Asia-Pacific
Economic Cooperation

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

Fostering an Enabling Policy and Regulatory Environment in APEC for Data-Utilizing Businesses

APEC Policy Support Unit

July 2019

Prepared by:

Vishal Beri and Dr Peter Hendy
Aegis Consulting Group

Nigel Cory
Information Technology and Innovation Foundation

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

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

APEC#219-SE-01.6

CONTENTS

EXECUTIVE SUMMARY

Data and growth

- Advancements in information and communication technologies (ICT) including broadband, cloud computing and the Internet of Things (IoT) have lowered the cost of adopting data analytics on a large scale and along with it, the benefits and possibilities brought about by the adoption.

- The importance of data in business will only accelerate as more and more people and devices are connected to the internet. Indeed, increasing number of literature are indicating the importance and contribution of data to economic growth as well as employment although it should be recognized that limitations means such statistics are often incomplete and may only provide rough estimates.

- APEC recognizes the importance of digital economy including e-commerce in linking their member economies. Recent initiatives include the APEC Framework on Cross-border E-commerce Facilitation, the APEC Internet and Digital Economy Roadmap (AIDER), and the establishment of the Digital Economy Steering Group (DESG).

- This study aims to better understand the role of data in the business models of various firms and the challenges they face pertaining to data utilization through case study approach. 39 firms from 12 economies have participated in this project. They come from a diverse group of industries, including aviation, logistics, shipping, payment services, encryption services, and manufacturing.

- Data plays an important role to firms in both the traditional as well as new industries. Firms across different sectors collect and/or use significant volumes of data for a wide range of purposes. In the transport and logistics sector, for example, these include tailoring attractive loyalty schemes for their customers as well as monitoring and assessing the safety, capacity and efficiency of asset deployment. In the manufacturing sector, data are used across the various stages of the value chain from pre-production to post-production (including post-sales). For example, firms use data analytics to reduce machine downtime, track inventories and process reordering when levels fall below certain threshold among others.

- For payment services providers, data is integral in every step involved in processing a transaction, but such data is only one component of the whole spectrum of data collected and used. In fact, firms carry out data analytics to glean valuable information coming from various and diverse sources. Specifically on electronic invoicing, data captured in electronic invoices can facilitate transparency and hence authorities' expanded use of tax, accounting as well as various data sources to ensure compliance. Other uses of data analytics include detecting anomaly, combating fraud and providing enterprise solutions.

- Firms generally recognize the important role of data in ensuring the viability of their businesses and to this end, have undertaken various activities to ensure the privacy and security of data collected and managed by them. These include ensuring that their policies, procedures and practices are consistent with international quality assurance instruments governing data security and privacy; undertaking regular and systematic review of various laws and regulations on data privacy and security to ensure compliance; and applying sophisticated and comprehensive in-house data governance framework covering areas such as hardware, cyber protection teams and encryption.

Challenges across economies

- The importance of data as a new asset has brought to the fore concerns on how firms use and protect the data that they have. These fears in a data age are not unfounded. News articles abound with hacking incidents and data leaks. Furthermore, the practices of some well-known firms have left more to be desired.

- In support of public policy objectives such as ensuring better data protection and security, rapid access to data and benefitting more from the digital economy, governments across the world have put in place or are in the midst of enacting various regulations aimed at data such as those regulating data collection, storage, processing and transfer; and those requiring disclosure of intellectual property (incl. source code), building back-doors to applications and use of mandatory encryption standards.

- While these regulations have been enacted for legitimate public policy objectives, some of them may not be the best way forward. For example, as security is a function of several elements including technical, financial and personnel, the association between data localization and data security may not be a given. Furthermore, some data-related regulations including localization may have the unintentional effect of increasing the cost of doing business. Literature has also shown the limited impact of some data-related regulations on employment and investment creation as well as in enhancing innovation and productivity. Moreover, some data-related regulations may be a second-best option of addressing domestic security/concerns.

- Alternative, middle-ground approaches to data-related issues (i.e. with relatively minimal impact on firms' access and use of data and at the same time, supportive of legitimate public policy objectives) are available. These approaches include recognizing voluntary standards, reviewing potential and existing domestic regulations against privacy guidelines/framework, complementing lighter touch regulations with effective enforcement, and enhancing cross-border data flows through various mechanisms such as adequacy status, mutual recognition system and free trade agreements among others. Specifically on enhancing domestic security, alternative mechanisms can include reforming mutual legal assistance treaties (MLAT), signing Memorandums of Understanding (MoU) on bilateral and multilateral data sharing, and unilateral approaches which focus on mandating access to specific types of data.

Challenges across organizations

- Data-related issues, in particular data sharing are not confined only to between economies, but also between organizations. Despite being an important factor for unlocking innovation and realizing the potentials of digital economy, the practice of data sharing is not widespread for various factors including data privacy regulations, anticompetitive behavior and lack of interoperability of data formats and standards.

- Facilitating data sharing between organizations could be enhanced through approaches such as introducing open data policies, promoting data commons, developing data sharing standards as well as guidelines.

Way forward

- APEC can build on the insights from the study and contribute to the endeavor of improving data-related regulations among its members by:

    - Facilitating information and experience sharing/exchange on these middle-ground approaches. These can include how to operationalize these approaches, how to monitor and evaluate their impacts as well as how they can be further improved in terms of implementation and awareness among others.

    - Organizing dialogue sessions to identify ideas and ways to overcome bottlenecks that have led to standstill or little progress in some middle-ground approaches such as those pertaining to regulatory alignment, multilateral rules on data flow facilitation and MLAT reform.

    - Developing capacity-building activities to assist member economies in enhancing and improving on their existing data-related and complementary regulations including those pertaining to IPR protection. These can include workshops and technical training assistance on establishment of competent data protection authorities and on enhancing cross-border enforcement among others.

CHAPTER 1: SYNTHESIS REPORT

1. Data and growth

1.1. Introduction

As early as two decades ago, APEC had recognized the importance of digital economy including e-commerce in linking their member economies. In the 1998 Declaration, APEC Leaders commended the APEC Blueprint for Action on Electronic Commerce which set out principles for promotion and development of e-commerce in the region[1]. The Electronic Commerce Steering Group (ECSG) was established in 1999 to implement activities based on the principles identified in the Blueprint. In 2014, APEC Leaders endorsed the APEC Initiative of Cooperation to Promote Internet Economy and the Ad-hoc Steering Group on Internet Economy (AHSGIE) was established to guide the discussion on issues arising from this area[2].

In line with the increasing importance of the digital economy, the interest to cooperate in this area remains strong. In the 2017 Declaration, APEC Leaders indicated that they would work together to realize the potential of the internet and digital economy, and welcomed the adoption of the APEC Internet and Digital Economy Roadmap (AIDER) and the APEC Framework on Cross-border E-commerce Facilitation[3]. Specifically on AIDER, it is a living document which is envisioned to promote the development and growth of internet and digital economy in the region and to advise APEC fora on potential areas of cooperation. It comprises 11 focus areas including the promotion of interoperability, promoting coherence and cooperation of regulatory approaches affecting the internet and digital economy, and facilitating the free flow of information and data for the development of the internet and digital economy while respecting applicable domestic laws and regulations. In 2018, under the Chairmanship of Papua New Guinea and the theme of "Harnessing Inclusive Opportunities, Embracing the Digital Future", APEC Leaders endorsed the APEC Action Agenda on the Digital Economy which among others, welcomed the establishment of the Digital Economy Steering Group (DESG), a new governance mechanism to monitor and evaluate progress made in the implementation of focus areas identified in AIDER[4].

The objective of this study, led by the Committee on Trade and Investment, is to contribute to the strand of work on digital economy by raising the awareness and deepening various stakeholders' understanding about the role of data in facilitating firms' business models and the challenges they face, as well as emerging legal and policy mechanisms related to data security and privacy protection. It also attempts to analyze the policy environment which allows data-utilizing businesses of different sizes to succeed and creates further data-utilizing business opportunities.

Case study approach

This project has taken a case study approach to better understand how firms utilize data and ensure the privacy and security of these data, as well as how policy environment are affecting their operations positively and/or negatively. The project has benefited from firm nominations by economies, as well as consultants' own network of contacts including trade associations, think tanks, academics and

[1] https://www.apec.org/Meeting-Papers/Leaders-Declarations/1998/1998_aelm
[2] https://www.apec.org/Meeting-Papers/Leaders-Declarations/2014/2014_aelm
[3] https://www.apec.org/Meeting-Papers/Leaders-Declarations/2017/2017_aelm
[4] https://www.apec.org/Meeting-Papers/Leaders-Declarations/2018/2018_aelm

individual firms[5]. Essentially, PSU or consultants would first contact these firms with additional information about the project and secure their agreements to participate. Guiding questionnaire provided by the PSU or consultants was generally open-ended and aimed at obtaining some basic information which were then expanded upon during the interview proper, follow-up emails and/or phone conversation. The response time by firms varies and can range from days to months.

In total, 39 firms from 12 economies have been interviewed and/or completed the questionnaire (Table 1). These firms come from a good diversity of industry sectors, including aviation, logistics, shipping, payment services, encryption services, and manufacturing (Table 2). Of these firms, 5 are small firms, 11 are medium firms, while the remaining 23 firms are large enterprises[6].

Table 1. Summary of participating firms by economy

Economy	Total no. of firms that have been interviewed and/or completed the questionnaire
Australia	3
Canada	2
Chile	1
Indonesia	1
Japan	12
Malaysia	2
Mexico	1
The Philippines	3
Singapore	4
Chinese Taipei	3
The United States	2
Viet Nam	5
Total	39

Source: Compilations by APEC Policy Support Unit (PSU) (as of 22 April 2019).

Table 2. Summary of participating firms (those that have been interviewed and/or completed the questionnaire) by sector[7]

Sector	No. of firms
Aviation	2
Logistics	5
Other transport (incl. railways and shipping)	2
Digital services and e-commerce	20
Health and education	2
Energy	2
Manufacturing	7

Note: Digital services and e-commerce also include data analytics services, cloud storage services, payment services, encryption services and artificial intelligence firms.
Source: Compilations by APEC Policy Support Unit (PSU) (as of 22 April 2019).

[5] APEC Policy Support Unit (PSU) has commissioned/engaged Aegis Consulting Group Pty Ltd and Information Technology and Innovation Foundation (ITIF) to undertake the project.
[6] A firm is categorized as small if it employs up to 20 people, medium if it employs between 20 and 200 people, and large if it employs more than 200 people.
[7] Note that the total number of firms in Table 1 and 2 do not tally as one of the firms is reflected twice in Table 2 for providing insights pertaining to digital services and e-commerce as well as manufacturing.

In addition, three focus group discussions had been conducted: on the margins of the Asia-Pacific Financial Forum event held in Singapore in June 2018; on the margins of the Digital Innovation Forum held in Taipei City in July 2018; and with Japan Electronics and Information Technology Industries Association (JEITA) and Japan Information Technology Services Industry Association (JISA) in Tokyo in September 2018. An additional meeting was conducted with JEITA in April 2019. Meetings were also conducted with representatives from the Confederation of Asia-Pacific Chambers of Commerce and Industry and Japan Institute for Promotion of Digital Economy and Community (JIPDEC).

Despite the insights, it should be acknowledged that reasons such as technical knowledge of participants as well as sensitivity around some issues including the utilization of cutting edge technology and/or services and broader business confidentiality reasons make it challenging to obtain more detailed information from some of these firms. The chapters in this report have identified some firms, but have also anonymized most of the firms as they prefer to remain anonymous as condition for their participation.

This synthesis chapter, prepared by PSU, is structured as follows. Section 1.2 presents a brief overview of the role of data on trade and growth. Section 1.3 provides some illustrations about how various traditional industries have adapted data utilization into their businesses, and how new industries (so called 'disruptors') are harnessing data to drive their businesses. Section 2 looks at the challenges to data utilization across economies and considers alternatives to some of the contemporary regulations. As challenges to data utilization also exist between organizations, Section 3 explores the factors contributing to the current state on data sharing and discusses several approaches to facilitate it. Section 4 concludes and proposes the way forward including the possible role of APEC in improving data-related regulations.

1.2. Data, trade and data-driven growth

Data analytics is arguably not a new phenomenon[8]. Business intelligence, as well as historical trend analysis and patterns have long been an integral part of many firms before the current development, which different stakeholders have termed by various names including data-driven growth, fourth industrial revolution, Industry 4.0. For example, firms in a particular sector would be interested to ascertain the most popular products sold in a specific economy before deciding whether to enter the market and if so, the strategies to capture market share. Many firms would also be keen to find out the preferences of their customers in terms of color, taste and size for instance.

However, this does not imply that it is business as usual. Advancements in information and communication technologies (ICT) have lowered the cost of adopting data analytics on a large scale and, along with it, the benefits and possibilities brought about by the adoption. Until several years ago, the cost of broadband subscriptions would have been prohibitively high for many firms and individuals that only a very small percentage had access to it. Fast forward to the present, the cost has fallen significantly in many economies. In the case of APEC, for example, the average monthly cost of fixed-broadband has fallen from purchasing power parity (PPP)$52.59 in 2008 to PPP$34.43 in 2017[9]. Likewise, the average cost of 1GB mobile broadband has fallen from PPP$28.92 in 2013 to PPP$24.08

[8] In this study, data is defined as any factual information that can be used for reasoning, discussion, and/or calculation. There are many different ways by which data can be categorized. Examples include personal and non-personal, quantitative and qualitative, specific and aggregated.

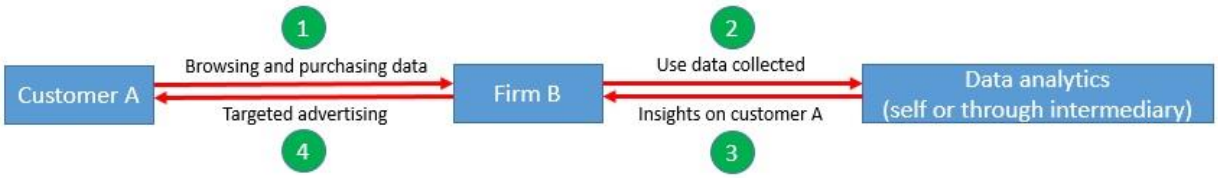
[9] Based on information from ITU, the fixed-broadband sub-basket is based on a monthly data usage of (a minimum of) 1 GB for comparability reasons. For plans that limit the monthly amount of data transferred by including data volume caps below 1 GB, the cost for the additional bytes is added to the sub-basket.

in 2017 (International Telecommunication Union (ITU), 2019). Twenty-three per 100 inhabitants in APEC collectively have access to fixed broadband in 2017, more than double the number in 2008 (9.4 per 100 inhabitants). With broadband comes increased bandwidth and hence, the rate at which data is generated and collected. Indeed, McKinsey Global Institute (2016) estimated that at approximately 210 terabytes per second, the amount of global data flows in 2014 was 45 times greater than that in 2005. Data flow was projected to increase by another 9 times over the next five years. Furthermore, the same publication showed that economies with higher internet penetration reap up to 25 percent more benefit from cross-border data flows than those with limited penetration. The advent of 5G technology is expected to further increase bandwidth and lower cost.

