ensure compliance by business with underlying standards.
- Another area where APEC should focus is on giving confidence to regulators that having data reside outside their borders will not undermine regulatory capacity and law enforcement, another driver of data flow restrictions. USMCA and the US-Japan digital trade agreement include commitments that balance the need for access to data with a commitment not to require data to be localized. APEC should aim to extend this solution across APEC. However, as much of the data that regulators need is held by private business, this will require participation of the private sector. APEC could focus initially on building trust that such commitments to access will work. For instance, when it comes to access to financial data held by banks and other financial institution, APEC could develop financial data sharing and access principles agreed to by governments and the private sector. These principles could then form the basis for MOUs between APEC regulators and the private sector institutions holding the data.

Introduction

Within APEC, the ability to transfer data globally is transforming international trade, creating new opportunities for participation in the global economy, particularly for developing countries and SMEs. Use of data and digital technologies such as AI should also drive increased productivity and economic growth.³

APEC has already recognized the importance of the digital economy. For instance, the 2017 APEC Leaders Declaration called on APEC to work together to realize the potential of the internet and the digital economy. APEC has established the APEC Digital Economy Roadmap and APEC Cross-Border E-commerce Facilitation Framework and in 2018, APEC established the Digital Economy Steering Group.

Despite the elevation of digital issues within APEC, cross-border data flows are increasingly restricted. This paper focuses on the role of cross-border data flows for international trade and provides policy recommendations which could inform part of the digital economy work of APEC. The paper proceeds as follows; Part 1 outlines what is meant by data and the growth in cross-border data flows, Part 2 discusses the impact of data and data flows on economic growth and trade, Part 3 analyzes APEC regulations affecting cross-border data flows, the scope of the regulations and levels of restrictiveness, Part 4 assesses what could constitute an APEC program aimed at supporting data flows within APEC, and Part 5 concludes.

1. The internet, data and its online collection

What is data?

Data can be distinguished from information, knowledge and wisdom. Figure 1 shows a data-information-knowledge-wisdom pyramid.⁴ This schematic is useful as it distinguishes data, which refers to raw facts and figures as well as text, words, statements, pictures and video, from information which consists of value extracted from data. Higher levels of value-add include knowledge which provides the know-how and tends to be action orientated, and wisdom, which deals with values and how to exercise judgement.⁵

³ Erik Brynjolfsson et al., "Artificial Intelligence and the Modern Productivity Paradox: A Clash of Expectations and Statistics", NBER Working Paper no. 24001, October 2017 (revised December 2017), p. 10

⁴ Russell L. Ackoff, "From Data to Wisdom", Journal of Applied Systems Analysis 16 (1989): 3-9

⁵ Id.

Figure 1: Data-Wisdom



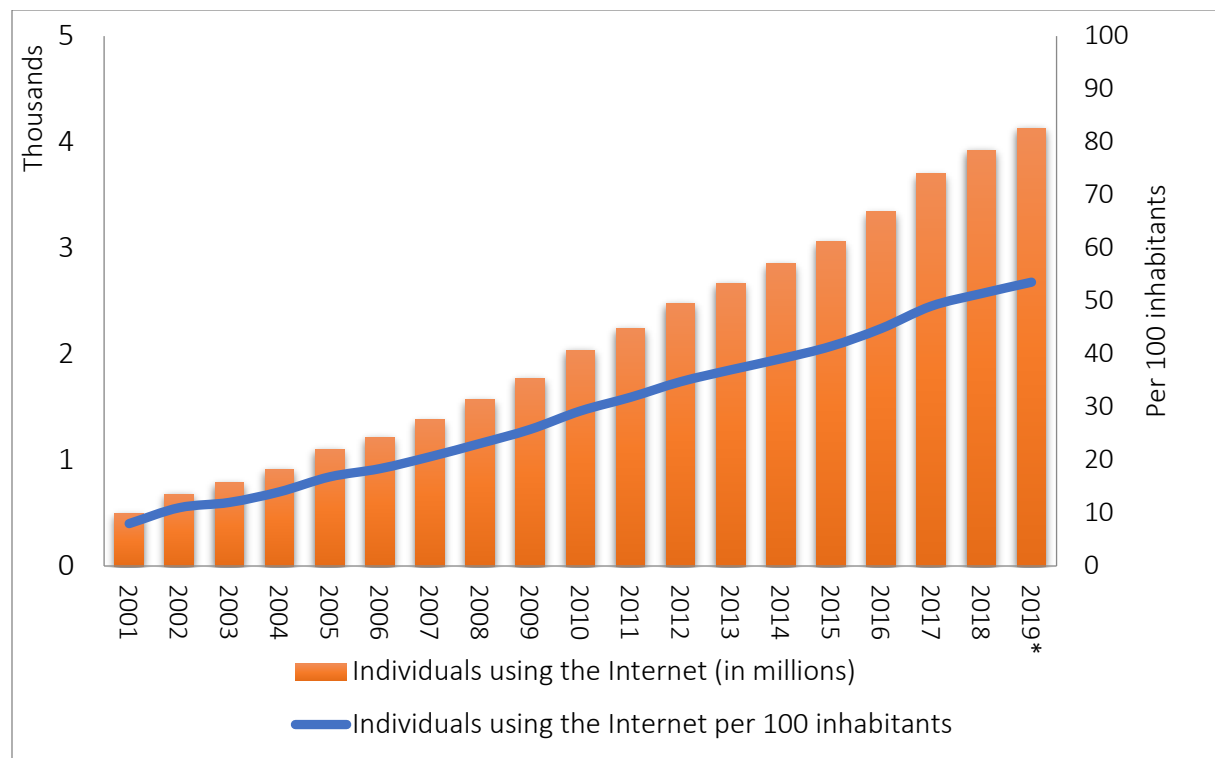
Data which is collected online is by itself, usually of limited value. In contrast, information and higher order levels of knowledge and wisdom gained by applying computing power to large data

The value of data as a source of insight arises from the enormous growth in data that is now being generated online. According to one estimate, in 2020 alone there will be forty times more bytes of data created than stars in the observable universe.⁶ This growth in data creation arises from the globalization of the internet and growth in the number of people and things that are online. As Figure 2 shows, over half of the world is online, and this is expected to grow to 5.6 billion people or two thirds of the world's population by 2023.⁷

⁶ Domo, Data Never Sleeps 7.0 <https://www.domo.com/learn/data-never-sleeps-7>

⁷ Cisco Annual Internet Report 2018-2023 White Paper

Figure 2: Approximately half the world's population is now online



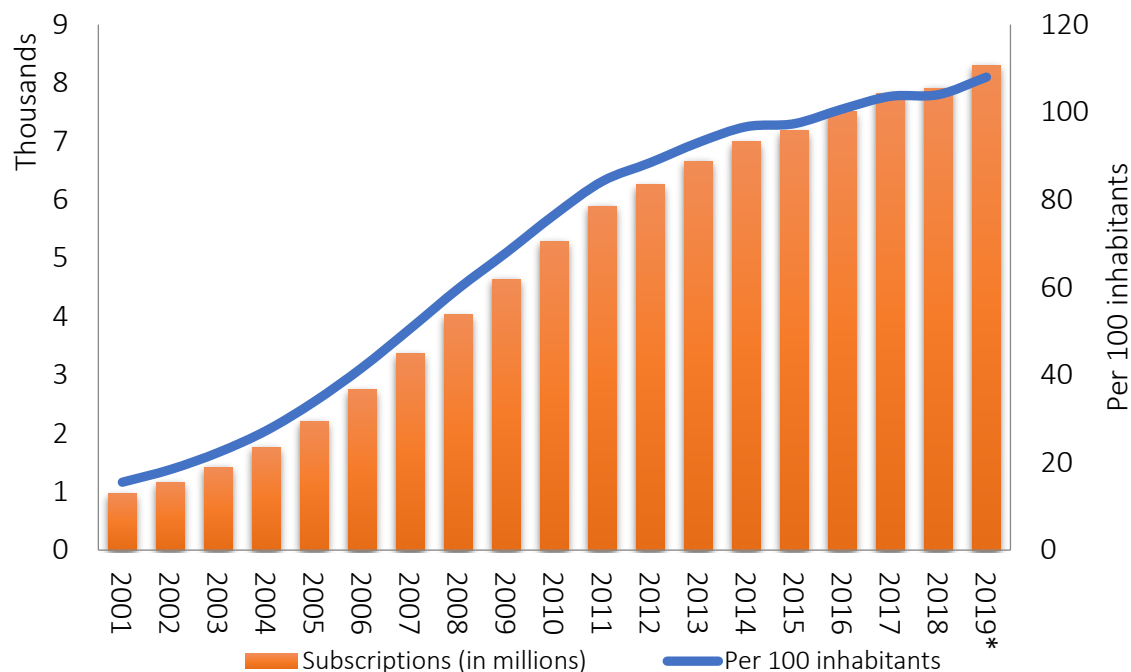
Source ITU World Telecommunications/ICT Indicators database

Figure 3 shows that internet access is also increasingly accessed using mobile devices including phones, tablets, laptops. This growth in mobile connectivity will grow further with 5G and the expansion of the internet-of-things (IoT). In fact, according to CISCO by 2023 the number of devices connected to the internet will be triple the global population.⁸ This will underpin 300% growth in mobile data traffic between 2017-2022, the largest growth being in mobile data, particularly in the Middle East, Africa and the Asia Pacific.⁹ This mobility and growing internet access creates a positive feedback loop that incentivizes industries to go digital to take advantage of the data being generated.

⁸ Cisco Annual Internet Report 2018-2023 White Paper

⁹ https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html#_Toc532256803

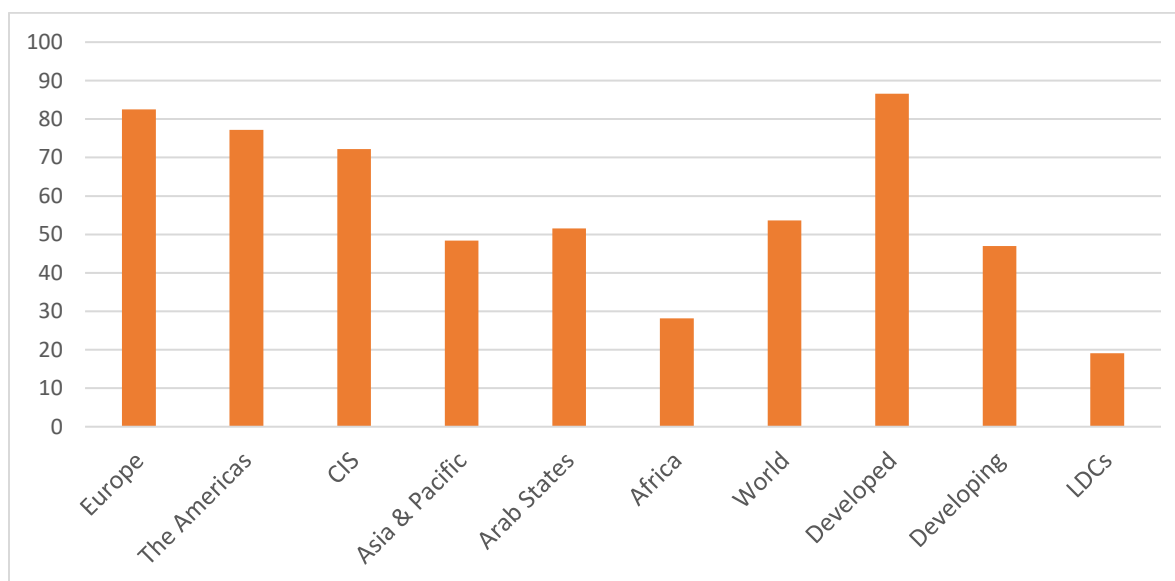
Figure 3: Global mobile-cellular subscriptions are growing



Source ITU World Telecommunications/ICT Indicators database

Despite the fact that the internet is global, figure 4 shows that internet use globally is uneven. In the developed world, over 85 percent of people use the internet while only 47 percent of people use the internet in the developing world and less than 20 percent in LDCs. In the Asia Pacific region, which covers a lot of APEC economies, less than 50 percent use the internet.

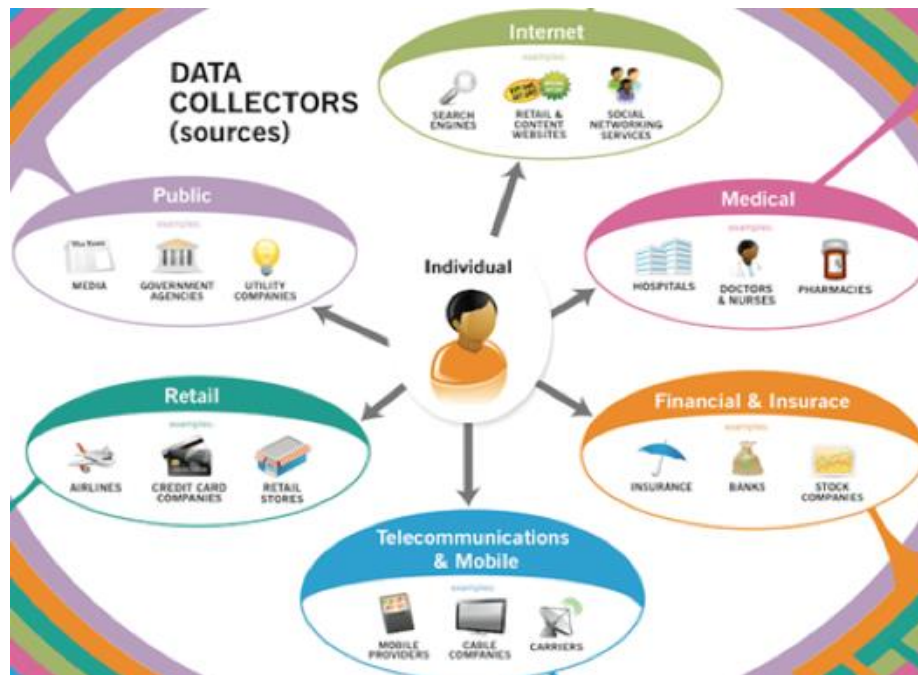
Figure 4: There are large differences in internet use amongst regions



Source: ITU Measuring Digital Development 2019

Figure 5 shows the various ways that data is continuously collected from people online. As can be seen, as economies go digital, data is being collected by various economic sectors and industries, including health care data, financial data, retail data and government data. To this we can add geo-location data derived from mobile devices, cars and IoT sensors. Video and picture are also increasingly important data source. It is estimated that 1.3 billion digital photos were taken in 2017, compared with 3.8 billion photos in all of human history until 2011.¹⁰ This data underpins AI applications from autonomous vehicles to facial recognition.

Figure 5: The multiple points for the collection of data



Personal data collected from peoples' interactions with the internet is not the only driver of data and data flows. Data is also generated and collected from devices as they move across borders, such as data collected by Rolls Royce as it continuously monitors jet engines. As will be discussed in Part 2, cross-border data flows are increasingly being used to deliver services across borders, whether it be professional, financial or IT, such as cloud computing. Finally, even when a digital interaction may seem purely domestic, such as an email sent within a country, a cross-border data flow may be involved as the internet routes data along available routes.

2. The impact of data on economic growth

¹⁰ <https://sloanreview.mit.edu/article/the-rise-of-visual-content-online/>

Data access and use is underpinning the digitization of economies and international trade. The economic importance of data is potentially significant.¹¹ For instance, McKinsey estimated that in 2014, global data flows contributed US\$2.8 trillion to the global economy,¹² a figure that could reach US\$11 trillion by 2025.¹³

Data is a key building block of technology development and innovation.¹⁴ Take artificial intelligence (AI)—a data-driven technology which could add trillions of dollars to global output over the next 10 years and accelerate the transition towards a services-driven global economy.¹⁵ Data is also a key enabler of digital technologies such as cloud computing, robotics, and the internet-of-things. The McKinsey Global Institute estimates that AI could add around 16 percent, or \$13 trillion, to global output by 2030.¹⁶ Cloud computing, another technology that relies on cross-border data flows, is vital to deliver computing services online.¹⁷

Calculating the size of the digital economy in individual countries remains a work in progress.¹⁸ A key challenge is that available statistics fail to identify which activities are digital.¹⁹ There is also no common definition of the digital economy. Narrow definitions focus on the ICT sector including telecommunications, internet, IT services, hardware and software. A broader definition such as the one used by the G20 includes data-based information and knowledge as the key factor of production, modern information networks and ICT.²⁰ For instance, in Australia,

¹¹ World Bank, 2016; “World Development Report 2016: Digital Dividends.” World Bank, Washington D.C.; supra note 3, 105-130.

¹² McKinsey & Company. 2016. *Digital globalization: The New Era of Global Flows*.

<http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows>.

McKinsey & Company. 2015. *By 2025, Internet of things applications could have US\$11 trillion impact*.

<http://www.mckinsey.com/mgi/overview/in-the-news/by-2025-internet-of-things-applications-could-have-11-trillion-impact>.

¹³ Id

¹⁴ OECD Digital Economy Outlook 2017

¹⁵ Jacques Bughin et al. “Notes from the AI Frontier, Modeling the Impact of AI on the World Economy,” *McKinsey Global Institute Discussion Paper*, September 2018. Paul Daugherty and Mark Purdy. “Why AI is the Future of Growth?” 2016. https://www.accenture.com/t20170524T055435_w/ca-en/acnmedia/PDF-52/Accenture-Why-AI-is-the-Future-of-Growth.pdf.

¹⁶ Jacques Bughin et al. “Notes from the AI Frontier, Modeling the Impact of AI on the World Economy.” *McKinsey Global Institute Discussion Paper*, September 2018.

¹⁷ Amazon Web Services 2019. “Data Residency”, November 2019

https://d1.awsstatic.com/whitepapers/compliance/Data_Residency_Whitepaper.pdf

¹⁸ Nadim Ahmad and Jennifer Ribarsky, “Towards a Framework for Measuring the Digital Economy”, OECD Working Paper prepared for the 16th Conference of the International Association of Official Statisticians (IAOS) OECD Headquarters, Paris, France, 19-21 September 2018

¹⁹ Nadim Ahmad and Jennifer Ribarsky, “Towards a Framework for Measuring the Digital Economy”, OECD Working Paper prepared for the 16th Conference of the International Association of Official Statisticians (IAOS) OECD Headquarters, Paris, France, 19-21 September 2018 ; see also OECD (2019), “A measurement roadmap for the future”, in *Measuring the Digital Transformation: A Roadmap for the Future*, OECD Publishing, Paris, www.oecd.org/going-digital/measurement-roadmap.pdf

²⁰ G20 Digital Economy Development and Cooperation Initiative 2016

digital economic activities have been identified across retail and wholesale trade, media, telecommunications, professional, technical and scientific services. The U.S. International Trade Commission (ITC) found that digitally intensive industries in the US include content industries; communications; finance and insurance; retail; health care, education and manufacturing.²¹

Despite these challenges, a number of APEC economies have estimated the size of their digital economies, though different definitions of the digital economy limit the ability to compare estimates. A study by the U.S. ITC found that in the US in 2014, digital trade (within the U.S. and globally) raised US GDP by 3.4 to 4.8 percent by increasing productivity and lowering the costs of trade; increased wages and likely contributed to as many as 2.4 million new jobs.²² A more recent 2018 study by the U.S. Bureau of Economic Analysis using a narrow definition of the digital economy concluded that from 2006-2016 the U.S. digital economy grew at an average annual rate of 5.6 percent, outpacing the average annual rate of growth for the overall U.S. economy of 1.5 percent, accounted for 6.5 percent of US output, 3.9 percent of employment and 6.7 percent of employee compensation.²³ A report by China's Academy for Information and Communications Technology (CAICT) used a broad definition of the digital economy to find that China's digital economy accounted for almost 40 percent of Chinese GDP. In Australia, a study by the Australian Bureau of Statistics defined the digital economy as digital infrastructure, digital media and e-commerce, found that the digital economy comprised 5.7 percent of production in 2016-17.²⁴

The impact of data on international trade

The economic opportunities of global data flows and digital technologies is also transforming international trade in the following ways.

International e-commerce opportunities

Already, around 12 percent of global goods trade is via international e-commerce.²⁵ Businesses can have their website or use digital platforms to become global. This is comprised of purchasing online and having the good delivered offline. According to a 2019 U.N. Conference on Trade and

²¹ USITC 2014, "Digital Trade in the U.S. and Global Economies, Part 2", Pub. No 4485, August 2014, p., 275.

²² United States International Trade Commission, Digital Trade in the U.S. and Global Economies, Part 2, Investigation 332-540, Pub. No.4485, August 2014; Castro, Daniel. 2013. "The False Promise of Data Nationalism." Information Technology & Innovation Foundation (ITIF). <http://www2.itif.org/2013-false-promise-data-nationalism.pdf>.

²³ Barefoot, K, et al (2018), Defining and Measuring the Digital Economy, Bureau of Economic Analysis Working Paper, 3/15/2018

²⁴ Australian Bureau of Statistics 2019, "Measuring Digital Activities in the Australian Economy", <https://www.abs.gov.au/websitedbs/D3310114.nsf/home/ABS+Chief+Economist+-+Full+Paper+of+Measuring+Digital+Activities+in+the+Australian+Economy>

²⁵ McKinsey & Company. *Digital globalization: The New Era of Global Flows*. 2016. <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows>.

Development (UNCTAD) report, e-commerce globally was worth \$29 trillion in 2017, with around 1.3 billion people shopping online—up 12 percent from the previous year.²⁶

E-commerce provides a potentially significant opportunity to increase small business participation in international trade.²⁷ For instance, having a website gives small businesses an instant international presence without having to establish a physical presence overseas. In addition, the internet provides access to advertising and communication services, as well as information on foreign markets—all of which help small businesses participate in international trade.²⁸ In Korea for instance, 100 percent of small businesses on eBay are exporters compared to 20 percent of offline peers.²⁹ Similar results play out across developed and developing countries. AI is also relevant here. For example, eBay's machine translation service has increased eBay-based exports to Spanish speaking Latin America by 17.5 percent.³⁰ To put this growth into context, a 10 percent reduction in distance between countries is correlated with increased trade revenue of 3.51 percent—so a 13.1 percent increase in revenue from eBay's machine translation is equivalent to reducing the distance between countries by over 35 percent.

Digital services trade

Internet access and cross-border data flows are going to be particularly significant for growth in services trade.³¹ Services can increasingly be purchased and consumed online. This is particularly true for information technology (IT), professional, financial, retail, and education services.³² New digital services such as cloud computing are becoming crucial business inputs.³³ The finance industry relies on the ability to transfer data across borders in order to complete electronic transactions and make money transfers.³⁴ AI requires access to large data sets as machine learning needs to be able to incorporate into future predictions as many past outcomes as possible.³⁵

²⁶ UNCTAD. "Global e-commerce sales surged to \$29 trillion." 2019.

<https://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=2034>.

²⁷ Meltzer, Joshua P. "Supporting the Internet as a Platform for International Trade: Opportunities for Small and Medium-Sized Enterprises and Developing Countries." *Brookings Working Paper*, 69, February 2014.

²⁸ OECD. "Top Barriers and Drivers to SME Internationalization." *Report by the OECD Working Party on SME and Entrepreneurship*. Paris: OECD Publishing, 2009.; Schoonjans, Bilitis, Van Cauwenberge, Philippe and Heidi Vander Bauwhede et al. Formal Business Networking and SME Growth. *Small Business Economics*. 41, 2013.