Cloud computing is yet another example of ICT advancements. Sometime ago, an entrepreneur whose business requires her to invest in an in-house server and hire large engineering team to build the systems from scratch among others would have raised her upfront capital investment and corresponding overheads significantly, a cost which not many entrepreneurs can afford given the budget constraint. Today, one of the many options available to her would include buying incremental server capacity from cloud computing service providers (e.g. Alibaba Cloud, Amazon Web Services, Google Compute Engine and Rackspace) and if necessary, hiring smaller development team to build on top of the pre-existing platforms instead. Essentially, cloud computing has turned a fixed ICT cost into a variable operating cost. Depending on the business model, the affordability made possible by cloud computing has reduced the cost of starting a business to as low as USD3,000 in contrast to about USD2 million in the 1990s (Pepper et al, 2016). Based on industry data, the United States International Trade Commission (USITC, 2017) estimated that about 70 percent of all internet traffic went through cloud data centers in 2015, up from approximately 30 percent in 2011.

The incorporation of Internet of Things (IoT) in many everyday objects such as refrigerators and televisions has also contributed to this data-driven economy as it allows large number of items that were previously unconnected to connect to the internet and therefore, send and receive data. Complementing the adoption of these technologies are the exponential growth in computing power, as well as many tools and solutions which have allowed firms to make sense of the huge amount of data collected in the form of big data analytics[10] within a reasonable amount of time. For example, analysis of a consumer's past transactions and search history allows firms to draw insights and predict her preferences and likely future behavior (Figure 1). Aggregating these information by categories such as age groups and locations and further analyzing them enables firms to infer the preferences of this category of people and produce tailor-made advertisements targeting them.

Figure 1. Simple illustration of how targeted advertising works



Source: Authors

Consequently, although data has always been an integral part of many firms for a considerable period of time, the above factors have served to further embed its role, particularly in areas where its utilization would have been out of reach until recently. As readers will see in later sections which provide more

[10] There is currently no agreed definition of big data. However, one general understanding is that it is a collection of large datasets obtained through a wide range of online and offline sources. The data collected may be unstructured, structured and/or both and organizations are able to analyze them to predict patterns and trends among others depending on their ability.

specific examples on how firms utilize data, not only do data enable other flows including goods, services and people (e.g. coordinating international production and enhancing efficiency of customs clearance at the border), they are also useful in their own rights (e.g. allowing firms to better understand the profile of their customers). The importance of data in business will only accelerate as more and more people and devices are connected to the internet. Cisco (2018) estimated that the number of networked devices will increase by about 10.5 billion between 2017 and 2022. Moreover, the number of networked devices per capita would be 3.6 in 2022, up from 2.4 in 2017.

Increasing number of literature are indicating the importance and contribution of data to economic growth as well as employment although it should be recognized that limitations means such statistics often reveal partial picture and may only provide rough estimates. McKinsey Global Institute (2016) found that global flows raised world GDP by at least 10 percent (which is valued at USD7.8 trillion in 2014) and that the contribution of data flows is only second to that of goods (USD2.3 trillion vs. USD2.7 trillion). Moreover, considering that cross-border data flows also enable other types of flows including goods[11], the combined indirect and direct contribution of data flows to world GDP would be higher than that of goods. Furthermore, economies at the margins/border of the data flow network stood to benefit more than those at the center, with some of them potentially growing their GDP by more than 50 percent.

Meijers (2014), which used internet penetration as proxy for data flows, demonstrated that a ten percentage point increase in internet penetration led to a 0.17 percentage point increase in economic growth indirectly. Qiang et al (2009) estimated that a 10 percent increase in broadband access is associated with a 1.38 and 1.21 percentage point increase in GDP growth in developing and advanced economies respectively. Osnago and Tan (2016) found that a 10 percent increase in internet penetration in exporting economy leads to a 1.9 and 0.6 percent increase in exports along the extensive and intensive margin respectively.

The internet also led to increased trade through its impact on firm productivity. For example, USITC (2014) indicated that the internet improved the productivity of digitally intensive industries by 7.8 to 10.9 percent. Grimes et al (2012) found that broadband access increases firm productivity by 7 to 10 percent. McKinsey Global Institute (2011) showed that the internet creates 2.6 jobs for every job destroyed.

1.3. Role of data in various sectors[12]

Transport and logistics

Firms in the transport and logistics sectors collect significant volumes of personal data, including information provided by customers when booking flights, shipping services and railway tickets; information provided by customers when booking ancillary services offered in conjunction with the main services (e.g. accommodation, car hire and leisure programs); customer information provided by third-party booking services such as travel agents and internet-based travel booking sites.

[11] For example, cross-border e-commerce now accounts for 12 percent of global goods trade. Data flows allow service exports to be delivered digitally. Digital transactions and communication enable FDI. People flows have also benefited from digital platforms such as Booking.com and AirBnB.

[12] Materials for this section are obtained mainly from the sectoral chapters provided by Aegis Consulting Group Pty Ltd, ITIF and PSU, and complemented with desktop research by PSU. The sectoral chapters are appended in this report as Chapters 2 to 9.

In addition, firms collect performance data from assets such as aircrafts, vehicles, shipping fleets and trains both directly during inspections and remotely. Specifically on the latter, data collection is facilitated by satellite and GPS technology. Where firms have alliances and partnerships with other firms in the form of code sharing arrangements for instance, data collected also include information of shared customers as well as assets jointly used by partners.

Firms use the data for various purposes. For instance, firms use personal data of customers to develop and tailor attractive loyalty schemes in the form of discounts, new/improved services, ancillary benefits, etc. and in so doing, lead to more purchases of their main offerings (i.e. provision of transport and logistics services). Likewise, data shared between partner firms ensures seamless travel experience and more satisfied customers, hence increasing the likelihood of repeat purchases. Indeed, customer relationship management is one of the key activities to grow firms' market share in competitive markets.

With regards to performance data of assets, firms use them to monitor and assess the safety, capacity and efficiency of asset deployment. These are then employed to enhance safety, improve cost recovery, increase cargo yields, optimize competitiveness and strengthen customer responsiveness in terms of tracking and delays for example. KPMG (2017) indicated that bus operators usually put in place a common fleet management system to facilitate fleet management and schedule adherence so that drivers can more accurately estimate distance between it and earlier bus, as well as compare its position to a scheduled position. Data on delivery routes and timings are used to provide customers with better estimates of delivery lead times. In fact, many providers now provide customers with the ability to track their parcels in real time.

Manufacturing

Manufacturing firms collect and utilize significant amount of data to ensure the smooth functioning of their global value chains (GVCs). Cross-border data flow is increasingly vital as critical information need to be exchanged internally between R&D centres, production facilities, headquarters as well as externally with other parties including suppliers, logistics providers and customers which tend to be scattered all over the world. The types of data include technical data, production data, procurement and sales logs, product usage information and customer information among others.

Efficient data flow allows R&D teams which are located across different economies to communicate and collaborate with one another. It also allows firms to plan and coordinate production activities across different facilities and provide remote technical assistance and guidance where necessary. By live monitoring the production machineries, firms are able to reduce downtime by preparing immediate replacements and scheduling predictive maintenance. After the products have been sold, information such as usage information and customer feedback can be collected and analyzed in order to create more value-add such as effective after-sales services and product improvements.

Consumer services (energy, healthcare and education publishing)

Firms in the consumer services sectors also collect significant volumes of data. For instance, the firm which supplies smart meters and provides metering service collect information provided by individual customers when they become service users. Another firm which publishes education materials and distributes them worldwide digitally collect information provided by customers when they purchase e-books online.

Firms use the data collected for a wide range of purposes. The firm which supplies smart meters, for example, provides the relevant data to energy retailers for the purpose of customer billing. Being an intermediary, the firm is also well-positioned to provide energy pricing and products to end customers and in so doing, support sales of the energy retailers. Moreover, the firm provides data (but not necessarily the same data) to network providers for the purpose of network load management. Both this firm as well as the one which distributes e-books are believed to also use customers' data to develop

loyalty programs and tailor experience based on their preferences. Firms in the healthcare industry may use data collected from different economies for collaborative research activities. For patients who travel for medical treatment, some medical data pertaining to him/her may have to be shared between institutions based in different economies to facilitate diagnosis. In some cases, medical data may have to be sent to another location for remote diagnosis.

Encryption services

Encryption is the process of securing data from unauthorized access or use by changing it from a readable format (such as plaintext) to a non-readable one (such as cipher text). Data is central to encryption services providers because it essentially justifies their very existence. With the advent of digital economy, encryption is likely to become more important as increasing number of people and firms put their data online and data traffic continue to increase.

Besides being a sector in its own right, encryption services play both direct and indirect role in supporting the digital economy. By ensuring the integrity of underlying data, encryption and other cryptographic tools allow for complete execution of authentic instructions by users. It also enables firms and consumers to securely engage in various online activities including logging on to specific applications and communicating privately via email and instant messaging. Many firms also use encryption to protect the confidentiality of their R&D activities from competitors and hackers.

Payment services

Data is integral in every step involved in processing a transaction, but such data is only one component of the whole spectrum of data collected and used by payment services providers. These include identity and demographics data such as identity number, age, nationality, address, education as well as credit history, transactions data and online interactions.

Firms carry out data analytics to glean valuable information contained in both traditional and alternative data as well as structured and unstructured data. At the most basic level, firms aggregate, summarize and provide traditional and structured data in the form of standard daily transactions report to merchants. At the same time, firms also use advanced analytics on other collected data to provide value-added services to customers and merchants so as to remain competitive. For example, depending on available data, firms can determine the payment obligations of individual customer so as to evaluate his/her debt service ratio and remaining net income. Firms are also able to predict the likely behavior of customers based on information such as credit incidents and debt falling due among others. The fact that payment services providers act as intermediary between banks, merchants and customers means that they are able to collect customers' perceptions of the service level provided by banks as well as merchants.

Electronic invoicing services

Electronic invoices (EIs) record an entity's commercial transactions data in electronic form. EIs and the corresponding data recorded within them can contribute to significant improvement in other related services. For example, data captured in EIs can facilitate transparency and hence authorities' expanded use of tax, accounting as well as other data sources to ensure compliance. Authorities can also employ data analytics on these information to cross-reference and better understand the complex relationships between various stakeholders and if necessary, trigger audits. Indeed, the interviewed firm shared that it provides a single platform to integrate and transform invoices from different enterprise resource planning (ERP) services into an electronic format, which is then transferred to local tax authorities for validation and processing.

In addition, by extending EI to electronic payrolls (EPs) that include information on salaries for example, authorities are able to determine accurately the social security contributions and personal income tax payable to a specific individual. The traceability associated with it means that EIs and its

underlying data have also opened other possibilities. For instance, it was indicated that EIs' traceability has made it possible for relevant agencies to analyze the local value-added contribution and market composition of specific production networks as well as entire economic sectors. Specifically on supporting cross-border digital trade and e-commerce, EIs can facilitate the development of more transparent, efficient and secure factoring (i.e. the selling of invoices or accounts receivables for cash so as to meet working capital needs), especially for SMEs.

Artificial intelligence (AI)-related services

Data is at the center of firms using AI-based analytics as a business in itself or as a part of their business model. This is because these firms rely on the ability to collect, use, transfer, and share a large volume and diversity of data to offer their services. One of the interviewed firms employs a hybrid of techniques ranging from decision-based rules and statistical methods to machine learning (ML) and artificial intelligence (AI) to undertake real-time data analytics, pattern recognition and anomaly detection. These are then subsequently used to audit past activity, detect inadmissible behavior and prevent potential transgressions among others.

Yet another firm provides rapid screening services of employees, contractors and tenants by checking criminal records, credit reports, and motor vehicle and driver records from around the world. Essentially, it is able to conduct both basic and enhanced identity verification services. Although data may be at the center of their business, it is not always the case that the firms providing the analytics services also collect the underlying data. This further underscores the importance of facilitating data flows. One interviewed firm, for instance, helps its clients develop and use its proprietary AI and ML technology to improve their collection, organization, and analysis of their own data so as to enhance efficiency in areas such as logistics and marketing.

Other digital services (e.g. business information services, e-commerce, cloud computing)

Despite providing very diverse services, one general similarity among firms in the digital sector is the huge amount and type of data that they collected. They range from personal information such as names, addresses, biometric profiles and financial data to performance data of assets. These data have been collected from various sources, including those provided by their business clients to the extent necessary to provide required services; by third-party providers; and by their own customers. In addition, firms collect performance data from their own products, websites, as well as devices running their applications remotely.

Firms use the data for various purposes depending on the type of services that they offer. For instance, firms which provide a range of software services to other sectors analyze the data to provide enterprise solutions. Another firm assists business clients with large digital databases in combatting fraud. One firm analyzes the performance data of their business clients' assets to enhance reliability, improve efficiency and avoid unplanned downtime. Yet another firm helps clients to make sense of their customers' responses in social media platforms and in so doing, enable their clients to adapt and improve their offerings.

Specifically for firms specializing in digital advertising, they are usually able to aggregate and categorize customers' data into different segments, allowing advertisers to then access specific segments for a fee. They can also analyze customers' purchasing habits and correspondingly display advertisements on platforms that are most relevant to customers. Furthermore, advancements in algorithms have enabled them to offer dynamic advertising, that is, reminding customers who had viewed some products but did not complete the purchase and offering them additional discounts, hence raising the conversion rate.

1.4. Supporting factors to optimize the use of data in a data-driven economy

Besides advancements in ICT which have lowered the cost of adopting data analytics, other supporting factors are needed to fully optimize the benefits of the data-driven economy. Some of them are discussed here.

Strong internal data privacy and security governance

Given the important role of data in ensuring the viability of their businesses, firms need to take data privacy and security seriously. To this end, many interviewed firms generally indicated that they have undertaken various activities to ensure the privacy and security of data collected and managed by them. These include ensuring that their policies, procedures and practices are consistent with international quality assurance instruments governing data security and privacy. Several firms shared that this is primarily achieved by complying with ISO27001 and BS10012. The ISO27001 is the international standard for information security and provides the basis for achieving the technical and operational requirements necessary to comply with EU's General Data Protection Regulation (GDPR), while the BS10012 provides the core standards that firms need to comply when collecting, storing, processing, retaining or disposing personal records related with any individuals[13]. Firms also undertake regular and systematic review of various laws and regulations enacted by economies to govern data privacy and security so as to ensure compliance.

Several firms indicated that they apply sophisticated and comprehensive in-house data governance framework and that it usually consists of firstly classifying all data according to its sensitivity and restricting access to data within the firm based on sensitivity level. Trainings are also provided to staff who handled different types of data including customer and business data so as to raise their awareness about cyber security and to impart best practices.

Furthermore, firms endeavor to manage data flows within secure, transparent and auditable frameworks in various ways. For example, they assess the most secure and trusted hardware and location when choosing storage infrastructure; Many firms also have their own cyber protection teams which are usually involved in the design and operation of their data governance frameworks. In addition, firms apply end-to-end encryption on all data flows over the internet and across the borders. Most firms also have governance structures where relevant officers must report against certain agreed key performance indicators pertaining to data security and privacy. Increasingly, many firms have specific executives such as the General Counsel and Chief Information Officer whose main responsibility include data privacy and security management.

Openness to new technologies and digital literacy

Despite the perception that new technologies and innovation including data analytics are around us, the fact is different economies, sectors and firms have unevenly embraced technology including digital ones. A case in point would be the United States where a study by McKinsey Global Institute (2015) indicated that it only captured about 18 percent of its digital potential even though it is one of the most digitized economy. Looking at individual sectors, the study found that sectors such as agriculture & hunting, mining, construction, and entertainment & recreation had relatively low digitization compared to sectors such as ICT, media, and professional services. The gap in adoption and utilization between sectors and firms on the frontier vis-à-vis the rest of the economy appears to have widened in certain cases.

[13] See section 2.4 of this chapter for more details.

Although multiple factors determine the pace and extent of technology adoption, openness is arguably one of them and firms with less risk aversion to new technologies are more likely to benefit compared to their peers. McKinsey Global Institute (2015) indicated that in most digitized sectors, profit margins and productivity have grown by 2 to 3 and 4 times, respectively compared to less digitized sectors on average.