²⁹ Ebay 2016. "Small Online Business Growth Report", January 2016

³⁰ Brynjolfsson, E, X Hui and Meng Liu. "Does Machine Translation Affect International Trade? Evidence from a Large Digital Platform." 2018.

³¹ Aaditya Mattoo and Sacha Wunsch-Vincent, "Pre-empting Protectionism in Services: The GATS and Outsourcing", *Journal of International Economic Law* 7(4), 2004

³² United States International Trade Commission. *Digital Trade in the U.S. and Global Economies, Part 2*. Investigation 332-540, Pub. No.4485, August 2014, p. 42.

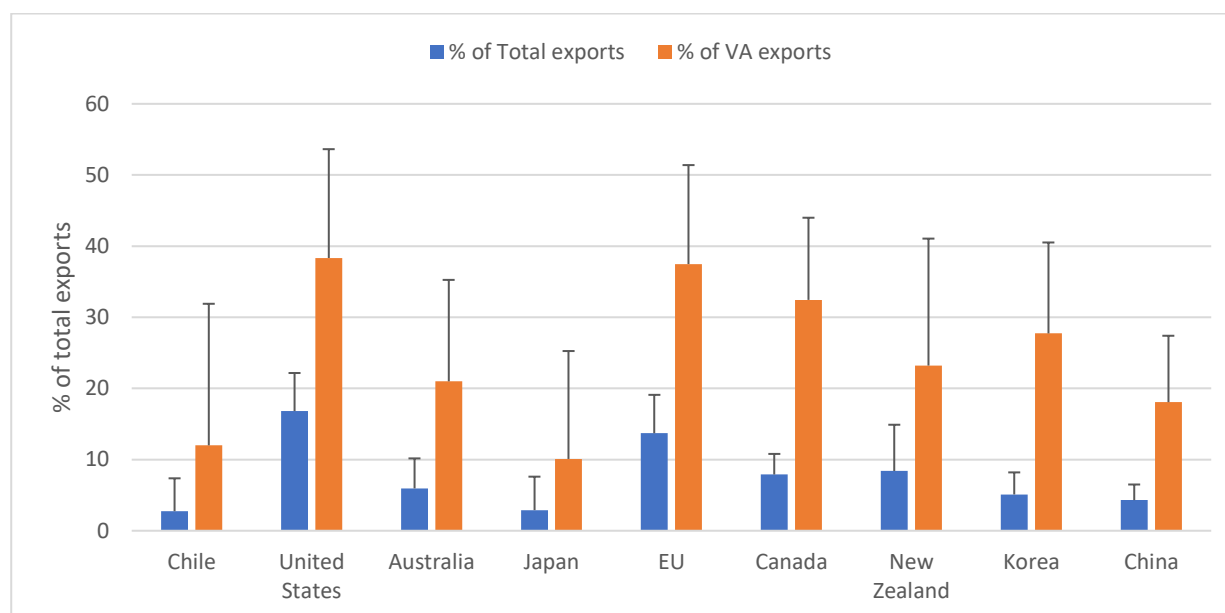
³³ United States International Trade Commission. *Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions*. Pub. No 4716, August 2017, pp.58-66.

³⁴ D. Gozman and J. Liebenau. "The Role of Big Data in Governance: A Regulatory and Legal Perspective of Analytics in Global Financial Services." *SWIFT Institute Working Paper*, No. 2014-009, 6. 2015.

³⁵ Generative adversarial networks or use of digital twins can minimize need for large data sets to train AI.

Figure 6 shows opportunities for exports of digital-deliverable services (DDS)—services that could be delivered online. In New Zealand for instance, DDS could be as high as 15 percent of total exports, and the value of DDS embodied in goods and services exports could account for over 40 percent of total exports.

Figure 6: Digitally deliverable services exports



Source: OECD TiVA, own calculations

Engaging in digital services trade is also a development opportunity for some countries. For instance, India's ICT enabled exports in 2016-2017 were \$103 billion or 63 percent of total services exports and 80 percent of these digital services were delivered via Mode 1—over the internet.³⁶ More specifically, the key role of services as inputs into production means that the opportunity for digital trade to liberalize services alongside effective regulation can contribute to broad-based improvements in efficiency and economic growth.³⁷ For example, according to the WTO, using digital technologies to reduce trade costs could increase world trade by up to 34 percent by 2030.³⁸ This includes using digital technologies to reduce transport by increasing the efficiency of logistics, using robots to optimize storage and inventory, and using blockchain to facilitate customs processing.

Digital services are also increasingly key inputs into manufacturing processes. This includes commercial services such as research and development (R&D), design, marketing, and sales. A 2016 PricewaterhouseCoopers survey of more than 2,000 companies identified data and data

³⁶ "India's Exports of ICT-enabled Services, An All-India Survey: 2016-2017." Indian Ministry of Commerce and Industry, June 2018, <http://dgciskol.gov.in/Writereaddata/Downloads/IctExportReport.pdf>.

³⁷ Aaditya Mattoo. "Developing Countries in the New Round of GATS Negotiations: Towards a Pro-Active Role", in *Legal Aspects in International Trade*, Proceeding of a World Bank Seminar 2001.

³⁸ WTO Trade Report 2018.

analytics as the key for successful transformation to smart manufacturing.³⁹ It reflects the importance of digital services in manufacturing for increasing productivity, which affects the capacity of firms to compete domestically and overseas.⁴⁰ The centrality of services in manufacturing is well understood.⁴¹ From a developing country perspective, it means that access to cutting edge services is a key part of any strategy to develop the manufacturing sector, and that in the digital age, access to best in class digital services must be part of this agenda.⁴²

The digitization of goods exports

Data collection and analysis are allowing new digital services to add value to goods exports. Data flows across borders enable digitization of the entire manufacturing enterprise, faster lifecycles, and collaborative and connected supply chains.⁴³ Business also rely on cross-border data flows in their operations. For example, as a Boeing plane flies across the Pacific, Boeing tracks its jet engine performance in real time from a data center in Washington state, USA. Vestas – the Danish wind-turbine manufacturer - relies on cross-border data flows to manage its global manufacturing network and uses sensors located in globally distributed wind turbines to increase their efficiency. Data collected from sensors attached to mining and farming equipment allows businesses to improve their operations and thereby the value from the use of such equipment. These are examples of which underscore a broader point – that business models rely on the ability to move data freely across borders.

Increased participation in global value chains

Global data flows underpin global value chains (GVCs), creating new opportunities for participation in international trade.⁴⁴ For many economies, such participation in GVCs is the

³⁹ PricewaterhouseCoopers 2016. Industry 4.0: Building the digital enterprise. 2016 Global Industry 4.0 Survey.

⁴⁰ Hoekman, B. and Aaditya Mattoo. "Services Trade and Growth." *Policy Research Working Paper* No. 4461, Washington DC: World Bank 2008.; Liu, Xuepeng, Aaditya Mattoo, Zhi Wang, and Shang-Jin Wei. 2017. "Services Development and Comparative Advantage in Manufacturing." Unpublished manuscript.

⁴¹ Claire H. Hollweg 2019., "Global value chains and employment in developing economies", in Global Value Chain Development Report 2019: Technological Innovation, Supply Chain Trade, And Workers in a Globalized World", WTO, IDE-JETRO, OECD, UIBE and World Bank Group Publication, 2019

⁴² Satoshi Inomata and Daria Taglioni 2019., "Technological progress, diffusion, and opportunities for developing countries: lessons from China", in Global Value Chain Development Report 2019: Technological Innovation, Supply Chain Trade, And Workers in a Globalized World", WTO, IDE-JETRO, OECD, UIBE and World Bank Group Publication, 2019

⁴³ L. Yu, et al. "Current Standards Landscape for Smart Manufacturing Systems." *NIST, NISTIR 8107*, February 2016.

⁴⁴ Baldwin, R. "The Great Convergence: Information Technology and the New Globalization." Boston: Harvard University Press. 2016.

deciding factor for trading internationally. More than 50 percent of trade in goods and over 70 percent of trade in services is in intermediate inputs.⁴⁵ Data and digital technologies are affecting GVC participation in several ways. The development of GVCs has been enabled by global connectivity and cross-border data flows that facilitate communications and can be used to coordinate logistics.⁴⁶ Global data flows are also enabling so-called supply chain 4.0—where information flows are integrated and omnidirectional instead of linear flows from supplier to producers to consumers and back.⁴⁷ Integrated information flows enabled by supply chain 4.0 are creating new opportunities to enhance productivity and expand employment opportunities. There is a trend towards increasing the use of imported services inputs in manufactured goods exports, suggesting that digital services are being traded within GVCs as well.⁴⁸ This includes allowing SMEs to plug into GVCs to offer their own specific service or to strengthen more traditional e-commerce offerings. Global data flows have also allowed digital platforms to source key digital services globally, creating entirely digital value chains. Take Gojek, an Indonesian ride sharing platform. Gojek’s digital supply chains includes a cloud-based company from Singapore, a payment service based in Singapore and New York and mapping service and software APIs from Silicon Valley.

3. Cross-border data flow restrictions in APEC

APEC restrictions on cross-border data flows continue to grow

As the opportunities presented by global data flows and digital technologies grow, governments are increasingly regulating in ways which restrict global data flows. This is a global phenomenon as well as occurring within APEC.⁴⁹ Figure 8 shows the cumulative growth in data flow restrictions in APEC. As can be seen, data flow restrictions have grown from one such regulation in 1988 to seventy-three in 2020. There was a particularly large increase in the number of regulations over 2013-2019, from twenty-three regulations restricting cross-border data flows in 2013 to seventy-one such regulations in 2019, an increase of over 300 percent.

These figures are also conservative. Not included is regulation aimed at taxing foreign e-commerce providers. For example, Indonesia requires foreign e-commerce businesses to have a permanent establishment in Indonesia in order to apply domestic taxes. This regulation is not included as its impact on cross-border data flows is more indirect and the question of taxation of digital companies is being addressed by the G20 and the OECD work on Base Erosion Profit

⁴⁵ OECD. “Mapping Global Value Chains”, TAD/TC/WP/RD(2012)9. 2012.

⁴⁶ Helpman E. “Understanding Global Trade.” Cambridge, Mass: Harvard University Press. 2011.