Adoption of new technologies also need to be complemented with corresponding human capital who are able to make use of them efficiently and productively. These include data scientists, cybersecurity as well as privacy professionals. Indeed, KPMG (2017) indicated that among some of the main challenges faced by firms in employing greater use of data analytics is the lack of skilled labor, particularly those with sufficient industry experience. Trade associations interviewed as part of this project concurred with this observation. They shared that many of their member firms had reported skill shortages in digital capability. As indicated in the APEC Economic Policy Report 2017, developing active labor market policies, a holistic coordination mechanism that link different components of skills training and development on one hand, and job search and skills matching on the other, could be one way of overcoming this issue. Reforming the education systems to ensure that basic skills in the science, technology, engineering and mathematics (STEM) fields can be better integrated into school curriculum, as well as to enhance the teaching of skills such as creative thinking and logical reasoning/problem solving are among the other solutions to ensure that there is a healthy pipeline of human capital capable of contributing to and benefiting from the data-driven economy.

Supportive regulatory framework

New technologies bring with it new and innovative ways of doing business, models which existing regulatory framework may not have considered for various reasons including the fact that many of these models were not prevalent when the framework was formulated. Take e-commerce for example. In an APEC Policy Support Unit (PSU) policy brief, Pasadilla and Wirjo (2018) noted that there are still many economies which require sellers listed on domestic-based e-commerce platforms to be registered domestically. The resources required to comply with such regulations may effectively foreclose the chances of many MSMEs to sell through these platforms. Other regulations that vary across economies add to the difficulties. For example, the use of e-signature (and by extension e-contracts) are regulated to varying extent by individual APEC economies[14], which may make online contract fulfillment more burdensome and costly. In many economies, de-minimis value as well as customs procedures act as burdens to the full utilization of e-commerce as a sales/revenue channel by many firms.

Developing balanced regulatory frameworks is critical because on the one hand, those which are not in line with the evolving economic landscape may limit the opportunities brought forth. On the other hand, over-regulations may risk nipping innovative and promising ideas in the bud unintentionally. In line with the main objective of this project, the rest of this synthesis report will focus on data-related policies and how they affect data-utilizing businesses.

2. Challenges across economies

2.1. Calls for more legitimate data privacy, protection and security

Naturally, the importance of data as a new asset has brought to the fore concerns on how firms use and protect the data that they have. While customers and businesses benefit from targeted marketing and

[14] https://www.docusign.com/how-it-works/legality/global.

customized product offering in a sense that they are offered products which are more closely aligned with their preferences, the ability of businesses to use these personal information has also led to concerns around data privacy. The increasing dependency of businesses and the economy collectively on data means that there is an ever-present danger of cyberattacks aimed at exploiting them and causing massive damage to the economy. As much as data is an asset, it has arguably become a liability as well.

These fears in the data age are not unfounded. News articles are abound of hacking incidents and data leaks. For example, India's Aadhaar system which provides a 12-digit unique identity number to its residents based on their biometric and demographic data was hit sometime in 2018. Specifically, the Aadhaar numbers and bank details of more than 134,000 beneficiaries on Andhra Pradesh Housing Corporation's website were leaked online[15]. In October 2018, Cathay Pacific announced that it discovered unauthorized access to its system which contained personal information of 9.4 million customers. While there was no evidence of data misuse so far, information accessed include particulars such as nationality, date of birth, address, phone number, travel history, as well as 860,000 passport numbers, 245,000 identity-card numbers, 403 expired credit card numbers and 27 credit card numbers without security code[16]. Amazon shared that the data of some customers were unintentionally exposed due to technical error but did not provide more details about the incident and the number of affected users[17]. In 2016, it was discovered that Uber had covered up a massive breach involving the personal details of about 57 million passengers and drivers[18].

More recently, Quora, a question-and-answer website, reported a data breach where 100 million user accounts were compromised. Fifty million users were affected when Facebook was hacked. The hacking of Marriott exposed the personal data of 500 million people[19]. The browser-based role playing game Town of Salem started 2019 with a discovery that its complete player database was breached. Data containing email addresses, IP addresses, passwords and billing information of more than 7.6 million players were exposed[20].

In terms of costs, a study conducted by the Center for Strategic and International Studies (CSIS) and McAfee (2018) noted that close to USD600 billion is lost to cybercrime annually, up from about USD445 billion in 2014. It further indicated that some cybercriminals are as sophisticated as the most advanced ICT companies and had adopted technologies such as cloud computing, AI, Software-as-a-Service (SaaS) and encryption.

The practices of some well-known firms also leave more to be desired. Facebook, for example, was revealed to have given other firms far greater access to data than it had disclosed. In addition, it claimed that it was not required to seek the consent of users before sharing data with most of its partners since

[15] Straits Times. 2018. India's biometric ID system hit by leaks. August 24. https://www.straitstimes.com/asia/south-asia/indias-biometric-id-system-hit-by-leaks

[16] Cathay Pacific. 2018. "Cathay Pacific Announces Data Security Event Affecting Passenger Data." October 24. https://news.cathaypacific.com/cathay-pacific-announces-data-security-event-affecting-passenger-data; Park, K., and Hong, J. 2018. "Millions of Passengers Hit in Worst Ever Airline Data Hack." *Bloomberg*, October 25. https://www.bloomberg.com/news/articles/2018-10-25/cathay-pacific-reports-data-breach-affecting-9-4-million-fliers

[17] Straits Times. 2018. Amazon says some customers' data exposed. November 23. https://www.straitstimes.com/world/united-states/amazon-says-some-customers-data-exposed

[18] Straits Times. 2017. Uber concealed cyber attack that exposed data of 57 million users and drivers. November 22. https://www.straitstimes.com/world/uber-says-cyber-breach-compromised-data-of-57-million-users-drivers

[19] BBC. 2018. "Marriott Hack Hits 500 Million Starwood Guests." November 30. https://www.bbc.com/news/technology-46401890

[20] Winder, D. 2019. "Town of Salem Hacked Leaving More Than 7.6M with Compromised Data." *Forbes*, January 3. https://www.forbes.com/sites/daveywinder/2019/01/03/town-of-salem-hacked-leaving-more-than-7-6m-with-compromised-data/#4c9f357a30d3

they are considered an extension of Facebook. Using internal records which contain data-sharing deals involving more than 150 companies, it was reported that Facebook allowed Microsoft's Bing search engine to see the names of almost all Facebook users' friends without their consent. The same report also claimed that Facebook gave some firms like Netflix and Spotify the ability to access and read users' private messages and granted access to Amazon to obtain users' names and contact information through their friends. Assuming that these partnerships are legal, the findings that partners were still able to access data even after the partnerships had ended are certainly questionable[21].

Another report indicated that Facebook had allowed developers access to photos that users had uploaded but never posted[22]. Perhaps one of the most damaging is the finding that a political consulting firm had obtained information on millions of Facebook users and used them for targeted political advertising in some economies[23]. Google and Twitter were alleged to have violated data privacy too[24].

Consequently, there have been increasing calls to ensure data protection and security for reasons such as improving privacy of individuals and protecting domestic security. There are also other public policy objectives. For example, governments may wish to: 1) have rapid access to data in order to solve past crimes and/or thwart future crimes including terrorist attacks; 2) control huge amount of information which some firms may exploit to become a natural monopoly and potentially exert to gain certain market power; and 3) benefit more from the digital economy in terms of employment, innovation/technology know-how, etc.

2.2. Emerging regulations including data protection laws

In response, governments across the world have put in place or are in the midst of enacting various regulations aimed at data including its protection, privacy/security and access. These regulations usually pertain to the following non-exhaustive areas such as: those defining personal/sensitive data; those regulating data collection, storage, processing and transfer; those requiring firms to undertake certain procedures to ensure data protection and privacy are embedded in their operations (e.g. designating data protection officer), and to put in place procedures that would be activated in the event of data breach (e.g. informing affected customers about their data being compromised within certain time from discovery). Some of these regulations, in particular those shared by participating firms are elaborated below.

Local data storage, processing and/or transfer

[21] Dance, G.J.X., LaForgia, M., and Confessore, N. 2018. "As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants." *The New York Times*, December 18. https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html; The Straits Times. 2018. "Facebook Says Companies Got Access to Data Only After User Permission." December 19. https://www.straitstimes.com/world/united-states/facebook-says-companies-got-access-to-data-only-after-user-permission; The Straits Times. 2018. "Facebook Used People's Data to Favour Certain Partners and Punish Rivals, Documents Show." December 6. https://www.straitstimes.com/world/europe/british-lawmakers-release-internal-facebook-documents

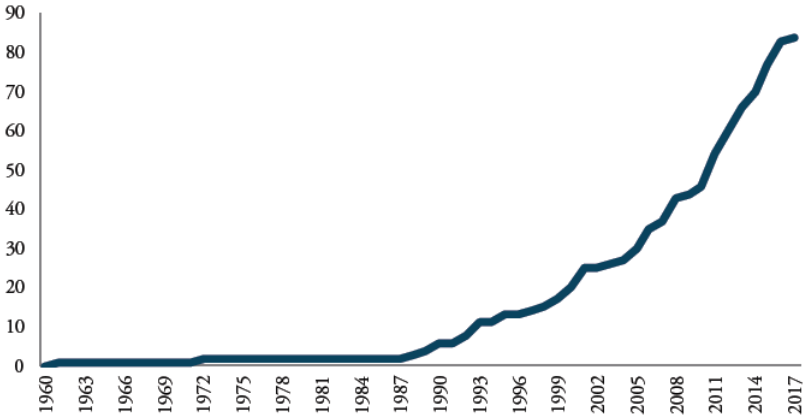
[22] BBC. 2018. "New Facebook bug exposed millions of photos." December 14. https://www.bbc.com/news/technology-46567131

[23] Dance, G.J.X., LaForgia, M., and Confessore, N. 2018. "As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants." The New York Times, December 18. https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html

[24] Ibid.

Among the regulations enacted by economies, those related to local data storage, processing and/or transfer are arguably one of the most numerous. Based on her own compilations, Ferracane (2017) showed that the number of regulations, specifically restrictions on cross-border data flows has increased significantly over the last decade or so (Figure 2). Such regulations put varied constraints on free flow of data between economies.

Figure 2. Cumulative Number of Restrictions on Cross-border Data Flow (1960-2017)

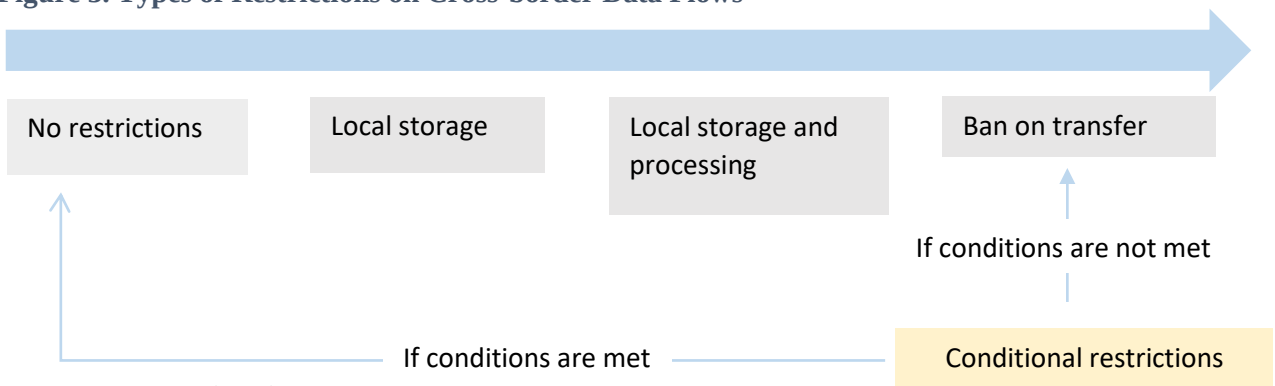


Source: Ferracane (2017)

Regulations on local storage, processing and/or transfer can be grouped into several categories. In the same paper, Ferracane (2017) classified the current restrictions into two major groups, namely those imposing strict restrictions and those imposing conditional restrictions on cross-border data flows. Specifically on the former, it is further split into three main categories depending on the level of strictness: 1) only local storage requirement; 2) both local storage and processing requirement; and 3) complete ban on data transfer (Figure 3).

With regards to the latter group (i.e. those imposing conditional restrictions), she further categorized them into whether: 1) the conditions apply to the recipient economy; or 2) to the data controller or processor. It is important to note, however, that a conditional restriction is not necessarily less restrictive (and hence less costly) relative to a strict restriction, as the condition could be very difficult to meet that transferring data cross border becomes almost close to impossible for most firms. An economy usually employs a mix of strict and conditional restrictions in its privacy regimes.

Figure 3. Types of Restrictions on Cross-border Data Flows



Source: Ferracane (2017)

Strict restrictions - local storage

Based on the definition, local storage requirement (or data mirroring) is arguably the least restrictive compared to the other two as it does not restrict data flow including cross-border transfer as long as a

copy is stored domestically. It usually applies to certain types of information such as tax and accounting records or social documents for the purpose of legal and easy access by law enforcement officials. For instance, Sweden enacted the Bookkeeping Act in 1999 which requires firms to keep their annual financial reports and balance sheets in Sweden physically for a period of seven years (Ferracane, 2017). One APEC economy enacted a law in 2013 which requires a wide range of firms providing online services such as social networks and online game providers to build at least one data server locally to allow for inspection, storage, and provision of information at the request of the authorities (Cory, 2017).

Strict restrictions – local processing

Local processing requirements require firms to store and process data domestically. To fulfill this requirement, firms usually need to establish their own data centers, or use local data processing providers. Firms are allowed to transfer the processed data abroad for business or other legitimate purposes, if no other requirements are set in the law. As an illustration, one interviewed firm shared that one APEC economy enacted a new payment systems law a few years ago which require international payment providers to transfer their processing capabilities (with respect to their domestic operations) to a local state-owned operator. In Turkey, the Law on Payments and Security Settlement Systems, Payment Services and Electronic Money Institutions requires firms to maintain data storage and processing facilities in the economy.

Strict restrictions – ban on transfer

A complete ban on data transfer requires data to be stored, processed and accessed within the border and does not allow any copy of data to be sent overseas. This usually applies to extremely sensitive information such as tax, health and financial data. In 2012, one APEC economy enacted the Personally Controlled Electronic Health Records Act, which requires that personal health information should not be held or taken outside the economy. Such information cannot be processed or handled outside the economy as well.[25] Another APEC economy requires all federal tax information be received, processed, stored or transmitted by servers within its territories, embassies, or military installations.[26] Two provinces in yet another APEC economy regulate that personal data held by public institutions including schools, hospitals and public agencies shall be stored and accessed only in the economy, except for certain cases (Cory, 2017). In the financial sector, the central bank of one APEC economy stipulated in 2011 that the personal financial data gathered within the economy by commercial banks or financial institutions should be stored, processed and analyzed within the border, and such information is not allowed to be transferred overseas.[27]

Conditional restrictions

Conditional transfer of data does not explicitly require local data storage or processing, but specifies what the data recipients, controllers and/or processors need to fulfill before they can transfer and receive data. The conditions vary and can range from obtaining approval from the relevant authorities to seeking consent from the data providers. For instance, one APEC economy enacted the Personal Information Protection Act in 2011, which provides some general guidance on handling of personal information.

---

[25] Australia. 2012. *Personally Controlled Electronic Health Records Act 2012*. https://www.legislation.gov.au/Details/C2012A00063

[26] U.S. Department of the Treasury, Internal Revenue Service. 2016. *Publication 1075*. https://www.irs.gov/pub/irs-pdf/p1075.pdf

[27] People's Bank of China. 2011. "Notice of the People's Bank of China on Urging Banking Financial Institutions to Protect Personal Financial Information." http://www.gov.cn/gongbao/content/2011/content_1918924.htm

Specifically on the transfer of personal data, it requires firms to inform and obtain the consent of the data subjects.[28]

Other forms of conditions include requiring security assessment by a law enforcement agency before data can be transferred abroad. One example is an APEC economy's Cybersecurity Law, which came into force in June 2017. It requires that personal information or important data collected and produced within the economy by critical information infrastructure operators should be stored domestically[29]. Meanwhile, it indicated that if cross-border data transfer to other economies is necessary for the purpose of business operations, a security assessment needs to be done in accordance with the procedures issued by relevant departments, unless laws or regulations provide otherwise.[30]

It is worthwhile to note that the above classification only aims to give a simplified categorization of various data-related regulations. In reality, regulations are more complex and come with many prescribed circumstances or exceptions. Thus, it is challenging to categorize each regulation into a single, mutually exclusive category. For instance, even a strict ban on data transfer would usually allow for exceptions if certain conditions are met. Going by this argument, all restrictions are technically conditional in nature. In one APEC economy, despite its personal data protection regulation indicating that data cannot be transferred outside the economy unless the place has been specified by the government, exceptions are given in certain circumstances such as when consent has been given by the data subject.[31]

Disclosure of intellectual property (including source code), building back-doors and use of mandatory encryption standards

Besides regulations on local storage, processing and/or transfer, those pertaining to encryption and source code disclosure represent another group of data-related policies enacted by governments. In an effort to improve privacy, firms have enhanced the security level of their product offerings. For instance, communication applications such as Whatsapp and Signal have employed end-to-end encryption which allow only the sender and intended receiver to view the messages. While privacy has been enhanced, it has at the same time created investigation obstacles by law enforcement officials particularly when criminals use these applications to avoid surveillance. To circumvent it, governments have instituted various regulations such as mandating technical assistance from firms to decrypt information, building back-doors in their digital products so as to give authorities access to the encrypted information of the users, requiring the use of certain domestic encryption standard as well as disclosure of intellectual property including source code.

Within APEC, one economy was indicated to have mandated the use of domestic encryption products in telecommunications infrastructure, such as for 4G. Another economy recently passed a bill which requires technology firms to provide technical assistance to governments in accessing encrypted

---

[28] Korea. 2011. *Personal Information Protection Act.*
http://koreanlii.or.kr/w/images/0/0e/KoreanDPAct2011.pdf

[29] The critical information infrastructure (CII) refers to network facilities and information systems of important industries and sectors including but are not limited to public communication and information services, power, traffic, water resources, finance, public services, e-government, as well as of other industries whose data may cause severe harm to domestic security, people's livelihood and public interests if those infrastructure are damaged, malfunction, and/or suffer from data leakage.

[30] China. 2016. *Cyber Security Law of the People's Republic of China*.
http://www.miit.gov.cn/n1146295/n1146557/n1146614/c5345009/content.html

[31] Malaysia. 2016. *Personal Data Protection Act 2010.*
http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20709%2014%206%202016.pdf

information. The same bill also allows government to compel firms to create a back-door which allows access to encrypted messages without the user's knowledge.[32]

Non-alignment between regulations

Economies have their own, divergent objectives for putting in place certain regulations (including those pertaining to data). As a result, firms often have to deal with different regulations in multiple jurisdictions at the same time. Besides raising their compliance burden, these competing views may impact the capacity and liabilities of firms to collect, manage and use data.

Several interviewed firms, for example, raise perception on data ownership as an issue which varies between economies. In some economies, all data are assumed to be owned by the consumer, whereas other economies consider that data are owned by the firm or the government. The multiplicity of approaches derived from this fundamental difference in assumptions can pose as a burden to firms that wish or already operate in more than one market.

Despite the United Nations Commission on International Trade Law (UNCITRAL) taking steps to improve the uniformity of economies' legal rules on e-transactions and e-signatures via model law development for instance, there remain significant differences on how economies enact their regulations pertaining to e-signature. A review by OECD and WTO (2017) put e-signature as among the top four challenges faced by firms and consumers.

In some cases, lack of mutual recognition essentially leads to duplication of procedures across economies where firms operate. For example, without arguing in favor of GDPR, it was shared that although firms using data of EU residents are already subjected to strict GDPR requirements which represents a comprehensive approach to data protection by the European Union (EU), other economies continue to put in place their own data protection regimes without due consideration that they may be duplicative in objective and intent.

[32] BBC. 2018. "Australia Data Encryption Laws Explained." *December 7*. https://www.bbc.com/news/world-australia-46463029

Box 1. Non-data related challenges faced by firms

Besides indicating how data-related regulations are affecting their business models, firms also shared about aspects of regulations which are arguably not related to core data handling per se but are nonetheless important and should be addressed if the full potentials of these firms are to be realized.

Lack of transparency and clarity

Firms noted the lack of clarity in some broadly defined regulations which raise more questions on what needed to be done exactly to fulfill the requirements. One firm cited as example the requirements to disclose the source code of its wireless communication devices by a non-APEC economy. As it was unclear the extent of disclosure needed, the firm decided to put on hold customs clearance of its products. Several firms also indicated that lack of transparency and clarity have led them to take the 'safer' route of not entering the market or dealing with certain customers/transactions (i.e. derisking) and/or over-regulating themselves (i.e. take strict interpretation of the regulations), both of which are costly.

Unintended effect of outdated regulations (i.e. in terms of market access, licensing, etc.)

The economic landscape is evolving rapidly but the fact that some existing regulations are put in place earlier means that they may not have taken into account the rapid changes. As a result, many firms, particularly those with innovative business models end up being negatively affected by these regulations inadvertently. For example, it was noted that there are limitations on the establishment and operation of non-bank payment providers in some economies. Existing policy frameworks may also make it challenging to ensure interoperability between mobile money and the financial system.

Source: various

2.3. But are some of these regulations the way forward?

While many of these regulations have been enacted with legitimate public policy objectives, there are questions on whether they are able to meet these objectives.

Data protection and security

As indicated in the previous section, one of the most common regulations that economies have enacted to ensure data protection and security is to require data localization. The fact that security is a function of several elements including technical, financial and personnel, however, means that the association between data localization and data security may not be a given. Furthermore, data localization regulations may have the unintentional effect of increasing the cost of doing business and therefore penalizing some firms, particularly those whose in-house security teams and data frameworks are already adequate.

Data localization requirements also mean that unless cloud computing providers base their servers there, users in the economy would not be able to access the services by these providers, including security practices which may be among the best in the world. Essentially, data localization requirements may have the inadvertent effect of weakening data protection and security instead of strengthening it.

Employment and investment creation

Data-related regulations such as data localization have been viewed as a tool to encourage the establishment of domestic data centers and therefore employment creation. However, information gleaned from several literature has shown that the employment aspect of domestic data centers may not be as rosy as expected. While they create some temporary construction jobs, data centers are mostly self-regulating and autonomous with minimal employees once in operation. For example, Facebook's massive data farm in Sweden employs only 150 people, one for every 25,000 employees in the economy (Lund and Manyika, 2017). Apple's USD100 billion data center in North Carolina in the United States generates 50 full-time jobs and 250 support jobs in other areas including security and maintenance. Microsoft's new data center in Virginia expects to create dozens of permanent jobs at most (Cory, 2017).

Supporters of data localization argue that it is one way to bring in the investment especially in infrastructure and level the regulatory playing field (i.e. the idea of needing to apply existing regulation to new digital entrants). Specifically on the latter, it was suggested that over-the-top (OTT) service providers use existing telecommunications infrastructure without paying license fees and therefore, are free-riding on infrastructure which is paid for by other users. Based on various sources, however, Meltzer and Lovelock (2018) noted that OTT providers do invest in infrastructure. For example, Facebook, Google and Netflix were said to invest in their own networks including cables, satellites as well as innovative alternatives such as balloons and drones.

Virtuous cycle is also created in the traditional sector in that users who subscribed to OTT services demand faster speed, which in turn spurs investment in broadband infrastructure and hence more OTT services offerings. OECD (2016) noted that policies promoting such virtuous cycle in the United States could have been responsible for driving the increase in investment by broadband providers by about USD212 billion between 2011 and 2013, more than any three-year period since 2003. In contrast, Castro and McQuinn (2015) showed several scenarios where data localization regulations negatively impact investment. Arguably, such regulations increases the cost of doing business in the economy and if the return of investment is not significant, firms may decide not to enter the market altogether.

Innovation and productivity

Investments are believed to bring technology know-how and along with it, improved productivity and additional innovation for the sector and the economy as a whole. This is indeed one of the main reasons why economies have generally been interested to attract foreign direct investment (FDI) and be part of the global value chains (GVCs). However, it is important to realize that not all investments bring the prized know-how or more appropriately, the desired diffusion. The nature of certain investments such as data centers which require minimal manpower means that only a handful would benefit and that is assuming the tasks undertaken by these people are of relatively high value.

Technological advancements such as broadband and cloud computing have made offsite data storage and analysis possible. In fact, it is these advancements that have made the business models of some firms viable. Strict data localization (collection, storage and processing) means that firms may find it difficult to combine data sets from different economies so as to perform collective data analytics which could be beneficial in providing more inclusive insights, hence negating their innovative business models and primary objective for entering the market.

It would also mean increase in the cost of doing business which may lead to firms deciding not to operate in the market. Consequently, client firms may face challenges accessing better and cheaper analytical tools than what are available in the domestic market, therefore nullifying the original intent of the regulations to improve innovation and productivity. In other words, the regulations would have inadvertently nipped something with potentials in the bud before it has a chance to thrive and benefit the economy in the long run.

The implications of this are arguably larger to micro, small and medium enterprises (MSMEs) than their larger counterparts. Take e-commerce as an illustration. If platform operators decide not to enter the market, in the worst case scenario, it would end up closing one sales/revenue channel that MSMEs can tap to access the global markets. In a report by eBay Public Policy Lab (2016), it was shown that almost all MSMEs that are registered as eBay online sellers in surveyed economies export globally, while relatively smaller percentage of those using traditional channels (offline) do so. It also noted that 90 percent or more of eBay sellers export to more than 10 international markets in some economies such as China; Korea; Indonesia; and Thailand. Facebook estimated that more than 50 million SMEs are on its platform and about 30 percent of their fans are cross-border (McKinsey Global Institute, 2016).

Specifically on intellectual property rights (IPR), even if there are valid grounds for economies to require disclosure, it is important that economies complement this requirement with strong IPR protection. Indeed, some interviewed firms in the transport and logistics sector have expressed concerns about disclosure requirements in joint venture and/or open innovation projects, particularly in economies which have challenges in enforcing intellectual property rights. Firms in the digital sector also expressed fairly similar concern. Failure to address these concerns may inadvertently affect investment and innovation, reasons that have led to the requirements in the first place.

Addressing domestic security

Part of the data-related regulations such as data localization as well as those requiring firms to provide back-door access to the relevant authorities are arguably intended to provide law enforcement officials quicker means of entry to data, which can then be used to solve past crimes and/or prevent future crimes. There are two considerations. One, if it pertains to cross-border access of data by officials, there is already a process under the mutual legal assistance treaties (MLAT). Some economies have also negotiated data sharing agreements. If the current process (such as the time taken to respond to a request) can be further improved, then reforming the MLAT and/or these data sharing agreements should be the first-best option[33]. Instituting data-related regulations has other unintended costs and therefore, a second-best option.

Two, data localization is not equivalent to allowing full data access by officials. Firms realize the importance of ensuring data privacy and protection. Indeed, several interviewed firms viewed such commitment as part of their social contracts to operate. In other words, firms are likely to have certain frameworks in place to ensure that any request for data access is legal rather than to allow open, blanket access.

Specifically on provision of back-door access, several argue that the regulations ironically run counter to the principles behind data security and privacy. In fact, the existence of back-door makes the products more vulnerable to hackers and undermine the overall security of the products.

[33] See section 2.4 of this chapter.

Box 2. Cost of data-related regulations

Despite being enacted with certain public policy objectives in mind, the discussions in this section have alluded that contemporary data-related regulations including data localization and fragmented regulations have real economic costs. What are the costs exactly?

Christensen et al (2013) evaluated the impact of EU's GDPR proposal on SMEs and concluded that SMEs that use data rather intensively are likely to incur substantial costs in complying with these new rules. The authors compute this result using a simulated stochastic general equilibrium model and show that in the baseline scenario, close to 200,000 jobs could disappear in the short-run and more than 300,000 in the long run.

By analyzing proposed or enacted data localization rules in seven economies, Bauer et al (2014) found that they lowered GDP in all cases by between 0.1 and 1.7 percent. In terms of overall domestic investments, the model estimated a fall of between 0.5 and 4.2 percent.

In a 2016 Center for International Governance Innovation (CIGI) and Chatham House study which used an index to proxy for data-related administrative regulations in each economy, Bauer et al showed that restrictive data regulations, including data localization, increase prices and decrease productivity across a range of economies. Specifically, a one standard deviation change in the index would decrease total factor productivity and increase price by 3.9 and 5.3 percent, respectively on average.

Ferracane and van der Marel (2018) showed that strict data policies negatively and significantly impacted imports of data-intensive services. Therefore, economies applying restrictive data policies, particularly with respect to the cross-border flow of data, suffer from lower levels of services traded over the internet. The negative impact is stronger for economies with better developed digital networks. In another paper which used firm-level and industry-level data across economies, Ferracane et al (2018) also showed that stricter data policies have a negative and significant impact on the performance of downstream firms in sectors reliant on electronic data (i.e. sectors that rely more on data in their production process). The adverse effect is stronger for economies with strong technology networks and for servicified firms.

Source: Christensen et al (2013); Bauer et al (2014, 2016); Ferracane and van der Marel (2018); Ferracane et al (2018).

2.4. Are there middle-ground approaches to some of the data-related regulations?

Questions on whether there are middle-ground approaches to data-related regulations have been brought to the fore. In this report, middle-ground means regulations that have relatively minimal impact on firms' use of data (including across borders) and at the same time, support the public policy objectives of ensuring data protection and security as well as addressing domestic security among others. Literature review points out to the availability/presence of several non-mutually exclusive approaches. This section summarizes some of these approaches.

Recognizing the adoption of industrial standards

Firms shared that industrial standards provide the baseline requirements pertaining to areas such as privacy and security protocols, policies and rules and are usually consistent with data protection legislation in individual APEC economies governing data flows and its use in business to business

(B2B) and business to consumer (B2C) activities[34]. Indeed, some interviewed firms highlighted that adhering to such standards is one way to build trust regarding data management in their businesses.

International Organization for Standardization (ISO) certifications are examples of such standards. ISO/IEC27001 (or ISO27001) is the best-known standard in the family of ISO/IEC27000, with 2013 being the latest version. The standard helps organizations of all sizes and in all sectors to keep their information assets secure. It certifies the entire information security management systems (ISMS) of an organization, which includes people, processes and IT systems ("ISO/IEC27001 Information Security Management" n.d.). The detailed requirements that ISMS must fulfil in order to be certified can be found in sections 4 to 10 of the standard and encompasses areas such as leadership, planning, and performance evaluation.

Furthermore, the standard includes 14 security control clauses, 35 control objectives and 114 security controls. As an illustration, some of the 14 security control clauses that an organization must meet include: asset management, access control, cryptography, physical and environmental security, information security incident management, and information security in business continuity management. According to the 2017 data retrieved from ISO, five APEC economies are among the top 20 economies with the highest number of certified firms, collectively making up close to half of the certified firms.