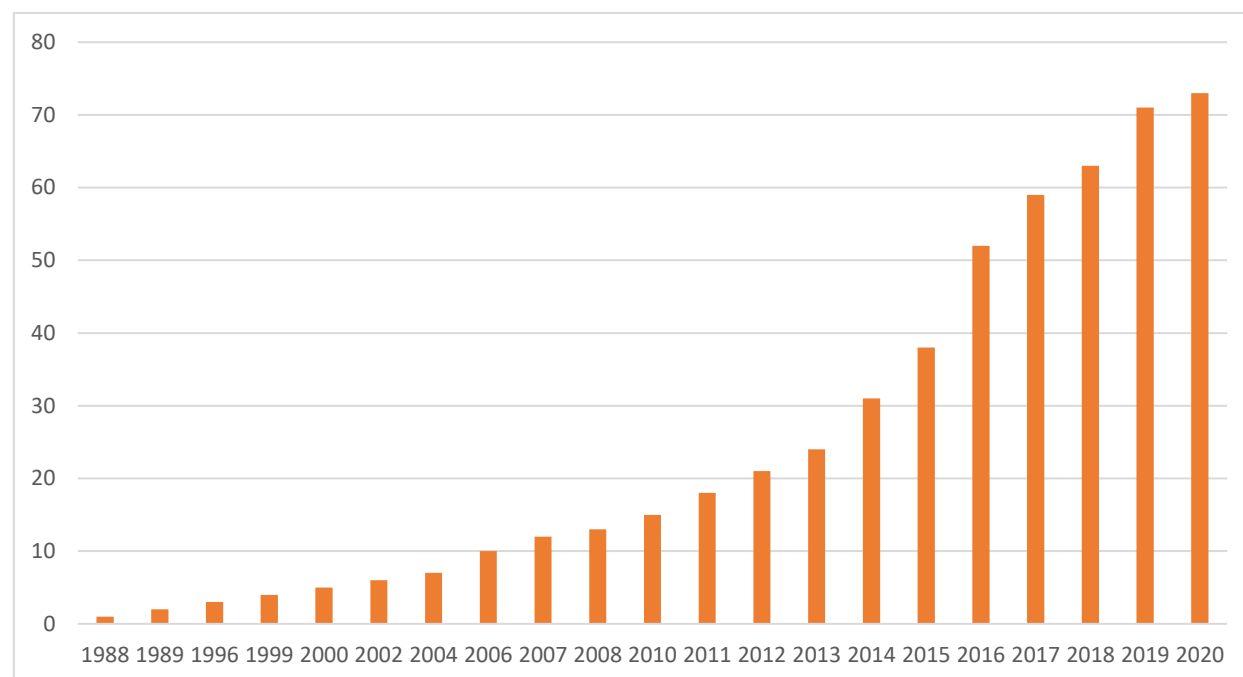
⁴⁷ Michael Ferentina and Emine Elcin Koten 2019, “Understanding supply chain 4.0 and its potential impact on global value chains”, in Global Value Chain Development Report 2019 (WTO, IDE-JETRO, OECD, UIBE, World Bank)

⁴⁸ Miroudot S., Charles Cadestin. Services in Global Value Chains: From Inputs to Value-Creating Activities.” *OECD Trade Policy Paper* 197, p. 16. 2017.

⁴⁹ OECD. “Trade and cross-border data flows.” TAD/TC/WP(2018)19/FI. 2018. Martina Ferracane, “Cross-border Data Flows: A Taxonomy”, ECIPE Working Paper No. 1/2017

Shifting.⁵⁰ There are also various draft and recent laws and regulations whose impact on cross-border data flows is potentially significant, but whose impacts are not known at this stage, and are therefore not included. This includes Russia's 2019 Sovereign Internet Bill which seeks to create an independent internet within Russia and Indonesia's 2017 E-commerce Roadmap that will affect a range of internet and e-commerce services but whose impact remains unclear until further regulations are developed. These examples underscore that the trend in APEC continues to be toward increasing restrictions on cross-border data flows.

Figure 7: Cumulative growth in cross-border data flow restrictions in APEC



Source: USTR 2020, ECIPE, authors own research *Data flow restrictions are in pursuit of various goals*

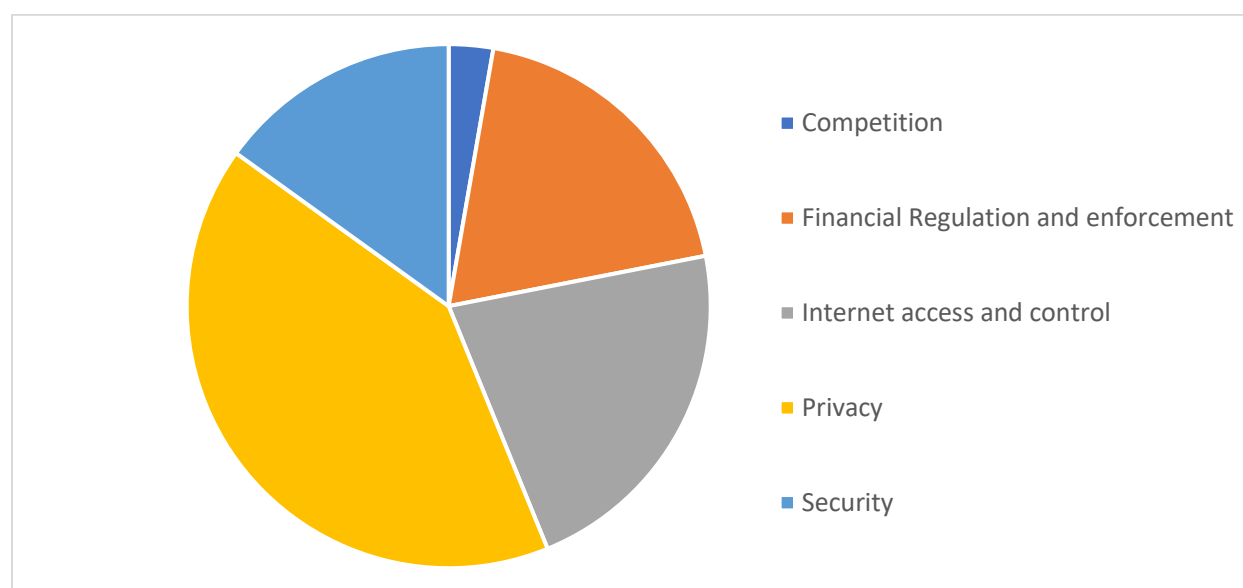
In APEC, the restrictions on cross-border data flows are in pursuit of a range of regulatory goals. As can be seen in in figure 9, the key regulatory goals are privacy, security, competition (which covers restrictions aimed at helping a domestic industry), internet access and control and financial regulation and law enforcement. Privacy is by far the main reason for data flow restrictions in APEC, counting for over 40 percent of regulation. Internet access and control is the second most salient reason for restricting data flows, accounting for 22 percent, followed closely by financial regulation at 20 percent, then security at 11 percent and competition at 2 percent.

The regulatory goals are reflected in a variety of regulation targeting different sectors. For instance, while many APEC economies have privacy laws, privacy of personal data is also being

⁵⁰ <http://www.oecd.org/tax/beps/>

pursued in other types of regulation, such as Australia’s limits on transfers of health data and China’s requirement that public health data is stored within China and not transferred overseas. Privacy goals are also reflected in some of the data flow restrictions on the financial sector, such as Korea’s substantial consent requirements before a financial institution in Korea can transfer personal data to affiliates outside of Korea, or China’s requirement that personal information collected by financial institutions are stored within China. The regulatory goal of internet access and control is also reflected in a range of regulation, though most such regulation is focused on the telecommunications and ISPs as key points of control over data flows. These include China’s prohibition on telecoms companies offering VPNs to reach overseas data centers, Indonesia OTT regulation that requires data localization, Russia’s requirement that telecom providers and ISP store data locally and Vietnam’s local server requirements for online social networks, general information websites, mobile telecoms network-based content services and online games services.

Figure 8: The regulatory objectives of cross-border data flows restrictions



Source: ECIPE, USTR, ABLI Privacy Law Compendium, authors own research

Identifying the regulatory goals is a first step towards designing a response that can address the need for restriction on cross-border data flows. However, identifying regulatory goals is not straightforward. Often regulation will not state a goal or there may be more than one goal. In addition, regulation that restricts cross-border data flows, such as domestic privacy requirements, will also often have a negative impact on trade by harming competition from overseas services providers who rely on data flows.⁵¹ Determining whether a regulation is about achieving a legitimate objective or is a disguised restriction on trade is an issue and

⁵¹ Mattoo, Aaditya and Joshua P. Meltzer. “Data Flows and Privacy: the conflict and its resolution.” *Journal of International Economic Law*, Vol 21, Issue 4.

challenge for trade policy broadly. In this paper, the assumption is that regulation is not about restricting competition unless it is clearly the predominant driver. As a result, there are only a few regulations classified as being about restricting competition, but this should not be taken to mean that data flow restrictions for other goals do not also impact competitive opportunities and international trade.

There are three key drivers of data flow restrictions

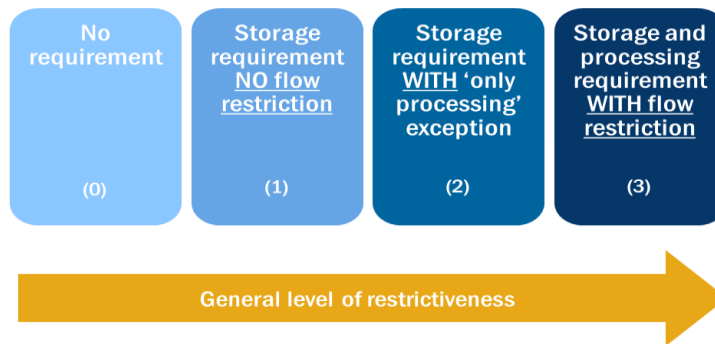
The need to restrict data flows to achieve a range of regulatory goals has three underlying drivers. One is the regulatory concern that allowing data to be transferred to a third country will undermine domestic regulatory standards. This is a key rationale for privacy law restrictions on transfers of personal data and is at play for various security focused regulations. For example, Russia's restrictions on transfers of personal data to another jurisdiction unless there is an adequate level of privacy protection seeks to ensure that domestic privacy standards are not undermined by cross-border transfers of personal data to a jurisdiction with a lower level of privacy protection. A second driver is regulatory concern that allowing data to reside in a third country will negatively affect the ability of regulators to do their job. This leads to many of the regulations requiring the financial sector to localize data. For example, China requires that insurers localize data in order for the insurance regulator to perform its responsibilities. A third driver is the impact of access to information on political and social stability. This is at play for those restrictions aimed at internet access and control, and partly for those addressing security concerns. For example, Vietnam's 2018 Cybersecurity Law requires local retention of a range of personal and other data of Vietnamese users, in part so the state can regulate online content, which could include information opposing or offending the Socialist Republic of Vietnam or to block "defamatory propaganda," such as any critical or dissenting statements made against the government.⁵²

Data flow restrictions are increasingly restrictive

This range of regulation restricting cross-border data flows are also of varying levels of restrictiveness. They include measures that disallow the transfer of data outside national borders; measures that allow cross-border transfers but require a copy to be maintained domestically; and requirements of various types of consent before data can be transferred overseas. There are also data localization restrictions that often also include restrictions on data flows. Figure 10 provides a taxonomy of local storage requirements and their impacts on cross-border flows.

Figure 9: Taxonomy of data localization requirements

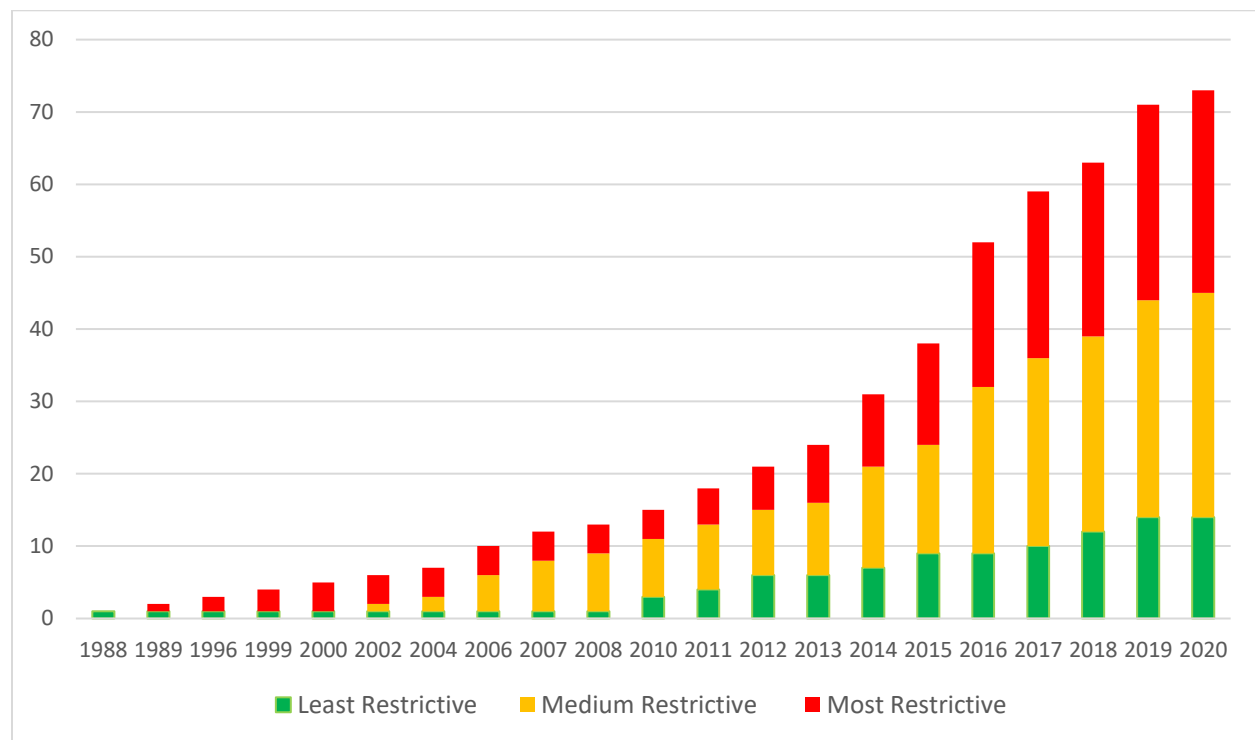
⁵² Vietnam Decree No. 72 /2018/NC-CP amending and supplementing Decree No. 72/2013/ND-CP on Internet Services and Online Information; over-the-top refers to services that bypass traditional telecom and media distribution channels—e.g., Skype or Netflix.



Source: OECD

The following figure 11 shows cumulative growth in data flows restrictions in APEC in terms of the levels of restrictiveness. As can be seen, the growth in restrictions on data flows in APEC has occurred across all levels of restrictiveness but has been most pronounced in measures that are medium and most restrictive. Looking at the last 20 years, least restrictive data flow regulations – almost all of them privacy laws – has increased from 1 in 2000 to 14 in 2020. In contrast, over this period, regulations with medium levels of data flow restrictiveness have gone from zero in 2000 to thirty-one in 2020, and the most restrictive cross-border data flow regulations have increased from four in 2000 to twenty-eight in 2020. To put it another way, in 2020, 20 percent of data flow restrictions were least restrictive, forty-two percent were of medium restrictiveness and thirty-eight percent were most restrictive.

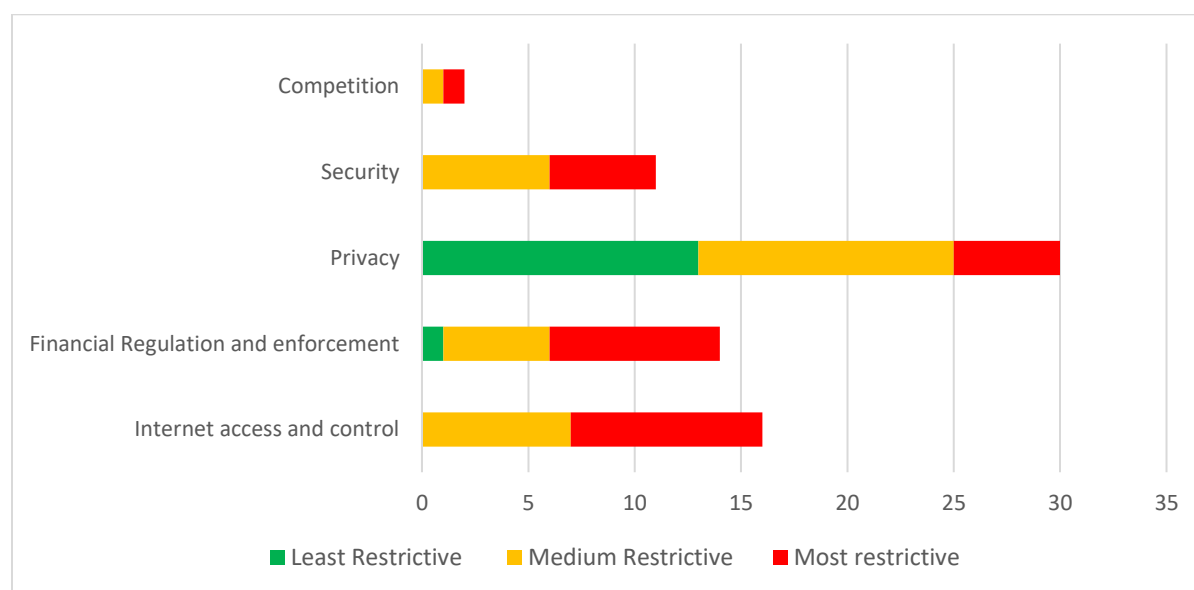
Figure 10: breaks down the data flows restrictions in APEC by levels of restrictiveness.



Source: ECIPE, USTR, ABLI Privacy Law Compendium, authors own research

Figure 12 disaggregates the different regulatory goals by level of restrictiveness. Many of the least restrictive data flow restrictions concern privacy protection and are requirements of consent for data to flow. For example, a number of APEC economies including Mexico, New Zealand and Chinese Taipei require consent to transfer personal data to third countries. Other countries such as Canada and Australia do not require prior consent but require that the entity transferring the personal data to take reasonable steps to ensure that the data is processed consistent with domestic privacy standards.

Figure 11: Regulations affect cross-border data flows differently



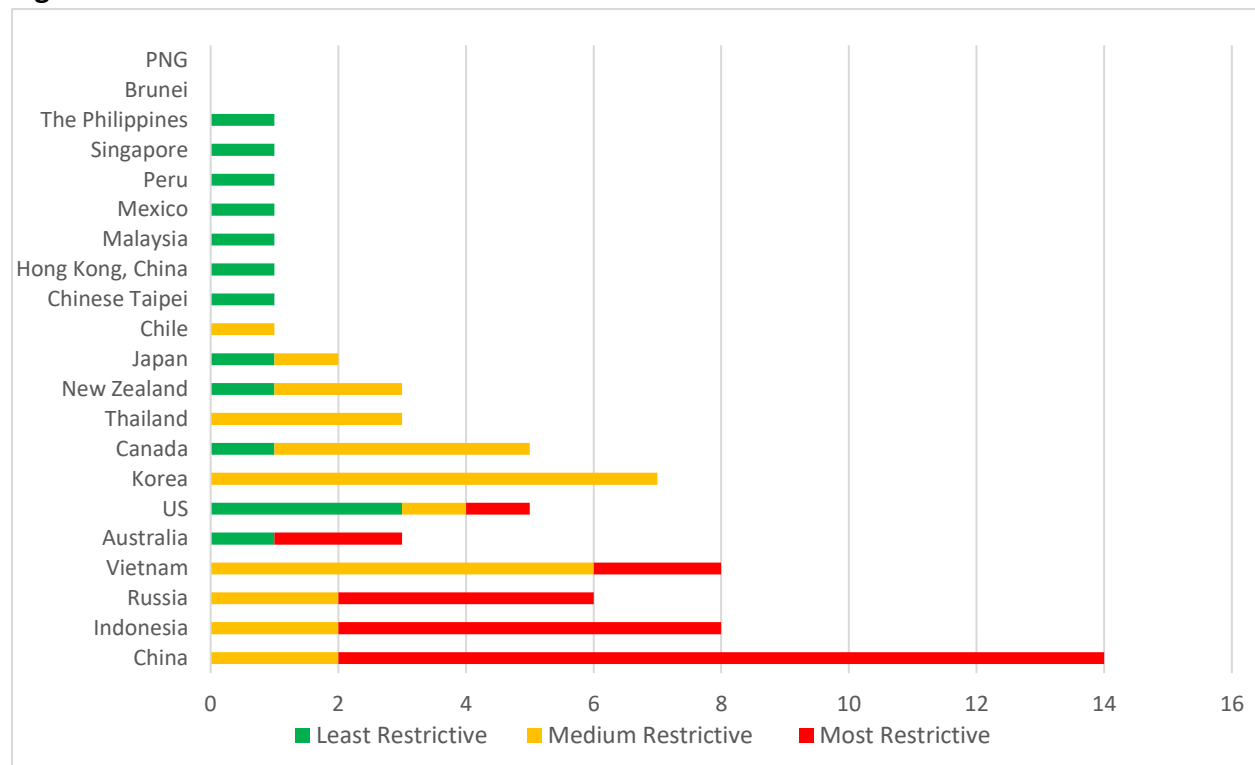
Source: ECIPE, USTR, ABLI Privacy Law Compendium, authors own research

A range of cross-border data flow restrictions are of medium restrictiveness. These include privacy regulation such as Canada's provincial level privacy regulation that have increasingly stringent limits on the ability to transfer personal data outside of Canada. Russia's privacy regulation which has a GDPR-like 'adequacy' condition for transfers of personal data outside of Russia, falls into this category. There are also a range of financial regulations that are of medium restrictiveness. This includes Korea's prohibition on electronic commerce firms selling goods in Korean Won, storing customers' credit card numbers in company information systems, and Vietnams requirement that all domestic retail credit and debit transactions be processed though the National Payments Corporation of Vietnam.

The most restrictive cross-border data flow regulations are found across all regulations and are most prevalent when it comes to security, internet access and control and financial regulation and enforcement. In the financial sector, China and Indonesia require banks and insurers to localize data. Restrictive regulation addressing internet access and control include Vietnam's local server requirements, Russia's requirement that ISPs localize data for at least 6 months, and China's requirement that all data collected in China be stored within China. There are also a range of most severe data flow restrictions for security purposes. This includes Vietnam's data localization requirement for ISPs and China's data localization requirements under its cybersecurity law. Some privacy laws are also the most restrictive, such as Indonesia's requirement for consent in writing before personal data can be transferred across borders and Vietnam requiring localization of personal data. And some of the most restrictive data flow regulation appear also to be for competitive reasons, such as China requiring localization of data collected by online taxi operators.

As seen in figure 13, the growth in regulation that is most restrictive on cross-border data flows has been concentrated in four APEC economies: China, Indonesia, Russia and Vietnam. These include China's guidelines for Personal Information Protection and Cybersecurity Law, Indonesia's various financial data regulations, Russia's national security and counterterrorism laws and Vietnam's various Decrees affecting flows of financial information. Korea also has a high number of regulations that are medium in their cross-border data flow restrictiveness. The United States has a relatively large number of regulations affecting data flows, many of which stem from the growth in state-based privacy laws.

Figure 12: Growth in data flow restrictions are concentrated in four APEC economies



Source: ECIPE, USTR, ABLI Privacy Law Compendium, authors own research

Many of the regulatory goals driving data flow restrictions, such as protection of privacy and law enforcement, are themselves legitimate goals. Yet, whether data restrictions are optimal way of achieving these goals is less clear.⁵³ For instance, APEC economies privacy laws impact on cross-border data flows range from least to most restrictive, pointing to a range of ways to achieve privacy protection and impact on data flows. In other cases, such as cybersecurity, requiring data to be localized may be counterproductive where local data centers are less

⁵³ Joshua P Meltzer and Peter Lovelock, "Regulating for a Digital Economy: Understanding the Importance of Cross-Border Data Flows in Asia, Brookings Working Paper 113, March 2018

secure and by missing the opportunity for stronger cybersecurity protection provided by disaggregating data across global data centers.⁵⁴

4. Supporting Cross-Border Data Flows in APEC

The following looks at what APEC might do to facilitate cross-border data flows. As discussed, there are three key drivers of restrictions on cross-border data flows. Two of these drivers – concern about data flows undermining domestic standards and the need to access data to perform regulatory functions - are amenable to being addressed by APEC through international cooperation, improved information flows and regulatory understanding of the links between cross-border data flows, trade and economic growth. The third driver of data flow restrictions revolves around governments’ desire to control access to information, whether for political, religious or social reasons. In these cases, there may be only so much trade policy can do here. When it comes to restrictions on data flows to support domestic industry, this is a trade barrier that could violate existing WTO commitments and be inconsistent with commitments to the free flow of data and to data localization prohibitions in FTAs such as the Comprehensive and Progress Agreement for Trans-Pacific Partnership (CPTPP).⁵⁵ In this respect, commitments to the free flow of data and to data localization prohibitions in FTAs are important in getting for competitiveness as a driver of data flow restrictions.