Another example of a voluntary standard is the BS10012. It was developed by the British Standards Institution (BSI) in the United Kingdom as a best-practice framework for personal information management systems (PIMS). It is aligned with the principles of the EU General Data Protection Regulation (GDPR) by outlining core requirements that organizations need to consider when collecting, storing, processing, retaining or disposing of personal records related to individuals (BSI Group n.d., 100). BS10012:2017 is the latest version and includes among others, new definitions of what is personal and sensitive data, privacy by design, administrative requirements for Data Protection Officers; coverage of pseudonymized data, right to erasure, and security breach notification requirements (Muncaster 2017).

Enhancing domestic data-related regulations

Domestic data-related regulations play an important role in ensuring data protection and security because the Westphalian system that the world runs on puts major responsibility of enforcement on individual economies. However, as the earlier section has shown, there are numerous data-related regulations that may not be ideal for data-utilizing businesses. Therefore, the key is to come up with optimum regulations that meet the public policy objectives while not inhibiting the operations of data-utilizing businesses.

Privacy guidelines

One way to ensure that regulations do not go beyond their original remit of protecting data is to review potential and existing regulations against privacy guidelines/framework. An example is the OECD Privacy Framework, which is composed of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD, 2013).

Kuner (2013, 36-36) remarked that the OECD Guidelines is a non-binding instrument that economies may adopt with a double aim: on the one hand, achieving minimum standards for privacy and personal data protection, and on the other hand, reducing factors which might induce economies to restrict cross

[34] See Chapter 2

border data flows. These minimum standards are reflected in the basic principles contained in the OECD Guidelines, which are: the collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. The OECD Guidelines embody the widest consensus (in global terms) on what constitutes as best practices in the areas of data protection and transborder data flow regulation.

Similarly, the APEC Privacy Framework (APEC 2015) is composed of information privacy principles which are in line with the revised version of the OECD Guidelines from 2013. The nine information privacy principles covered are: accountability; notice; choice; collection limitation; integrity of personal information; uses of personal information; security safeguards; access and correction; and preventing harm. Those principles form a baseline of privacy protection but can be supersede in domestic legislation. Furthermore, the APEC Privacy Framework contains guidelines for domestic and international implementation. In the case of domestic implementation, APEC economies are encouraged to consider, amongst others, the establishment of privacy enforcement authorities and privacy management programs; the promotion of technical measures to protect privacy and the availability of appropriate remedies privacy breaches.

Besides ensuring that regulations do not go beyond their original remit, the fact that these privacy guidelines are formulated with the participation of many economies means that they can serve as starting points to promote regulatory alignment and cross-border data flows as well (more details below).

Complement lighter touch regulations with effective enforcement

Instead of putting in place strict regulations pertaining to data storage, processing and access, an alternative would be to implement regulations which are relatively lighter touch in nature but complemented with strong and effective enforcement if organizations and firms fail to ensure data protection and security. With regards to trends on domestic enforcement actions, the United Nations Conference on Trade and Development (UNCTAD 2016, xvii) indeed noted that "strong support exists for establishing a single central regulator when possible, with a combination of oversight and complaints management functions and powers. Moreover, the trend is towards broadening enforcement powers, as well as increasing the size and range of fines and sanctions in data protection".

Furthermore, the same report (UNCTAD 2016, 15) explained that "strengthening enforcement powers has been a major theme in amending and updating laws (notably in the Australia; the EU; Hong Kong, China; and Japan)." The use of fines as a mechanism for deterrence is deemed to be an effective way to enforce data privacy laws. On this aspect, the United States was indicated to have used massive fines and sanctions to deter privacy malpractice (UNCTAD 2016, 15). In other jurisdictions such as the EU, strong fines are also seen as a key factor to assure data privacy compliance. For instance, Google LLC was recently fined 50 million euros for GDPR violation by the French National Data Protection Commission (CNIL 2019).

Another example pertains to Korea's Personal Information Protection Act (enacted September 30, 2011). Despite not mandating general localization requirements except for certain types of data such as financial and medical data, it is considered among some of the world's strictest privacy regimes because its enforcement mechanism includes civil and administrative, as well as criminal sanctions. Typically, transfer of data abroad can occur after the data subjects' consent (Practical Law, n.d.).

While enforcement at the domestic level can be achieved through increased fines, it remains debatable if cross-border enforcement can work effectively. For this reason, it is important to ensure cooperation among data protection authorities, and the APEC Cross-border Privacy Enforcement Arrangement (CPEA) is a good practice in this regard.

Enhance cross-border data flows through various mechanisms

Adequacy status

Effective data protection and security does not necessitate strict bans on storage, processing and access. For instance, the GDPR streamlines cross-border data transfers when the other economy is accorded with an adequacy status (i.e. when two domestic regimes are deemed equivalent and no further regulatory approvals are needed, unlike binding corporate rules and codes of conduct as described below)[35], although it should be acknowledged that an adequacy status is hard to obtain. At the moment the EU Commission has conferred the adequacy status for a small group of economies outside the EU.[36] If an economy would like to qualify for an adequacy status, it should meet at least three factors, namely[37]:

- Existence of the rule of law, respect for human rights and fundamental freedom, existence of relevant legislation (including legislation for access of public authorities to personal data), data protection rules, enforceable and effective data subject rights, administrative and judicial redress, amongst others;
- Existence and effective functioning of data protection authorities (DPAs); and
- International commitments and other obligations in relation to the protection of personal data.

In practice, the conferment of adequacy status could also entail the analysis of other factors. Mattoo and Meltzer (2018, 9) observed that "equivalence relates not only to the level of data protection but also to whether the access of government agencies to personal data and data subjects' rights of redress are consistent with the GDPR". In the APEC region, transfers based on adequacy decisions are also an aspect found in Japan's Amended Act on Protection of Personal Information (Alston and Bird, n.d.) and the Privacy Shield between the United States and the EU.

Binding Corporate Rules (BCRs), Standard Contractual Clauses (SCCs) and Codes of Conduct

Besides adequacy decisions, other mechanisms employed by the GDPR to facilitate cross-border data flows include through Binding Corporate Rules (BCRs), Standard Contractual Clauses (SCCs) and Codes of Conduct. BCRs are approved business-specific frameworks that allow intra-organizational cross-border transfers of data from organizations within the EU to their affiliates outside of the EU and are regulated in detail in Article 47 of the GDPR as well as by WP 256 Rev.01 (Article 29 Data Protection Working Party 2018).

On the other hand, SCCs are model contracts designed and pre-approved (i.e. there is no need for further prior authorization) by the European Commission. They allow the export of personal data to third economies.[38] Non-EU firms can sign SCCs to receive data from the EU. However, the validity of SCCs

---

[35] See GDPR Articles 44-49. Under the GDPR, as a general rule, transfers of personal data to a third economy outside the EU can take place only based on: (i) adequacy decisions granted by the European Commission to a third economy or an international organization (e.g., privacy shield), which has the advantage of not having to obtain any further authorization in order to transfer data abroad; or (ii) appropriate safeguards, including, standard contractual clauses, binding corporate rules, approved codes of conduct, and approved certification mechanisms. If the above are not available, transfers can be based on the following derogations: explicit consent, contractual necessity, important public interest reasons, litigation necessity, vital interests, public register data and legitimate interest of the controller.

[36] Those are: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the United States. Japan has also recently been recognized as ensuring an adequate level of protection of personal data pursuant to Article 45 of the GDPR (https://ec.europa.eu/info/sites/info/files/draft_adequacy_decision.pdf)

[37] GDPR Article 45 paragraph 2

[38] ("Model Contracts for the Transfer of Personal Data to Third Countries" n.d.)

is currently being debated in an ongoing legal case brought by Maximillian Schrems for considering that SCCs do not adequately protect the data of EU individuals against government surveillance (Schrems II[39]).

Finally, Codes of Conduct are proposed by associations or representative bodies of a specific industry in relation to data processing activities. They must include information about how the code meets GDPR standards not only with regard to the collection and processing of personal data, but also transfers to third economies and how individuals can pursue their rights. Codes of Conduct require regulatory approval either by the domestic data protection authority or by the European Commission (GDPR Article 40).

While all the above instruments are formulated to facilitate cross-border transfers of personal data, they differ in that they are designed to cater to different data controllers and processors. For instance, BCRs might be of more benefit to large firms intending to carry out intra-group data transfers, while SCCs and Codes of Conduct might work better for small organizations with less complex personal data processing (Allen & Overy 2016).

Mutual recognition system

Yet, even when flexibilities for cross border transfers are built within domestic privacy laws (e.g. in the form of adequacy decisions, BCRs, SCCs and Codes of Conduct), the difference in specific requirements among domestic privacy laws can entail significant costs to firms. In fact, a specific aspect raised during the interviews was the increase in the level of spending in order to comply with the different regulations of different economies. This issue is known as "bracket creep regulation", whereby different compliance hurdles duplicate or increase compliance costs for firms[40].

One mechanism to avoid this is through some form of mutual recognition, whereby a firm fulfilling the data privacy regulations of one economy is regarded as meeting those of other economies which are part of the mutual recognition system. The APEC Cross Border Privacy Rules (CBPR) system is one such system. Essentially, it is a voluntary certification scheme that allows companies to transfer personal data (inter and intra company) across APEC members taking part in the system (Box 3). Moreover, the CBPR does not interfere with the ability of an economy to impose higher data privacy standards.

Despite the benefits that the CBPR system offers, however, only a handful of firms interviewed for this study were aware of its existence. Moreover, awareness does not always mean participating in the system. In the case of Japan, only three firms had applied and been certified although JIPDEC, the Japanese-based CBPR accountability agent, had conducted numerous promotional activities about it, some of which are targeted towards firms which had been pre-identified as potentially qualified to be certified. Reasons for the low participation can include the limited number of economies currently participating in the CBPR and firms not encountering much issues transferring data between these economies. Expansion of CBPR to cover more APEC economies and promoting interoperability between CBPR and other systems such as the GDPR are suggested as possible ways to enhance the uptake of CBPR by firms.

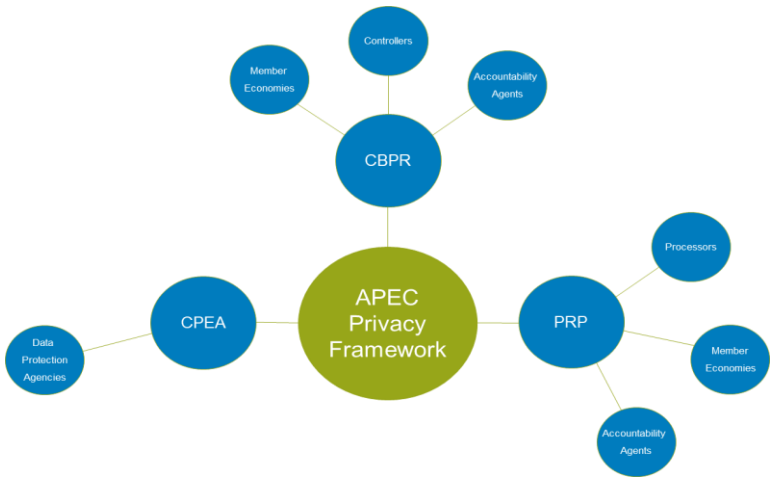
[39] 'Case C-498/16, Maximilian Schrems v Facebook Ireland Limited, (ongoing)'.
[40] See Chapter 2

Box 3. How Does APEC CBPR System Work?

The CBPR system is a voluntary certification scheme that allows companies to transfer personal data (inter and intra company) among APEC economies taking part in the initiative. Currently, these economies are Australia; Canada; Japan; Korea; Mexico; Singapore; Chinese Taipei and the United States. As APEC is composed of highly diverse members, the CBPR is designed to be a very pragmatic instrument and does not interfere with the ability of an economy to impose higher data privacy standards. It is perhaps one good example of how global interoperability of privacy regimes based on minimum standards can be promoted. As more member economies and companies join the system, the CBPR could well become an effective mechanism for privacy protection that works towards the avoidance of barriers to information flow, and ensures continuous trade and economic growth.

The CBPR applies to the controllers of personal information (i.e. information about an identified or identifiable individual) and is composed of four phases: self-assessment; compliance review; recognition/acceptance; and dispute resolution and enforcement. Under the first phase, applicant firms (from any of the eight economies taking part in the system) self-assess their compliance with the nine information privacy principles indicated in the APEC Privacy Framework (i.e. accountability; notice; choice; collection limitation; integrity of personal information; uses of personal information; security safeguards; access and correction; and preventing harm). Following that, they submit an intake questionnaire to one of the CBPR accountability agents (TRUSTe or JIPDEC). Under the second phase, the accountability agent reviews firms' compliance with the information privacy principles. Compliant firms are then issued with certificates and added to the compliance directory under the third phase. Finally, under the last phase, dispute resolution and enforcement are undertaken by the corresponding domestic privacy enforcement authority and the accountability agent.

The CBPR is complemented by the Privacy Recognition for Processes (PRP) system and the APEC Cross-border Privacy Enforcement Arrangement (CPEA). The latter is a multilateral arrangement that provides the first mechanism in the APEC region for privacy enforcement authorities to voluntarily share information and provide assistance for cross-border data privacy enforcement. The ecosystem of the CBPR system is as follows:



Source: Authors' own elaboration

Free Trade Agreements

Free Trade Agreements (FTAs) have emerged as another venue where frameworks for cross-border data transfers between economies could be agreed upon. While the first FTA with an electronic commerce provision was the Jordan-the United States FTA in 2000, the first FTA which included data flow related provisions was the Korea-United States FTA in 2007. For this reason, Elsig and Klotz (2018, 1) argued that these types of provisions are a rather recent phenomenon in trade agreements.

FTA provisions containing rules pertaining to ICT, big data, and data localization requirements among others are usually found in electronic commerce, services, and intellectual property chapters (Elsig and Klotz 2018, 3). Recent research points to leading rule makers in this area, namely Australia; Canada; the EU; Singapore; and the United States. Of the recent FTAs, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the United States-Mexico-Canada Agreement (USMCA) stand out for containing specific rules on cross-border data flows.[41] Box 4 elaborates on what some of these specific rules in the CPTPP are. Furthermore, Article 19.8 of the USMCA on Personal Information Protection recognizes the APEC CBPR System as a mechanism to facilitate cross-border data flows[42].

Box 4. Selected rules for data driven business contained in the CPTPP

The CPTPP (in force since December 20, 2018) is currently made up of 11 signatories, all of which are APEC economies (Australia; Brunei Darussalam; Canada; Chile; Japan; Malaysia; Mexico; New Zealand; Peru; Singapore; and Viet Nam). The Agreement includes innovative rules for contemporary digital trade scattered across different chapters. In light of the current uses of data, the most salient ones are:

In the e-commerce chapter (Chapter 14):

- Rules for the adoption or maintenance of legal frameworks for: (a) *online consumer protection* (Article 14.7); and (b) the *protection of personal information*. With regard to the latter, this can be composed of comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy. Furthermore, an economy Party to the CPTPP should publish how individuals can pursue remedies and how business can comply with any legal requirements. The CPTPP also encourages the development of mechanisms to promote compatibility between these different domestic privacy regimes, including recognition of regulatory outcomes or broader international frameworks (Article 14.8).
- Rules that allow the *cross-border transfer of information*, including personal information, by electronic means when such activity is for the conduct of business. Yet, Parties to the CPTPP are not prevented to adopt incompatible measures in order to achieve legitimate public policy objectives, to the extent that these measures are not discriminatory (Article 14.11).
- Rules prohibiting: (a) *localization requirements of computing facilities* as a condition for conducting business in that territory (14.13); (b) the *disclosure of source codes* as a condition for the import, distribution, sale or use of mass-market software (Article 14.17); and (c) *customs duties* on electronic transmissions (Article 14.3).
- Rules on cooperation on cybersecurity matters (Article 14.16).

[41] See CPTPP Article 14.11(2) and USMCA Article 19.11(1).
[42] See USMCA Article 19.8 (6).

In the intellectual property chapter (Chapter 18):

- Rules for the adoption of *criminal procedures and penalties for cyber theft* of trade secrets (unauthorized access to a trade secret held in a computer system, unauthorized and wilful misappropriation of a trade secret, including by means of a computer system; or fraudulent disclosure, or the unauthorized and wilful disclosure, of a trade secret, including by means of a computer system (Article 18.78).
- Rules for the adoption of laws and regulations providing that central government agencies use only *non-infringing computer software* (Article 18.80).

In the technical barriers to trade (Chapter 8):

- The prohibition to require technology transfer or access to proprietary information as a condition to manufacture, sale, distribute, import or use a product using *cryptography* (Annex 8-B, Section A-3).

In the financial services chapter (Chapter 11):

- The obligation to allow the cross-border supply of electronic payment services (i.e. processing infrastructure can be located off-shore) subject to certain conditions (such as registration with the relevant authorities). Measures adopted to protect personal data are allowed (Annex 11-B, Section D).

Source: Author's own elaboration

Multilateral rules

Mattoo and Meltzer (2018, 16) noted that the World Trade Organization (WTO) rules that can facilitate data flows are contained in the General Agreement on Trade in Services (GATS). In terms of *coverage*, GATS relevant commitments relating to digital services are CPC 843 for 'computer and related services', and CPC 844 for 'Data Base Services' which includes online processing services.

Yet, there is still uncertainty about the extent to which new digital services such as search engines and cloud computing are covered by existing GATS commitments. In terms of *substantive disciplines* such as Most-Favored-Nation Treatment (Article II), National Treatment (Article XVII) and Market Access (Article XVI)), Mattoo and Meltzer (2018, 17) pointed out that most WTO members have chosen to be relatively open in areas like computer services. For instance, among other economies, the EU has commitments on computer related services and database services where there are no restrictions on market access or national treatment. Nonetheless, the openness in those sectors is still subject to the exceptions contained in GATS itself. With regard to measures related to personal data, relevant GATS exceptions are the protection of privacy (Article XIV), and the exceptions for measures that members consider necessary for the protection of their domestic security (Article XIV bis).[43]

[43] See (OECD 2018, 2)

Box 5. Blockchain as technological solutions to address privacy

As have been indicated earlier, encryption is one technological solution to keep data private and safe. Besides encryption, other solutions such as blockchain have emerged, yet it is still unclear how some of these approaches may fit current privacy laws and regulations. Specifically on blockchain, Fink (2018, 4) explained that the way this technology works is by grouping data "into blocks that, upon reaching a certain size, are chained to the existing ledger through a hashing process. Through this process, data is chronologically ordered in a manner that makes it difficult to tamper with information without altering subsequent blocks".

In certain industries, blockchain can be used for data management purposes. Cheng et al. (2017) pointed out that "banks, payment-service providers, and insurance companies have shown the highest level of interest and investment in blockchain." One interviewed firm based in Chile uses blockchain to grant every invoice its own unique fingerprint and is planning to launch its services in several Latin American economies including Mexico; Colombia; Peru; and Brazil.

Moreover, blockchain transactions are anonymous. As anonymity and pseudonymity of personal data are some of the requirements of current data protection laws, blockchain could serve to achieve this purpose. As Kuner (2018, 14) points out: "*Widespread distribution of copies of the ledger, together with a consensus process that does not require any centralized, trusted, intermediary to manage the ledger, make Bitcoin and similar DLTs (distributed ledger technologies) attractive as platforms for use by large numbers of parties who do not trust, indeed may not even be able to identify, each other*."

However, other aspects of distributed ledger technologies can encounter difficulties in light of current privacy laws. Namely, Fink (2018, 6-7) pointed out that while privacy laws have been developed for centralized collection and processing of data (and therefore, depend on responsibilities assigned to controllers and processors), blockchain technologies work in a decentralized fashion for the collection, storing and processing of personal data. Indeed, while the current data economy largely depend on intermediaries that collect, control, process and monetize personal data, the promise of distributed ledger technologies is the decentralization of this process or what is often called "data sovereignty", implying "giving individuals control over their personal data and allowing them to share such information only with trusted parties." This represents a challenge especially for blockchains that are public and do not require consent.

Despite these legal uncertainties, patents using blockchain as a mechanism to tackle privacy are already being filed. This is the case for IBM, which filed a patent in the US Patent and Trademark Office detailing how distributed ledger technologies could be used to store data associated with drones flights paths.

Source: various

Enhance domestic security through various mechanisms

Reform mutual legal assistance treaties (MLAT)

An often cited reason for requiring servers to be located within an economy is to facilitate data access swiftly in the context of criminal investigations. As communications are mostly undertaken online, criminal investigations benefit from accessing communication, location and other types of data in a speedy fashion. These types of data constitute evidence to investigate and prosecute crimes more effectively.

However, data related to those investigations can be stored in servers around the world and access to it is typically facilitated by mutual legal assistance among jurisdictions. The legal grounds that enable this cooperation are bilateral, multilateral or regional mutual legal assistance treaties (MLATs), which are agreements between governments whose purpose is to ease the exchange of information relevant to an investigation happening in at least one economy involved.

Yet, MLATs predate the internet era and their functioning have been challenged by the explosion of digital communications, one of which is to reconcile data privacy protection versus law enforcement's need for evidence (Force Hill 2015). As a consequence of these legal uncertainties, the function of the MLAT system today is limited. Force Hill (2015) noted that "responses to MLAT requests for information are often abysmally slow; many of the requests are denied or only partially satisfied due to confusion over the rules governing data." Furthermore, Kent (2015) points out that domestic legislation can require the duplication of paperwork or even that communication between governments agencies involved should be via the traditional postal service.

A reasonable option would be to reform the MLAT system to allow for speedy cooperation on data access request for law enforcement. For instance, the Council of Europe has put on the table an annex to the Budapest Convention on Cybercrime, which increases and simplifies cross-border access to data for law enforcement.

Bilateral and multilateral data sharing

Besides reforming MLATs to facilitate quicker access to data where the need arises, economies have also negotiated data sharing agreements with each other for reasons such as enhancing cybersecurity cooperation and curbing tax evasion. For example, a two-year Memorandum of Understanding (MoU) was signed between Canada and Singapore in November 2018 and will cover cybersecurity cooperation in areas such as information exchange and sharing on cyber-threats and cyber-attacks. Indonesia and Singapore established an Automatic Exchange of Financial Account Information (AEOI) which would allow the two economies to exchange information on their taxpayers' bank accounts, revenues and account balances. The first exchange commenced in September 2018.

The U.S. Department of Justice released a draft legislation in July 2016 which was aimed to support cross-border data access through the use of bilateral agreements between the United States and participating economies. Basically, economies approved for these bilateral agreements can directly submit data requests to the U.S. electronic service providers instead of going through the U.S. courts first. It is believed that the new legislation could avert some economies from enacting requirements such as data localization among others. Lin and Fidler (2017) indicated that the United Kingdom is likely to be the first economy approved under the new legislation if advanced.

Unilateral approaches

Recognizing that focus should be on mandating access to data instead of where they are located, several economies have amended their regulations unilaterally. For example, Denmark changed its local data storage requirement for accounting data in 2015. With the change, firms are allowed to store their data anywhere so long as authorities are provided easy access to the data on request.

Concerned with their past experiences in accessing data of key banks during bankruptcy proceedings following the global financial crisis, legal reforms such as those enacted in the Dodd-Frank Act in 2010 require firms to disclose the way IT and data are managed to regulators as part of their regular prudential compliance activities. Specifically, extensive new rules require firms categorized as systemically important financial institutions (SIFIs) to prepare living wills, which elucidate firms' strategy pertaining to rapid and orderly resolution in the event of financial distress or failure. Part of the living wills include meeting stringent requirements about how data is stored, accessed and managed on an ongoing basis in the event of a crisis. Similarly, the focus of these regulations is on ensuring data access.

3. Challenges across organizations

3.1. Factors restricting data sharing

Data-related issues, in particular data sharing are not confined only to between economies, but also between organizations. Despite being an important factor for unlocking innovation and realizing the potentials of digital economy, the practice of legitimate data sharing is not ubiquitous for various factors:

Data privacy regulations

A study undertaken by the Competition Commission of Singapore (2017, 9) reveals that despite the benefits to share data across organizations, firms are generally not keen to share data with external parties because there is a need to comply with the relevant data protection regulations. Firms are also wary that their revenue may be affected due to the loss of customer trust should they discover that their information have been shared without consent. Similarly, a study undertaken by the European Commission (Scaria et al 2018, 44) found that firms also cite privacy concerns as a reason for not sharing data with other firms. This evidently represents a challenge for seizing the benefits of big data, especially when these concerns find legitimate grounds in prominent personal data breaches. Moreover, the challenges to share data across organizations can increase in cases of sensitive data, especially those pertaining to financial and/or health data.

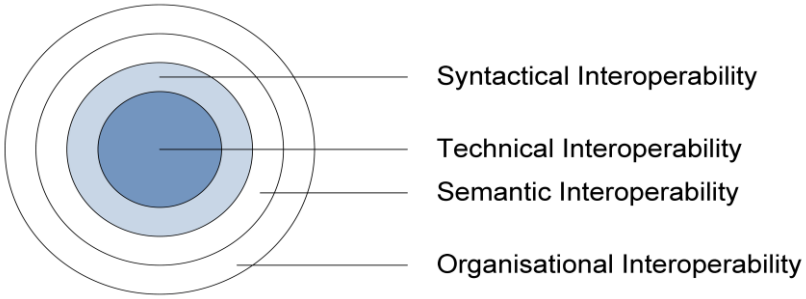
Anticompetitive behavior

Firms collect and aggregate large amounts of data coming from various sources (e.g. smart devices, social media, among others). Moreover, the increased adoption of the Internet of the Things (IoT) have led to an exponential increase in the collection of both personal and industrial data. In order to achieve or maintain dominance in a given market, firms may resort to anticompetitive behavior such as refusing to grant access to data, providing discriminatory access to data and using data as a tool for price discrimination. Indeed, the Competition Commission of Singapore (2017, 9) reported that some firms viewed data as a source of competitive advantage which would be lost if shared. Japan's Fair Trade Commission (2017) has also reflected on the issues of monopolization and oligopolization of digital platforms and suggested that competition law legislation should be reviewed to promote the entry of new firms to the market.

Lack of interoperability of data formats and standards

Data collected by organizations emanates from a variety of sources and hence have heterogeneous data formats. This leads to the high cost of managing, integrating and mining such data. At the same time, proprietary standards and protocols make data sharing and interoperability between devices and platforms challenging. van der Veer and Wiles (2008) identified at least four layers that are required to achieve full interoperability (Figure 4).

Figure 4. Four layers of interoperability



Source: van der Veer and Wiles (2008, 6)

At the core is technical interoperability which refers to adequate transmission of bits (e.g. internet protocols TCP/IP). Syntactic interoperability comes next and refers to data formats for packaging and transmission that allow the recipients to understand what those bits represent (e.g. HTML, XML, ASN, among others). Semantic interoperability is the layer where data can be processed together with other data and be transformed into information. For example, ISBN code for books represent the type of standards corresponding to this layer. Finally, organizational interoperability is the layer where users or firms can communicate and conduct activities seamlessly within each other.

As these layers built upon each other, lack of standardization or insufficient open standards at each layer reduces the chances of achieving full interoperability. This affects not only the prospects of data sharing across organizations, but also the outlook for IoT[44] and initiatives such as the reuse of public sector information.

3.2. Facilitating data sharing across organizations

From the discussions above, it can be surmised that factors inhibiting increased data sharing among organizations entail both valid as well as questionable ones. Listed below are some approaches to facilitate data sharing but without compromising on the valid factors such as adherence to legitimate data privacy regulations.

Introducing open data policies and initiatives

As the custodian of large amount of public data, governments can be a trailblazer and play an active role in promoting legitimate data sharing. OECD (2018b) noted that governments can promote business creation and innovative, citizen-centric services by encouraging the use, reuse and free distribution of datasets. Einav and Levin (2013, 9) went further by indicating that administrative data is a powerful resource for a number of reasons including high quality data and coverage of individuals or entities over time, hence creating a panel structure. In addition, the universal coverage means that administrative datasets can be linked to other potentially more selective data.

One way to do so would be via open data policies and initiatives. Open data refers to publicly available data which is structured to be fully discoverable and usable by end users. Open data policies in many economies evolve from a broader open data movement and are based mainly on eight principles, that is, data should be complete, primary, timely, accessible, machine-processable, non-discriminatory, non-

[44] In the IoT context, machine-to-machine communications will be the basis for smart devices, houses, cars, and cities, etc.

proprietary and license-free. The Open Government Data Act in the United States essentially requires government data assets made available by federal agencies to be published as machine-readable data.

The Open Government Partnership (OGP) is one of the many open data initiatives around the world where participating economies pledge access to government information. To date, participating APEC economies include Canada; Chile; Indonesia; Korea; Mexico; New Zealand; Peru; the Philippines; and the United States.

Promoting data commons

Data commons is another non-discriminatory access regimes that can be used to promote data sharing. Grossman (2016, 11) explained that data commons is frequently associated with science and research and has been conceptualized as "cyberinfrastructure that collocates data, storage, and computing infrastructure with commonly used tools for analyzing and sharing data to create an interoperable resource for the research community." Some of the latest applications of this framework are found in the medical field (e.g. NCI Genomic Data Commons, BRAIN Commons, BloodPAC Data Commons).

Developing data sharing standards

Standards for data sharing and reuse in the big data and IoT context are being developed by various standardization bodies (e.g. ITU, ISO) and similar organizations (e.g. World Wide Web Consortium). A comprehensive mapping is necessary in order to identify areas with insufficient standardization. The Big Data Standardization Roadmap released by ITU in 2016 is a good starting point in this direction. The document covers standardization landscape for big data in different organizations, identification and prioritization of technical areas as well as possible standardization activities. Table 3 provides an illustration of the current standards identified by ITU as relevant for big data. For instance, an area identified as lacking in technical standardization is Application Programing Interfaces (APIs) which are mostly being developed by open source projects.

Table 3. Standardization matrix of big data

	General/ definition	**Common requirement/ use case**	**Architecture**	**API, interface and its profile**	**Data model, format, schema**	**Others (e.g., guideline)**
Fundamental	ITU-T Y.3600 ISO/IEC 20546 ISO/IEC 20547-1	ITU-T Y.3600	ITU-T Y.BDaaS-arch ISO/IEC 20547-3			
Data exchange	ITU-T Y.BigDataEX-reqts	ITU-T Y.BigDataEX-reqts			OASIS AMQP 1.0 OASIS MQTT 3.1.1	
Data integration					W3C DCAT W3C JSON-LD 1.0 W3C LDP 1.0 W3C RDF 1.1 W3C OO	
Analysis /Visualization					DMG PMML 4.2.1	TMF BDAG
Data Provenance /Metadata	ITU-T Y.bdp-reats	ITU-T Y.bdp-reats			W3C MVTD W3C MTDMW	
Security /Privacy	ITU-T X.1601 ISO/IEC 27000	ISO/IEC 20547-4			ISO/IEC 27002 ISO/IEC 27018	ITU-T X.CSCDataSec ISO/IEC 27001

	IEO/IEC 29100					
Others	ITU-T Y.bDPI-Mec ITU-T Y.bDDN-fr	ITU-T Y.IoT-BigData-reqts ITU-T Y.dsf-reqts ITU-T Y.bDDN-req ISO/IEC 20547-2	ITU-T Y.SDN-ARCH			ISO/IEC 19944 ISO/IEC 20547-5

Source: ITU (2016)

It is also important to promote regulatory cooperation in standard setting as well as to take into account the views of different public and private stakeholders. Besides conferring legitimacy and ensuring wider adoption of the standards, trust in the standards can be further enhanced.