The following focuses on a role for APEC in addressing these drivers of data flow restrictions. As a starting point, it would be helpful for APEC to ground its approach by updating the Bogor goals of free and open trade and investment to include the free flow of data. Such a goal would send a strong signal of APEC’s support for data flows as a driver of trade and growth. To advance this goal in a way that produces meaningful outcomes in terms of reducing the trend towards greater data flow restrictions and improving opportunities for cross-border data flows, will require a work program with the following elements:

1. Domestic implementation of regulation the builds trust in cross-border data flows and reduces unnecessary restrictions.
2. Cooperation amongst APEC regulators to building interoperability mechanisms that enable cross-border data flows.

⁵⁴ Amazon Web Services 2019. “Data Residency”, November 2019
https://d1.awsstatic.com/whitepapers/compliance/Data_Residency_Whitepaper.pdf

⁵⁵ M. Burri (2017), ‘The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation’, U.C.Davis Law Review, 51: 65–133; A. D. Mitchell and N. Mishra (2018), ‘Data at the Docks: Modernising International Trade Law for the Digital Economy’, JETLaw, 20: 1073, 1095; M. Wu (2017), ‘Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System’, RTA Exchange, Geneva: ICTSD and IDB, November 2017

Committing to the free flow of data with appropriate exceptions

A number of APEC economies have already undertaken commitments in various FTAs to the free flow of information and to prohibitions on data localization. For example, the CPTPP, the United States-Mexico-Canada agreement (USMCA), the US-Japan digital trade agreement and Singapore-Chile-NZ Digital Economy Partnership Agreement (DEPA) include commitments to not restrict cross-border transfers of information, including personal information, by electronic means. These data flow commitments are subject to an exception provision modelled on GATT Article XX/GATS Article XIV exceptions provision, whereby the parties can restrict data flows to achieve a legitimate public policy objective, provided the measure restricting the cross-border flow of information is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination, or a disguised restriction on trade, and/or does not impose a restriction on transfers of information greater than are necessary to achieve the objective. These FTAs also include a commitment to not require the domestic location of computing facilities as a condition for doing business. This commitment is also subject to similar exception provisions.⁵⁶

Table 1 provides an overview of key FTAs where APEC economies have committed to the free flow of data and to avoiding data localization requirements. As can be seen, these various FTA commitments provide a strong basis for an APEC-wide commitment to data flows and prohibitions on data localization. In addition, the Regional Comprehensive Economic Partnership (RCEP) agreement which is slated to finalize in 2020, might also include commitments to data flows, which would add China, the Philippines and Thailand as APEC economies with such commitments.⁵⁷ This would leave only Russia, PNG and Taiwan without any trade commitment to cross-border data flows and to no data localization.

Table 1: Most APEC economies have trade commitments to the free flow of data

APEC Economies	Cross-border data flow	No data localization	Trade agreement
Australia	Yes	Yes	CPTPP, Sing-Aust FTA, Indo-Aust CEPA
Brunei Darussalam	Yes	Yes	CPTPP
Canada	Yes	Yes	CPTPP, USMCA
Chile	Yes	Yes	CPTPP
PRC	No	No	
Hong Kong, China	No	No	
Indonesia	Yes	Yes	Indo-Aust CEPA
Japan	Yes	Yes	CPTPP, US-Japan Digital Trade Agreement
Malaysia	Yes	Yes	CPTPP
Mexico	Yes	Yes	CPTPP, USMCA

⁵⁶ CPTPP art. 14.13.3, USMCA, art. 32.1.2.

⁵⁷ JOINT LEADERS' STATEMENT ON THE REGIONAL COMPREHENSIVE ECONOMIC PARTNERSHIP (RCEP) 4 November 2019, Bangkok, Thailand

New Zealand	Yes	Yes	CPTPP, DEPA
PNG	No	No	
Peru	Yes	Yes	CPTPP
Philippines	No	No	
Russia	No	No	
Singapore	Yes	Yes	CPTPP, Sing-Aust FTA
South Korea	Best endeavors	No	Korea-US FTA
Chinese Taipei	No	No	
Thailand	No	No	
United States	Yes	Yes	USMCA, US-Japan Trade Agreement
Vietnam	Yes	Yes	CPTPP

Signed and Ratified

Signed but not yet ratified

The free flow of financial information

In FTAs with commitments to the free flow of data, financial services have experienced a slightly different treatment. The exclusion of data held by financial institutions was a product of the regulatory driver that information needed to be stored locally in order for regulators to have the access needed to perform their regulatory duties. In CPTPP, for instance, financial institutions and cross-border financial services suppliers are carved out from the e-commerce chapter that includes data flows and data localization commitments. The CPTPP financial services chapter does contain a rule that parties must allow information transfers in electronic or any other form for business purposes, but does not include a prohibition on forced data localization.⁵⁸

This regulatory driver was addressed in the USMCA financial services chapter which includes a commitment to the free flow of information as well as a prohibition on data localisation requirements, subject to appropriate exceptions.⁵⁹ The prohibition against data localisation is subject to the party's financial regulatory authorities, for regulatory and supervisory purposes, having immediate, direct, complete and ongoing access to relevant information used by a covered person outside its territory. Before imposing data localisation, the parties also commit to providing a reasonable opportunity to covered entities to remediate any lack of information access. The US-Japan Digital Trade Agreement combines the USMCA digital trade chapter commitments and those found in the financial services chapter into a single commitment on data flows to all sectors (including financial services) and replicates the USMCA prohibition on data localization found in the digital trade chapter and the analogous provision in the financial services chapter, ensuring that every sector is covered by these important provisions.⁶⁰

⁵⁸ Comprehensive and Progressive Agreement for Trans-Pacific Partnership, Dec. 30, 2018, <https://www.iilj.org/wp-content/uploads/2018/03/CPTPP-consolidated.pdf> [hereinafter CPTPP].

⁵⁹ USMCA, art. 17.17.

⁶⁰ US-Japan Digital Trade Agreement Articles 11–13

Progress, but more is needed

The digital trade commitments in these FTAs are significant and will help support cross-border data flows in APEC. However, more is needed to address the growth in data flow restrictions. As outlined, one reason regulators are restricting data flows is to avoid data flows undermining domestic standards.⁶¹ Another reason for restricting data flows is due to regulatory concerns that this will limit or delay access to data needed to perform regulatory and law enforcement duties. Without getting at these regulatory drivers of data flow restrictions, commitments to cross-border data flows and to avoiding data localization will likely be accompanied by significant carve outs – as happened with respect to Vietnam’s data flows commitments under CPTPP. Alternatively, governments with such data flow commitments are likely to rely on the exception provisions to continue to justify data flows restrictions, risking the exception becoming the rule. For example, the EU proposal in the WTO E-commerce negotiations of a broad self-judging exception to data flows commitment with respect to the protection of personal data and privacy, shows how this reliance on exceptions to justify ongoing data flow restrictions could develop.⁶² Governments seeking to rely on such exceptions provisions must show that the regulation is ‘necessary’ – that no alternatives exist that are less restrictive and achieve the WTO Members’ legitimate regulatory objective.⁶³ In order for the exception provision to provide a meaningful discipline requires developing less trade-restrictive options that support domestic regulatory goals while minimizing the impact on cross-border data flows.

Building Trust Amongst Regulators

Building trust can reduce the regulatory concern that allowing data to flow to another country will undermine domestic regulatory goals. In order to build trust in cross-border data flows, this APEC agenda should have the following elements: the development and implementation of domestic regulation in areas such as privacy, consumer protection and cybersecurity that builds trust in cross-border data flows, and minimizing the regulatory impact on data flows.

Some progress on this agenda has been made in FTAs, and these commitments can underpin and guide APEC work. For example, in CPTPP and USMCA the parties have agreed to implement privacy laws as well as to protect consumers engaged in digital trade or e-commerce.⁶⁴ The CPTPP is the first trade agreement to recognize the importance of building

⁶¹ Mattoo, Aaditya and Joshua P. Meltzer. “Data Flows and Privacy: the conflict and its resolution.” *Journal of International Economic Law*, Vol 21, Issue 4. at 18.

⁶² EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce, Communication from the European Union, INF/ECOM/22 (Apr. 26, 2019).

⁶³ Appellate Body Report, *Brazil — Measures Affecting Imports of Retreaded Tyres*, WTO Doc.WT/DS33/AB/R (adopted Dec. 17, 2007) [hereinafter *Brazil-Retreated Tyres*]; Appellate Body Report, *US — Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WTO Doc. WT/DS285/AB/R (adopted Apr. 20, 2005) [hereinafter *US-Gambling*].

⁶⁴ CPTPP art. 14.7,14.8; USMCA art. 19.7, 19.8

cooperation on cybersecurity.⁶⁵ The USMCA builds on this and includes a hortatory commitment to developing risk-based approaches to cybersecurity threats that rely on consensus-based standards and risk management best practices.⁶⁶

Domestic regulation based on international standards

As discussed in more detail below, APEC also needs to develop interoperability mechanisms that enable cross-border flow of data. Existing interoperability mechanisms for transferring personal data such as CBPR rely on some convergence of domestic privacy laws. This highlights how domestic regulation that builds trust also supports international regulatory cooperation. To put it another way, the greater convergence there is amongst the regulation needed to build trust in cross-border flows, the greater will be the opportunity to develop ambitious interoperability mechanisms.

Reducing unnecessary regulatory diversity has been the work of trade policy already. Trade agreements already include commitments to use and develop international standards as a basis for domestic regulation. For example, the WTO Technical Barriers to Trade (TBT) Agreement deals with technical regulations applicable to trade in goods and includes a commitment by WTO members to use international standards, where they exist, as a basis for their domestic technical regulations.⁶⁷ Where this happens, such technical regulations are presumed to not be an unnecessary barrier to trade.⁶⁸ These WTO TBT commitments are often replicated in FTAs.

For a standard to qualify as an international standard for the purposes of the WTO TBT Agreement, the standard must be mandatory, non-discriminatory and approved by a recognized body for establishing such standards, and that is open to participation by all WTO members.⁶⁹ This would include standards produced by bodies such as the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC), which also produce international services standards.

APEC economies have already identified the need to develop international standards for the digital economy that enhance certainty for firms operating across borders.⁷⁰ International standards that become the basis for regulation in APEC economies can minimize regulatory diversity, thereby addressing concerns that allowing cross-border data flows will undermine domestic standards.

⁶⁵ CPTPP art. 14.16

⁶⁶ USMCA, art. 19.15.

⁶⁷ WTO TBT Agreement art. 2.4

⁶⁸ WTO TBT Agreement art. 2.5

⁶⁹ See TBT Committee Decision of 2000, which agreed six principles that should be observed by international standards setting bodies: transparency; openness, impartiality and consensus; effectiveness and relevance; and addressing the concerns of the developing world. FTAs such as CPTPP and USMCA references this TBT Decisions as laying out the process for establishing standards.