Developing data sharing guidelines

Data protection authorities (DPAs) can serve an important role in encouraging data sharing and reuse. As enforcer of data privacy regulations of their economies, DPAs are well-placed to provide guidance on what constitutes as legitimate data sharing procedures without compromising on the need to ensure that data remains protected and secured. For example, Singapore's Personal Data Protection Commission (PDPC) recently released a guide on data sharing[45].

4. Conclusion and way forward

This report has shown the critical role of data in both traditional and new businesses. Moreover, freer flow of data across economies and organizations are imperative in order to optimally realize the benefits of digital economy. However, for various legitimate public policy objectives such as ensuring data protection and security as well as enhancing domestic security, some contemporary regulations have inadvertently led to sub-optimal flows of data and consequently, with negative implications on innovation and growth.

Alternative, middle-ground approaches to data-related issues (i.e. with relatively minimal impact on firms' access and use of data and at the same time, fulfill legitimate public policy objectives) are available. With regards to challenges to freer data flow across economies, these approaches include recognizing voluntary standards, reviewing potential and existing domestic regulations against privacy guidelines/framework, complementing lighter touch regulations with effective enforcement, and enhancing cross-border data flows through various mechanisms such as adequacy status, mutual recognition system and free trade agreements among others. On challenges to data sharing among organizations, approaches include introducing open data policies, promoting data commons, developing data sharing standards as well as guidelines.

Despite these approaches being steps in the right direction, this report has also shown that some of them are not silver bullets at least in their current form and can be further improved in one way or another. For example, although the APEC CBPR system represents one way to enhance cross-border data flows, its effectiveness is very much dependent on the number of participating economies and awareness among firms on its existence. The multilateral approach to data flow facilitation represents the first best

[45] "Guide to Data Sharing" (Personal Data Protection Commission of Singapore, February 2018), https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Data-Sharing-revised-26-Feb-2018.pdf

option but uncertainty about the extent of coverage of existing GATS commitments persists, particularly with regards to new digital services such as cloud computing.

APEC can build on the insights from the study and contribute to the endeavor of improving data-related regulations among its members by:

- Facilitating information and experience sharing/exchange on these middle-ground approaches. These can include how to operationalize these approaches, how to monitor and evaluate their impacts as well as how they can be further improved in terms of implementation and awareness among others.

- Organizing dialogue sessions to identify ideas and ways to overcome bottlenecks that have led to standstill or little progress in some middle-ground approaches such as those pertaining to regulatory alignment, multilateral rules on data flow facilitation and reform of mutual legal assistance treaties.

- Developing capacity-building activities to assist member economies in enhancing and improving on their existing data-related and complementary regulations including those pertaining to IPR protection. These can include workshops and technical training assistance on establishment of competent data protection authorities and on enhancing cross-border enforcement among others.

References

1. Allen & Overy .2016. "Binding Corporate Rules" http://www.allenovery.com/SiteCollectionDocuments/BCRs.pdf
2. Alston & Bird. n.d. "May 30 Is Fast Approaching – Are You Ready for Compliance with the Amended Act on Protection of Personal Information in Japan?" Alston & Bird Privacy Blog. https://www.alstonprivacy.com/may-30-fast-approaching-ready-compliance-amended-act-protection-personal-information-japan/.
3. Article 29 Data Protection Working Party. 2018. "Working Document Setting up a Table with the Elements and Principles to Be Found in Binding Corporate Rules (WP 256 Rev.01)." http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109.
4. Australia. 2012. *Personally Controlled Electronic Health Records Act 2012*. https://www.legislation.gov.au/Details/C2012A00063
5. Bauer, M., Lee-Makiyama, H., van der Marel, E., and Verschelde, B. 2014. "The Costs of Data Localization: Friendly Fire on Economic Recovery." ECIPE Occasional Paper No. 3/2014. https://ecipe.org/wp-content/uploads/2014/12/OCC32014__1.pdf
6. Bauer, M., Ferracane, M.F., and van der Marel, E. 2016. "Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization." Global Commission on Internet Governance (CIGI) and Chatham House Paper Series No. 30. May 2016. https://www.cigionline.org/sites/default/files/gcig_no30web_2.pdf
7. Bsi Group. n.d. "BS 10012 Personal Information Management." Accessed December 28, 2018. https://www.bsigroup.com/en-GB/BS-10012-Personal-information-management/.
8. Bundeskartellamt. 2016. Big Data and Competition Law. http://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf;jsessionid=B433476372FD2F7A43EF4F482255113D.1_cid387?__blob=publicationFile&v=2.
9. Bughin, J., Hazan, E., Ramaswamy, S., Chui, M., Allas, T., Dahlström, P., Henke, N., and Trench, M. 2017. "Artificial Intelligence: The Next Digital Frontier." McKinsey Global

Institute. https://www.mckinsey.com/~/media/McKinsey/Industries/Advanced%20Electronics/Our%20Insights/How%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/MGI-Artificial-Intelligence-Discussion-paper.ashx

10. Castro, D., and McQuinn. A. 2015. "Cross-Border Data Flows Enable Growth in All Industries." Information Technology & Innovation Foundation. http://www2.itif.org/2015-cross-border-data-flows.pdf
11. Cheng, Steve, Matthias Daub, Axel Domeyer, and Martin Lundqvist. 2017. "Using Blockchain to Improve Data Management in the Public Sector." McKinsey & Company. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector.
12. China. 2016. *Cyber Security Law of the People's Republic of China*. http://www.miit.gov.cn/n1146295/n1146557/n1146614/c5345009/content.html
13. Christensen, L., Colciago, A., Etro, F., and Rafert, G. 2013. "The Impact of the Data Protection Regulation in the EU." http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.657.138&rep=rep1&type=pdf
14. Cisco. 2018. Cisco Virtual Networking Index: Forecast and Trends, 2017-2022. San Jose: Cisco. https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.pdf
15. CNIL. 2019. "The CNIL's Restricted Committee Imposes a Financial Penalty of 50 Million Euros Against GOOGLE LLC." https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.
16. Competition Commission of Singapore. 2017. Data: Engine for Growth - Implications for Competition Law, Personal Data Protection, and Intellectual Property Rights. Occasional Papers.
17. Cory, N. 2017. "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" Information Technology & Innovation Foundation. http://www2.itif.org/2017-cross-border-data-flows.pdf
18. De Rausas, M.P., Manyika, J., Hazan, E., Bughin, J., Chui, M., and Said, R. 2011. "Internet Matters: The Net's Sweeping Impact on Growth, Jobs and Prosperity." McKinsey Global Institute. https://www.mckinsey.com/~/media/McKinsey/Industries/High%20Tech/Our%20Insights/Internet%20matters/MGI_internet_matters_exec_summary.ashx
19. Drexl, Josef, Reto M. Hilty, Luc Desaunettes, Franziska Greiner, Daria Kim, Heiko Richter, Gintarė Surblytė, and Klaus Wiedemann. 2016. "Data Ownership and Access to Data: Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate." Max Planck Institute for Innovation and Competition. http://pubman.mpdl.mpg.de/pubman/item/escidoc:2339820/component/escidoc:2339821/Positionspaper-Data-Eng-08-31_def-korr%20Copy.pdf.
20. Deloitte. n.d. "Blockchain from a Perspective of Data Protection Law: A Brief Introduction to Data Protection Ramifications." Deloitte. Accessed December 31, 2018. https://www2.deloitte.com/dl/en/pages/legal/articles/blockchain-datenschutzrecht.html.
21. eBay. 2016. "Small Online Business Growth Report: Towards an Inclusive Global Economy." San Jose: eBay. https://www.ebaymainstreet.com/sites/default/files/ebay_global-report_2016-4_0.pdf
22. Einav, Liran, and Jonathan Levin. 2013. "The Data Revolution and Economic Analysis." NBER Working Paper, no. No. 19035 (May). http://www.journals.uchicago.edu/doi/abs/10.1086/674019.

23. Elsig, Manfred, and Sebastian Klotz. 2018. "Data Flow-Related Provisions in Preferential Trade Agreements." WTI Working Paper No. 03/2018. https://www.wti.org/media/filer_public/5f/92/5f920ca0-45b6-42e8-ad84-dae13c275c2a/wti_wp_03_2018_data_flow_related_provisions_in_ptas.pdf.
24. Ferracane, M.F. 2017. "Restrictions on Cross-Border Data Flows: A Taxonomy." ECIPE Working paper 01. https://ecipe.org/publications/restrictions-to-cross-border-data-flows-a-taxonomy/
25. Ferracane, M.F., Kren, J., and van der Marel, E. 2018. "Do Data Policy Restrictions Impact the Productivity Performance of Firms and Industries?" ECIPE DTE Working Paper 01. http://ecipe.org/publications/do-data-policy-restrictions-impact-the-productivity-performance-of-firms-and-industries/
26. Ferracane, M.F., and van der Marel, E. 2018. "Do Data Policy Restrictions Inhibit Trade in Services?" ECIPE DTE Working Paper 02. http://ecipe.org/publications/do-data-policy-restrictions-inhibit-trade-in-services/
27. Fink, Michele. 2018. "Blockchains and Data Protection in the European Union," Max Planck Institute for Innovation & Competition Research Paper. No. 18-01. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080322.
28. Forbes Technology Council. n.d. "Should World Governments Get Access to Encrypted Data? 11 Tech Experts Weigh In." Forbes. Accessed January 14, 2019. https://www.forbes.com/sites/forbestechcouncil/2018/10/26/should-world-governments-get-access-to-encrypted-data-11-tech-experts-weigh-in/.
29. Force Hill, Jonah. 2015. "Problematic Alternatives: MLAT Reform for the Digital Age." Harvard National Security Journal (blog). January 28, 2015. http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age/.
30. Grimes, A., Ren, C., and Stevens, P. 2012. "The Need for Speed: Impacts of Internet Connectivity on Firm Productivity." *Journal of Productivity Analysis* 37 (2): 187-201. https://link.springer.com/article/10.1007/s11123-011-0237-z
31. Grossman, Robert L, Allison Heath, Mark Murphy, Maria Patterson, and Walt Wells. 2016. "A Case for Data Commons: Toward Data Science as a Service." Computing in Science & Engineering 18 (5): 10–20.
32. ISO. n.d. "ISO/IEC 27001 Information Security Management." Accessed December 28, 2018. http://www.iso.org/cms/render/live/en/sites/isoorg/home/standards/popular-standards/isoiec-27001-information-securit.html.
33. ITU.2016. "ITU-T Y.3600 – Big data standardization roadmap." https://www.itu.int/rec/T-REC-Y.Sup40-201607-I/en
34. ITU. 2018. "ICT Statistics Home Page." Accessed January 3. https://www.itu.int/en/ITU-D/Statistics/Pages/default.aspx
35. Japan Fair Trade Commission. 2017. "Report of Study Group on Data and Competition Policy." http://www.jftc.go.jp/en/pressreleases/yearly-2017/June/170606.files/170606-4.pdf.
36. Kent, Gail. 2015. "The Mutual Legal Assistance Problem Explained." The Center for Internet and Society Blog. February 23, 2015. /blog/2015/02/mutual-legal-assistance-problem-explained.
37. Korea. 2011. *Personal Information Protection Act*. http://koreanlii.or.kr/w/images/0/0e/KoreanDPAct2011.pdf
38. KPMG. 2017. Understanding the Data and Analytics Landscape in Singapore: A Study of Data and Analytics Adoption and Practices in Six Sectors. Singapore: KPMG. https://www.cccs.gov.sg/-/media/custom/ccs/files/media-and-

publications/publications/occasional-paper/understanding-the-data-and-analytics-landscape-in-singapore--kpmg-16-aug-2017final.pdf

39. Krueger, A.O., San Andres, E.A., and Hredzak, T.L. 2017. 2017 APEC Economic Policy Report – Structural Reform and Human Capital Development. Singapore: APEC Secretariat. https://www.apec.org/Publications/2017/11/2017-APEC-Economic-Policy-Report
40. Kuner, Christopher. 2013. Transborder Data Flows and Data Privacy Law. First Edition. Oxford, UK: Oxford University Press.
41. Lewis, J. 2018. "Economic Impact of Cybercrime – No Slowing Down." Center for Strategic and International Studies (CSIS) and McAfee. https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email
42. López-González, J., and Ferencz, J. 2018. "Digital Trade and Market Openness." OECD. https://www.oecd-ilibrary.org/docserver/1bd89c9a-en.pdf?expires=1546854446&id=id&accname=guest&checksum=B54EB16F2C5E86DA4380BA3FC088A491
43. Lund, S., and Manyika, J. 2017. "Defending Digital Globalization." In *Foreign Affairs*. Accessed January 7. https://www.foreignaffairs.com/articles/world/2017-04-20/defending-digital-globalization
44. Malaysia. 2016. *Personal Data Protection Act 2010*. http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20709%2014%206%202016.pdf
45. Manyika, J., Lund, S., Bughin, J., Woetzel, J., Stamenov, K., and Dhingra, D. 2016. "Digital Globalization: The New Era of Global Flows." McKinsey Global Institute. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows
46. Manyika, J., Chui, M., Miremadi, M., Bughin, J., George, K., Wilmott, P., and Dewhurst, M. 2017. "A Future that Works: Automation, Employment, and Productivity." McKinsey Global Institute. https://www.mckinsey.com/~/media/mckinsey/featured%20insights/Digital%20Disruption/Harnessing%20automation%20for%20a%20future%20that%20works/MGI-A-future-that-works-Executive-summary.ashx
47. Manyika, J., Ramaswamy, S., Khanna, S., Sarrazin, H., Pinkus, G., Sethupathy, G., and Yaffe, A. 2015. "Digital America: A Tale of the Haves and Have-mores." McKinsey Global Institute. https://www.mckinsey.com/~/media/McKinsey/Industries/High%20Tech/Our%20Insights/Digital%20America%20A%20tale%20of%20the%20haves%20and%20have%20mores/Digital%20America%20Full%20Report%20December%202015.ashx
48. Mattoo, Aaditya, and Joshua P. Meltzer. 2018. International Data Flows and Privacy: The Conflict and Its Resolution. Policy Research Working Papers. The World Bank. https://doi.org/10.1596/1813-9450-8431.
49. Meijers, H. 2014. "Does the Internet Generate Economic Growth, International Trade, or Both?" *International Economics and Economic Policy* 11 (1-2): 137-163. https://link.springer.com/article/10.1007%2Fs10368-013-0251-x
50. Meltzer, J.P., and Lovelock, P. 2018. "Regulating for a Digital Economy: Understanding the Importance of Cross-Border Data Flows in Asia." Brookings Institution. https://www.brookings.edu/research/regulating-for-a-digital-economy-understanding-the-importance-of-cross-border-data-flows-in-asia/