⁷⁰ APEC 2019, APEC Economic Policy Report 2019: structural reform and the digital economy, p. 84

Developing APEC Specific Standards

APEC could develop a more systematic and comprehensive approach to standards for data flows. This will require extending beyond APEC's traditional focus on goods, as cross-border data flows implicate trade in goods and services. For example, the cross-border provision of cloud computing, apps and forms of e-commerce are trade in services. The development and expansion of IoT, as 5G is rolled out across APEC, will further expand opportunities to gather and use data, with implications for trade in goods and services – the physical thing and the software that enables the good to be networked. Moreover, IoT will likely heighten cybersecurity, privacy and consumer protection concerns, potentially leading to further restrictions on data flows.

APEC has demonstrated some capacity for developing APEC specific standards, such as the Privacy Framework - a set of principles to guide APEC economies on the development of their privacy laws - and progress could be made elsewhere on principles and standards relevant for data flows. For instance, APEC could seek to develop cybersecurity principles, building on the work program on cybersecurity in the APEC Telecommunications and Information Working Group that included information sharing on cybersecurity threats and sharing best practices.⁷¹ An APEC standard by dint of its limited membership is not an international standard under the TBT Agreement, yet APEC standards have found their way into FTAs, such as in USMCA which specifically refers to CBPR as an interoperability mechanism.

Box 1: APEC Cross-Border Privacy Rules

The APEC Cross-Border Privacy Rules (CBPRs), endorsed by APEC in 2014 is a voluntary mechanism to facilitate the transfer of personal information amongst APEC members. Under CBPR, participating businesses develop privacy policies based on the APEC Privacy Framework and which meet the CBPR program requirements. APEC Accountability Agent assess consistency of businesses privacy policy and practice with the APEC CBPR requirements. Businesses privacy policies that meet CBPR requirements and are subject to the laws of an APEC CBPR participating economy, can then be certified as compliant. There are eight APEC economies participating in the CBPR system in 2020: Australia; Canada; Japan; Korea; Mexico, Singapore; Chinese Taipei; and the United States. APEC Accountability Agents and Privacy Enforcement Authorities are responsible for enforcing compliance by business with APEC CBPR requirements.⁷² The APEC Cross-Border Privacy Enforcement Arrangement facilitates enforcement by enabling sharing of information and assistance for cross-border data privacy enforcement.

Incorporating international standards across APEC

APEC also could focus on supporting APEC economies use of international standards. Already, there are international standards, and more are being developed that could affect cross-border

⁷¹ APEC Telecommunications and Information Working Group Strategic Action Plan 2016-2020

⁷² See APEC Cross-Border Privacy Rules System, Policies, Rules and Guidelines, 10.

data flows. This includes the ISO/IEC 27000 cyber and information security standards. APEC can seek to build understanding and agreement on what further standards are needed and how alignment of domestic and international standards can help governments reduce the need for data flow restrictions. Where standards are being developed in international bodies, APEC could coordinate and support such work.

Under the APEC Sub-Committee on Standards and Conformance (SCSC), APEC currently does important work on aligning domestic standards with international standards, based on standards identified in the Voluntary Action Plan (VAP). To date, the VAP has focused on alignment with international goods standards. This work should be expanded to include standards that can support data flows. Consideration could also be given to domestic frameworks that use international standards, such as the US NIST Cyber Framework.⁷³

Limits to international standards in addressing restrictions on cross-border data flows

There are limits to the extent that APEC economies' domestic regulations will align with international standards. The reality is that domestic implementation of international standards often diverge as regulation adapts to local conditions. For instance, while the US and EU have privacy regimes based on the OECD Privacy Principles, each have privacy regimes that nevertheless diverge significantly. Divergent privacy laws also exist amongst APEC economies participating in CBPR, notwithstanding that their privacy laws are based on the APEC Privacy Framework. These divergences are manageable within the CBPR system, as long as they do not lead to such different privacy standards as to call into question whether transfers under CBPR undermine core domestic privacy standards. Yet, in the case of Japan at least, this has already happened as a result of Japan reforming its privacy standards to align with GDPR. The result being that at least for personal data received from the EU, CBPR is no longer available for Japanese businesses for onward transfers of EU personal data.

Despite these limits, the development of a common baseline on privacy principles has been useful. While not leading to common approaches in practice, OECD and APEC privacy principles have minimized regulatory heterogeneity, making the process of developing interoperability mechanisms that can bridge differences between domestic privacy regimes less challenging than it would otherwise be. In fact, Privacy Shield (and Safe Harbor before that) was facilitated by much of what is common (and OECD consistent) between the U.S. and EU on privacy. And as noted, the APEC CBPR relies on the common baseline of the APEC Privacy Framework.

Good Regulatory Practice Within APEC

APEC can also seek to minimize the impact of regulation on cross-border data flows by expanding its work on good regulatory practice (GRP) to include data flows. For instance, APEC can help regulators better understand how regulation is affecting data flows, trade and

⁷³ NIST 2020, Security and Privacy Controls for Information Systems and Organization, Draft NIST Special Publication 800-53, Revision 5

business opportunities, what other countries are doing in terms of best practice, and whether there are alternative ways to achieve the desired goal with less impact on data flows. These are all generic elements of GRP in that they are not specific to data flows and digital trade but can improve regulatory making broadly.⁷⁴

APEC has a well-developed work program supporting GRP. In 2005, the APEC-OECD Integrated Checklist on Regulatory Reform laid out a voluntary GRP framework for self-assessment on regulatory quality, competition policy, and market openness. In 2011 APEC developed the “Good Regulatory Practices in APEC Member Economies – Baselines Study”, which reviewed the application of GRP across APEC members. A 2016 APEC report assessed progress of APEC members applying GRP.⁷⁵

The 2016 review assessed progress coordinating rule making and managing regulatory reform, including: coordination with trade and competition officials, the capacity to use regulatory impact assessment to assess the impact of regulation, including its impact on trade, and the extent that APEC economies are using public consultation mechanisms when it comes to the design of regulation. These elements can also guide assessment of the impact of regulation on cross-border data flows. Currently, however, there does not appear to be any explicit consideration of how GRP can be expanded to include data flows. The following outlines ways that the existing GRP work within APEC could be adapted to be digitally relevant, with a specific focus on managing the interface between regulation and cross-border data flows.

Ex-ante assessment of the impact of regulation on cross-border data flows

What constitutes GRP should be expanded to include the impact of regulation on data flows as well as access to data. This can be done by requiring regulators to conduct a regulatory impact assessment that includes the impact on cross-border data flows. Having regulators consider the impact on data flows when developing regulation can also help identify less trade restrictive options.

Strengthen transparency, consultation and reason-giving by regulators

Another area of GRP already identified by APEC is the need for transparency, consultation, and reason-giving in the development of regulation.⁷⁶ Ex ante consultations with stakeholders can expand the information regulators have access to, which can help improve the regulatory outcome. Consultations can also strengthen the legitimacy of regulation, particularly when consultation is accompanied by reason-giving and explanation for why a particular regulatory approach was taken over other possible approaches. These reasons for consultation are true for regulation generally and are particularly important for the digital economy as the

⁷⁴ Basedow, Robert and Celine Kauffmann 2016. ‘International Trade and Good Regulatory Practices: Assessing The Trade Impacts of Regulation.’ *OECD Regulatory Policy Working Papers* No 4.

⁷⁵ APEC 2016, Final Report on Good Regulatory Practices in APEC Economies

⁷⁶ APEC 2019, APEC Economic Policy Report 2019: structural reform and the digital economy, p. 57

importance of data for economic growth means there is often limited appreciation within agencies of the impacts of regulation on data flows.

Seek to identify alternatives that are less restrictive on cross-border data flows

GRP also includes being least trade restrictive and not creating unnecessary barriers to trade. As commitments to data flows are included in FTAs across APEC, these agreements can drive GRP as they feed back into the domestic regulation making process. As outlined above, these commitments to cross-border data flows and to data localization prohibitions are subject to exceptions modeled on GATS Article XIV. These exceptions give regulatory space to restrict data flows in order to achieve legitimate goals. Mapping this legal commitment onto the regulation making process, GRP should require that regulators assess the impact of data flows, and where data flows are being restricted to achieve a legitimate goal, consideration of whether there are alternatives that can achieve the legitimate goal in ways that are less restrictive on data flows. Establishing interoperability models (see below) could also allow APEC economies to experiment with less data flow restrictive alternatives.

Improve cross-government coordination of regulation for the digital economy

Another relevant element of GRP is responding to how the increasing economy-wide use of data challenges current division of regulatory responsibility across agencies.⁷⁷ For example, use of telecommunications networks to provide video raise questions whether regulation of such providers is a responsibility of telecommunications agencies or cultural/content focuses. As platforms compete across transport, accommodation and retail for example, vertical regulatory silos seem increasingly poorly adapted. The need for cross-government regulatory coordination is not specific to the digital economy, but its need is made even more acute and challenging given the economy wide impacts of data combined with fast changing disruptive technologies.⁷⁸ Existing progress in APEC on developing coordination mechanisms should remain an area of focus while adding a lens which accounts for the importance of this agenda for regulating the digital economy.

Expanding regulatory cooperation within APEC

The second APEC agenda item should be on international regulatory cooperation that builds interoperability mechanisms which enable cross-border data flows given regulatory diversity. The importance of developing interoperability mechanisms was recognized in the 2019 Osaka Leader's Statement. The APEC Internet and Digital Economy Roadmap also identifies interoperability as a core area of focus.⁷⁹ Some recent FTAs have taken initial steps to develop interoperability mechanisms that build bridges between different domestic regulatory regimes.

⁷⁷ APEC 2019, APEC Economic Policy Report 2019: structural reform and the digital economy, p. 83; OECD 2019, "Vectors of Digital Transformation". OECD Digital Economy Papers No, 273., January 2019, p. 14

⁷⁸ APEC 2019, APEC Economic Policy Report 2019: structural reform and the digital economy, p. 83

⁷⁹ APEC Internet and Digital Economy Roadmap, 2017/CSOM/006

For instance, USMCA encourages the parties to develop “mechanisms to promote compatibility between these different [privacy] regimes”, and in this respect identified the APEC Cross-Border Privacy Rules system as one such mechanism “to facilitate cross-border information transfer while protecting personal information.”⁸⁰ The USMCA also includes a commitment by the parties to cooperation on the development of the APEC CBPR to “further the interoperability of privacy regimes”.⁸¹

As outlined, there are not insignificant challenges developing international standards and there are limits on the extent standards can overcome the regulatory diversity that leads to restrictions on data flows. This underscores that in addition to developing standards and aligning domestic regulation, there is a need for international regulatory cooperation that can bridge the differences in domestic regulation which leads to data flow restrictions.

Building bridges between countries with different regulatory systems to minimize trade costs is not new. The OECD has identified 11 forms of international regulatory cooperation. The following looks at how MRAs and recognition of equivalency can be developed in APEC to support cross-border data flows.

Mutual Recognition Agreements that enable data flows

There are various forms that an MRA can take. MRAs can be built on countries harmonizing underlying regulations and recognizing the conformity assessment done in the exporting country of compliance with the regulation. Agreeing on international standards can provide a pathway to this outcome but as noted, even common international standards do not necessarily produce harmonized domestic regulation. As a result, such comprehensive MRAs are relatively rare, having been realized in the EU internal market and under the Trans-Tasman Mutual Recognition Agreement (TTMRA). Less ambitious MRAs do not result in any changes in the underlying domestic regulation and instead recognize conformity assessment of compliance by the exporting country with the importing country’s regulation.⁸² Recognition of conformity assessment can be government-to-government or can involve arrangements between private conformity assessment bodies from different countries. MRAs can also be legally binding – such as the TTMRA, or voluntary, such as the APEC TEL MRA.⁸³

An MRA for data flows would require the data destination country to apply the data source regulations to data imports. To work effectively, this requires application by the data destination country of the data source standards, as well as the data source country recognizing the capacity of the regulator in the data destination country to assess conformity.

⁸⁰ USCMA Article 19.8.6

⁸¹ USMCA Article 19.14

⁸² J. Pelkmans et al., *The Contribution of Mutual Recognition to International Regulatory Cooperation*, OECD REGULATORY POL’Y PAPERS, WORKING PAPER NO. 2, (2016) [hereinafter Pelkmans et al.].

⁸³ APEC, *Mutual Recognition Arrangement for Conformity Assessment of Telecommunications Equipment*, WORKING PAPER NO. 1 APEC#202-TC-01.1, (1998), <http://publications.apec.org/Publications/1998/05/Mutual-Recognition-Arrangementfor-Conformity-Assessment-of-Telecommunications-Equipment>.

The U.S.-EU Privacy Shield arrangement is one example of what is in effect such an MRA.⁸⁴ Under Privacy Shield, participating U.S. businesses comply with standards equivalent to the GDPR and the EU recognizes enforcement/oversight by the US Department of Commerce and Federal Trade Commission.⁸⁵ The APEC CBPR is another type of MRA. APEC CBPR relies on the APEC Privacy Framework, and CBPR puts in place mechanisms aimed at ensuring compliance by businesses participating in CBPR with domestic privacy regulation.

Box 2: The US-EU Privacy Shield

Under the Privacy Shield, U.S. companies through an industry body or individually self-certify to the U.S. Department of Commerce that they will protect personal data consistent with the Privacy Framework, which includes the Privacy Shield Principles (Privacy Shield Framework 2018). These seven Principles (and supplemental principles) largely reflect the key elements of the EU GDPR. U.S. businesses are required to publish their privacy policies, and the Privacy Shield gives the U.S. Federal Trade Commission jurisdiction over such businesses should they breach their own policy. In addition, the United States provides various means of redress for people, whose personal data has been compromised, including a direct complaint to the business or a complaint to the Department of Commerce. Also, under the Privacy Shield, the United States has agreed to establish an ombudsperson to address complaints about government agencies' access to personal information from the EU on national security grounds.

Equivalence

Another approach is where a data source country recognizes that a data destination country's regulation is equivalent to its own. Equivalency can be granted unilaterally or by agreement. Equivalency is in effect what happens under GDPR when the European Commission issues a finding of adequacy with respect to another country's privacy protection regime.

The Interaction of Interoperability Mechanisms - APEC CBPR and GDPR

Given the outsized role of privacy laws and regulations in restricting cross-border data flows in APEC, the following looks more closely at CBPR and its limits, particularly with regard to GDPR – the EU approach to privacy that is in effect competing with CBPR as an alternative interoperability mechanism for moving personal data across borders.

CBPR is an important interoperability mechanism that facilitates cross-border data flows and privacy protection. There are growing numbers of APEC economies participating in CBPR, but the

⁸⁴ Mattoo, Aaditya and Joshua P. Meltzer 2018, "Data Flows and Privacy: the conflict and its resolution", J. Int'l Econ. L. Vol. 21, Issue 4, 18

⁸⁵ U.S. Department of Commerce. 2016. E.U.-U.S. Privacy Shield Framework Principles, Issued by the U.S. Department of Commerce. <https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg>

CBPR mechanism remain underutilized. Reforms are needed to CBPR to expand participating economies and its utility for business.

CBPR is also challenged by the expansion of GDPR adequacy findings to APEC economies. The key tension arises over the different CBPR and GDPR privacy standards. An assessment of the compatibility of Binding Corporate Rules (BCRs) – the GDPR mechanism that allows transfer of personal data within a global conglomerate – and CBPR made clear that GDPR and CBPR are not compatible.⁸⁶ Comparing GDPR with CBPR is beyond the scope of this paper. Analysis by others have identified a range of differences between the APEC Privacy Framework and GDPR, including the GDPR processing principles of ‘accuracy’, and the GDPR requirement that data is not kept longer than necessary (storage limitation).⁸⁷ The different privacy standards in GDPR and the APEC Privacy Framework mean that APEC economies with adequacy findings cannot use CBPR for onward transfers of EU personal data. This was one outcome of US-Privacy Shield where onward transfers from the US of EU personal data, are restricted.⁸⁸ More recently, Japan illustrates this CBPR/GDPR tension when it reformed its privacy laws as part of the process of obtaining an adequacy finding under GDPR.⁸⁹

Japan: GDPR/CBPR Tensions

In 2019, following reforms to Japan’s privacy laws, the EU granted Japan an equivalency decision under GDPR for private sector entities, and Japan simultaneously granted the EU White List status under its privacy laws. Prior to the reforms, Japan had allowed for cross-border transfers of personal data under the following conditions:⁹⁰

- Consent
- Where the data is sent to a third country which has been recognized by the Japanese Personal Information Protection Commission (PIPC) as providing an equivalent level of protection to the one guaranteed in Japan; or
- Where a person in a third country receives the personal data recognized as an international framework concerning the handling of personal data. This last mechanism for transfers of personal data would cover data transfers under APEC CBPR.

In the process of obtaining an adequacy finding, Japan introduced stricter regulation in the form of Supplementary Rules governing personal data received from the EU. Under these Rules,

⁸⁶ Article 29 Working Party, Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross-Border Privacy Rules submitted to APEC CBPR Accountability Agents, 6 March 2014 and Enforcement Rules for the Act on the Protection of Personal Information (Rules of the Personal Information Protection Commission No. 3, 2016).

⁸⁷ Maria Vasquez Callo-Muller, “GDPR and CBPR: Reconciling Personal Data Protection and Trade”, APEC Policy Support Unit Policy Brief No. 23, October 2018

⁸⁸ https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG, Annex 1 letter from ITA to EU Commissioner Jourova

⁸⁹ European Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, L 76/1

⁹⁰ Japan Act on the Protection of Personal Information (Act No. 57, 2003), Article 24

Japan agreed to tighten and limit transfers of EU personal data received from the EU under the adequacy decision to the following:

- A stricter form of consent that requires in addition to consent to the transfer, that the person is given information on the circumstances surrounding the transfer necessary to make a decision on his/her consent
- Retained the ability to transfer data to third parties located in a country with equivalent personal information protection equivalent to Japan's; or
- Where the third party who receives the data implements measures providing an equivalent level of protection (based on the Act and the Supplementary Rules) by means of a contract, other forms of binding agreements or binding arrangements within a corporate group.⁹¹

According to the EU, the effect of these Supplementary Rules is that Japan cannot rely on APEC CBPR to transfer to entities in third countries, EU personal data received under the EU adequacy finding.⁹² The EU provides two reasons here. One is that CBPR fails to bind the exporter and importer. The second is that the APEC privacy framework on which the CBPR system is based provides for a lower level of privacy protection than Japan guarantees under its domestic privacy rules. As a result, onward transfers would not accord EU personal data an adequate level of protection. This restriction is framed in terms of equivalent protection under Japan's revised laws, not the EU. Yet, in effect this is about ensuring that GDPR standards follow EU personal data, wherever it is sent.

Japan could limit the impact of this restriction on onward transfers by applying the Supplementary Rules to only those businesses receiving personal data from the EU, which business could comply by segregating EU personal data. For business, the question will be whether the benefits of CBPR are outweighed by the costs of segregating personal data received from the EU. As more countries in APEC receive adequacy findings, the costs of segmenting data will apply to a smaller number of APEC economies, tilting towards using GDPR across the business. The net result will be to further reduce the utility to business of using CBPR for transferring personal data within APEC.

Building confidence in access to data for regulatory needs

As outlined, another driver of data localization is regulatory concern that there will be delay or challenges in getting timely and complete access to data needed to perform regulatory duties and for law enforcement. Indeed, US Treasury and US Federal Reserve Bank concerns about getting access to data for regulatory purposes drove the decision to exclude the financial sector from the CPTPPs commitments to cross-border data flows and to no data localization.⁹³ The resolution of this matter in the context of the USMCA provides some guidance on a way forward. First, USMCA reaffirms the concerns financial regulatory have with allowing financial

⁹¹ ; https://ec.europa.eu/info/sites/info/files/draft_adequacy_decision.pdf, para 78

⁹² European Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, L 76/1

⁹³ CPTPP Article 14.1

data to reside overseas as follows: “The Parties recognize that immediate, direct, complete, and ongoing access by a Party’s financial regulatory authorities to information of covered persons, including information underlying the transactions and operations of such persons, is critical to financial regulation and supervision, and recognize the need to eliminate any potential limitations on that access”.⁹⁴ To address this concern, the no data localization commitment is subject to the party’s financial regulatory authorities having immediate, direct, complete and ongoing access to relevant information”.⁹⁵ A similar approach was taken in the US-Japan Digital Trade Agreement.⁹⁶

These commitments in USMCA and US-Japan Trade Agreement are underpinned by trust that the financial information will be made available on these terms. Yet, much of the financial data that regulators need access to, is stored by private companies – banks, insurance companies and other financial institutions who are not themselves subject to these commitments. Should compliance not be forthcoming by these private actors, enforcement will turn on the willingness and ability of governments to force their domestic financial actors to provide the information to the requesting government. Yet, in this event it would seem that the information requested by the regulatory authorities is not being provided in the immediate and director manner contemplated by these trade agreements.

What is needed is trust that such trade commitments will be complied with. APEC could consider developing an APEC wide mechanism aimed at strengthening trust amongst regulatory authorities that they will have access to the information needed to perform their regulatory functions. Success here would lay the groundwork for further commitments in FTAs addressing restrictions on cross-border flows where access to data is a regulatory concern. Initially, APEC could aim to develop principles that address regulatory concerns and needs with respect to data access and data localization requirements. More ambitious outcomes could include MOUs between financial regulators and the financial institutions that possess the data. Developing practice around data access for regulators should over time give regulators confidence that data localization requirements are not needed to address their legitimate regulatory needs.

5. Conclusion

Access to and use of data is already underpinning new and innovative business models throughout APEC. Data flows are also transforming international trade, providing opportunities for small business to go global, access world class cloud computing services and to participate in

⁹⁴ USMCA Article 17.18.1

⁹⁵ USMCA Article 17.18.2

⁹⁶ US-Japan Digital Trade Agreement, Article 13

global supply chains. Despite these opportunities, governments in APEC have introduced regulations restricting cross-border data flows.

Part of the challenge when regulating for the digital economy is the newness of the challenges. The emergence of data access and use as a key input into how businesses innovate, add value and compete, means that going digital is no longer an IT issue, but an opportunity for all economic sectors, including manufacturing, agriculture, services and government. This horizontal extension of data use across the economy also means that vertical regulatory arrangements in areas as diverse as transportation, consumer protection, health, education and food safety, can affect how data is accessed and used, including cross-border data flows.

The developments in the digital economy and the implications for how governments regulate underscores first and foremost the need for regulatory learning. In this respect, APEC as a non-binding forum for developing economic cooperation is well-placed to play a key role in strengthening understanding across APEC of the opportunities from data, best practices for regulating data flows while also achieving legitimate domestic regulatory goals such as privacy and security. As outlined, this needs to include developing domestic regulation that can build trust in cross-border data flows, minimizing regulatory divergence by aligning domestic regulation with international standards, and by applying principles of good regulatory practice.

APEC is also well placed to build on its experience with regulatory cooperation within APEC to develop interoperability mechanisms like CBPR. As discussed, APEC CBPR is an interoperability mechanism that builds trust in the privacy standards of participating APEC economies – thereby giving regulators confidence that allowing personal data to flow will not undermine domestic privacy standards. Interoperability mechanisms such as this are needed to expand trust that cross-border data flows will not undermine other domestic regulatory goals, such as consumer protection and cybersecurity.

Finally, APECs work on the digital economy and trade should be grounded by an overarching goal amongst APEC economies to the free flow of data. This is a natural extension and updating of the Bogor free trade goals. It would send the necessary signal that APEC recognizes and supports the opportunities of data and data flows for building economies and international trading links for this century.