51. "Model Contracts for the Transfer of Personal Data to Third Countries." n.d. Text. European Commission. Accessed May 3, 2018. https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en.
52. Muncaster, Phil. 2017. "BSI Upgrades Data Protection Standard." Infosecurity Magazine. May 11, 2017. https://www.infosecurity-magazine.com:443/news/bsi-upgrades-data-protection/.
53. OECD. 2013. The OECD Privacy Framework 2013. Paris, France: OECD Publishing. http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.
54. OECD. 2015. "Data-Driven Innovation: Big Data for Growth and Well-Being." Paris, France: OECD Publishing. http://www.oecd.org/sti/data-driven-innovation-9789264229358-en.htm.
55. OECD. 2016a. "Digital Convergence and Beyond: Innovation, Investment, and Competition in Communication Policy and Regulation for the 21st Century." Paris: OECD. http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP(2015)2/FINAL&docLanguage=En
56. OECD. 2016 b. "Stimulating Digital Innovation for Growth and Inclusiveness: The Role of Policies for the Successful Diffusion of ICT." OECD Digital Economy Papers 256.
57. OECD. 2018. "OECD Expert Workshop on Enhanced Access to Data: Reconciling Risks and Benefits of Data Re-Use." DSTI/CDEP/SPDE(2018)4. OECD Publishing. http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CDEP/SPDE(2018)4&docLanguage=En.
58. OECD 2018 b. "Open Government Data - OECD," accessed December 28, 2018, http://www.oecd.org/gov/digital-government/open-government-data.htm.
59. Osnago, A., and Tan, S.W. 2016. "Disaggregating the Impact of the Internet on International Trade." World Bank Policy Research Working Paper 7785. https://openknowledge.worldbank.org/bitstream/handle/10986/24866/WPS7785.pdf?sequence=4&isAllowed=y
60. Pasadilla, G., and Wirjo, A. 2018. "Globalization, Inclusion, and E-Commerce: APEC Agenda for SMEs." APEC Policy Support Unit. https://www.apec.org/Publications/2018/02/Globalization-Inclusion-and-E-Commerce---APEC-Agenda-for-SMEs
61. Pepper, R., Garrity, J., and LaSalle, C. 2016. "Cross-Border Data Flows, Digital Innovation, and Economic Growth." In *The Global Information Technology Report 2016 – Innovating in the Digital Economy*, edited by Silja Baller, Soumitra Dutta and Bruno Lanvin, 39-47. Cologny: World Economic Forum. http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf
62. People's Bank of China. 2011. "Notice of the People's Bank of China on Urging Banking Financial Institutions to Protect Personal Financial Information." http://www.gov.cn/gongbao/content/2011/content_1918924.htm
63. Practical Law. n.d. "Data Protection in South Korea: Overview." Accessed January 29, 2019. http://uk.practicallaw.thomsonreuters.com/2-579-7926?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1.
64. Qiang, C.Z., Rossotto, C.M., and Kimura, K. 2009. "Economic Impacts of Broadband." In *Information and Communications for Development 2009 - Extending Reach and Increasing Impact*, edited by Mohsen A. Khalil, Philippe Dongier, Valerie D'Costa, Christine Zhen-Wei Qiang, Peter L. Smith, Randeep Sudan, Eric Swanson, and Björn Wellenius, 35-50. Washington D.C.: World Bank.

https://openknowledge.worldbank.org/bitstream/handle/10986/2636/487910PUB0EPI1101Official0Use0Only1.pdf

65. Scaria, Elizabeth, Arnaud Berghmans, Catarina Arnaut, Marta Pont, and Sophie Leconte. 2018. Study on Data Sharing between Companies in Europe. European Commission. https://publications.europa.eu/en/publication-detail/-/publication/8b8776ff-4834-11e8-be1d-01aa75ed71a1/language-en.
66. U.S. Department of the Treasury, Internal Revenue Service. 2016. *Publication 1075*. https://www.irs.gov/pub/irs-pdf/p1075.pdf
67. USITC. 2017. Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions. Washington D.C.: USITC. https://www.usitc.gov/publications/332/pub4716_0.pdf
68. USITC. 2014. Digital Trade in the U.S. and Global Economies, Part 2. Washington D.C.: USITC. https://www.usitc.gov/publications/332/pub4485.pdf
69. Veer, Hans van der, and Anthony Wiles. 2008. "ETSI White Paper No. 3: Achieving Technical Interoperability -the ETSI Approach." ETSI. https://www.etsi.org/images/files/ETSIWhitePapers/IOP%20whitepaper%20Edition%203%20final.pdf.
70. Vásquez Callo-Müller, Maria. 2018. "GDPR and CBPR: Reconciling Personal Data Protection and Trade." APEC#218-SE-01.10. Singapore: Asia-Pacific Economic Cooperation Policy Support Unit. https://www.apec.org/Publications/2018/10/GDPR-and-CBPR---Reconciling-Personal-Data-Protection-and-Trade.
71. World Bank. 2018. "World Development Indicators." Accessed January 7. http://datatopics.worldbank.org/world-development-indicators/

CHAPTER 2: TRANSPORT AND LOGISTICS[46]

2.1. Sector overview

Aviation

The aviation industry is an essential contributor to cross border trade. By carrying people and freight between and within economies airlines are integral trade in services and goods. Air transport is estimated to support 32.9 million jobs and USD1.7 trillion in GDP in the APEC economies[47].

The efficient and safe transportation of goods and people, including by air, are key to APEC's goal of free and open trade in the Asia-Pacific region[48]. For example, in 2016 Tourism Ministers from APEC agreed that enhancing international and domestic air connectivity was important to foster the kind of efficient and secure travel needed to help APEC economies achieve their shared target of 800 million international tourists by 2025[49].

A key objective of the APEC Transportation Working Group (TPTWG) is encouraging transport liberalisation to support the broader APEC trade goals. In 1999 APEC leaders agreed to the *Eight Options for More Competitive Air Services with Fair and Equitable Opportunity*[50]. Each member economy is free to implement one or more of the options at their own pace.

Box 6. The Eight Options for More Competitive Air Services with Fair and Equitable Opportunity

Option 1: Ownership & Control (medium priority) "that APEC economies give consideration to relaxing the ownership and control requirements when considering designation made by partners under bilateral air services arrangements on a case-by-case basis."

Option 2: Tariffs (medium priority) "that APEC economies support the removal or progressive easing off tariff regulations through the bilateral air services arrangements where this promotes competitive pricing to the benefit of consumers."

Option 3: Doing Business (high priority) "that APEC economies work towards removing impediments to "doing business" matters whether under bilateral agreements or in domestic laws and by-laws."

Option 4: Air Freight (medium priority) "that APEC economies progressively remove restrictions in the operations of air freight services while ensuring that fair and equitable opportunity for the economies involved."

[46] This chapter discusses the collective views of firms consulted in the transportation (aviation, railways and shipping) and logistics sectors (postal, freight, and infrastructure operations management). The grouping of these industries has been selected because the firms consulted in these sectors are participating in the following common activities: 1) Directly providing people and/or freight transportation services locally and internationally; 2) Managing local and global infrastructure assets and operations to support people and/or freight transportation services; and 3) Employing large contingents of staff and/or contractors to provide their services.

[47] Air Transport Action Group 2016 https://aviationbenefits.org/around-the-world/apec/

[48] APEC, Bogor declaration 1994

[49] APEC, Tourism Working Group

[50] APEC Leader's summit, Auckland New Zealand 1999

Option 5: Designation (high priority) "that APEC economies include, as appropriate, multiple airline designation in their bilateral air services agreements."

Option 6: Charters (medium priority) "that APEC economies allow and facilitate the operation of both passenger and freight ad hoc charter services which supplement or complement scheduled services, having regard to the principle of reciprocity, as appropriate."

Option 7: Cooperative Arrangements (high priority) "that APEC economies facilitate cooperative arrangements such as code-sharing including third-economy code-share and code-share over domestic sectors, joint operations and block space arrangements, where it can be shown to be of benefit to consumers and airline (s), and where there are not anti-competitive effects."

Option 8: Market Access (medium priority) "that APEC economies and approach to progressively achieve more liberalised market access under their bilateral air services arrangements."

Some suggest that Option 3 in the *Eight Options for More Competitive Air Services with Fair and Equitable Opportunity* is one that naturally includes the regulation of data management where data is integral to airlines doing business. This can include for example the data involved in ancillary activities, such as "ground handling arrangements, the sale and marketing of air services products and access to computer reservation systems (CRSs)"[51].

Data regulation which affects the management of airline loyalty schemes and service/product pricing strategies can address or worsen barriers to entry. The OECD has identified these issues as common structural barriers in airline markets[52].

Logistics and transport (railways and shipping)

Logistics is integral to cross border supply chain management and international trade in any goods and services. But it is only one component affecting supply chains. Other important factors include the adequacy of infrastructure, the complexity of customs processes, and intermodal connectivity.

Data management can play an important role in improving the logistics necessary to facilitate efficient supply chain management. For example, it is reported that for fast growing APEC economies the average price for customs clearance is USD130, compared to Korea where it is USD30, much cheaper because of electronic documentation[53].

One initiative undertaken by APEC to improve the seamlessness and efficiency of logistics is via Asia-Pacific Model E-Port Network (APMEN). Nineteen ports/e-ports in APEC economies are part of this network and participate in sharing cargo and customs data with each other and customs authorities to increase freight clearance efficiency.

As an example, participating ports under the APMEN pilot project of Sea Freight Logistics Visualization are collaborating to exchange data pertaining to imports and exports logistics. The first phase was undertaken with the active participation from New South Wales (NSW) Ports, Shanghai E-Port and Xiamen E-Port. The project starts with the port-to-port information sharing of product location/situation, such as arrival, discharge, inspection, clearance and departure. Having the capability to undertake real-time tracking and tracing services can improve transparency and visibility of cross-

[51] Grosso, Air passenger transport in APEC: regulation and impact on passenger traffic, OECD, 2010
[52] OECD, Airline competition http://www.oecd.org/competition/airlinecompetition.htm
[53] PricewaterhouseCoopers, APEC's evolving supply chain 2012

border logistics, as well as contribute towards seamless integration and collaboration across different stakeholders.

2.2. Profile of firms interviewed

The nine firms whose views are reflected in this chapter are headquartered in Australia; Malaysia; Singapore; Chinese Taipei; and Viet Nam. Of the nine firms, six have international operations involving cross border trade. The largest firms employ over 20,000 staff and the smallest employ about 160 people.

Of those in the aviation sector, both Firms A and B are private firms and operate within their jurisdictions of origin and internationally. Key facts include:

- Firm A operates in up to 20 international jurisdictions accessing 500 destinations including outside the APEC region. It does this directly and via a network of codeshare partners.
- Firm B operates in 10 jurisdictions within the APEC region accessing 130 destinations. It accesses destinations directly. It has a parent firm and subsidiaries operating from each of the 10 jurisdictions.
- Both Firms A and B employ over 20,000 staff and are large enterprises.
- Firm A provides services to business (corporate account travel) and consumers (leisure travel) while Firm B provides services to consumers mainly.

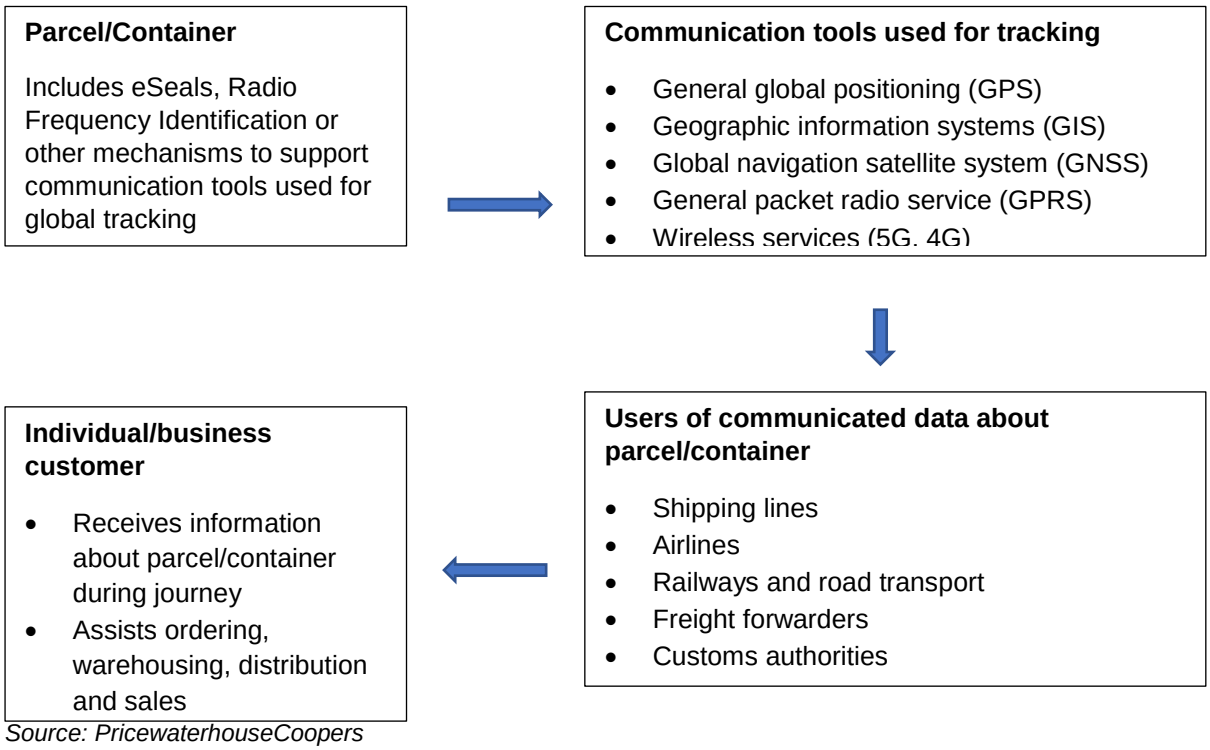
Of the logistics firms, four (Firms C, D E, F) are private firms and one (Firm G) is government owned. Key facts are:

- Firms C, D and G are involved in postal and freight management including parcel and cargo transportation and delivery, warehouse management, repackaging and processing, collection of payment, door to door delivery for customers, and customs brokerage. Of these Firm C is fully global with its own fleet of aircraft and ground vehicles while Firms D and G manage logistics services domestically with some cross-border trade facilitation via contractors. All offer online cargo/parcel tracking for customers.
- Firm E provides infrastructure support services at an international airport including ground handling, cleaning and catering for aircraft.
- Firm F is contracted by the Government to manage the compliance of trade documentation accompanying goods and services with local regulatory requirements.

Of the marine and rail transport firms, both Firms H and I are government owned. Firm H provides domestic and international freight shipping services and Firm I domestic railway services carrying passengers and freight.

One common contribution which Firms A-I make to global supply chains is the transportation and handling of international freight. Data collection, flows and monitoring can be integral to freight management as illustrated in the Figure 5 below.

Figure 5. How data supports freight management in international trade[54]



Source: PricewaterhouseCoopers

2.3. Role of data in firms' business models

The common ways in which these nine firms collect and use data to provide their services include the following:

Collection and use of customer data

- Collect personal data of individual customers via processes customers use to purchase services.
- Collect personal data of individual customers (including the service preferences of customers) via membership application processes, such as frequent flyer, regular commuter or other loyalty schemes.
- Collect the business data of corporate customers via processes customers use to purchase services on a regular or infrequent basis.
- Use personal and corporate data of customers to develop, tailor and offer account management and loyalty scheme services including the design and promotion of price discounts, service consolidation, improved service convenience, new services, and ancillary benefits to reward customer loyalty.
- Collect customer data to facilitate regulatory compliance with trading requirements.

Collection and use of their own business data

- Collect performance data from infrastructure assets such as aircraft, vehicle, shipping and railway fleets, courier and postal payment devices. This can occur directly from asset

[54] PricewaterhouseCoopers, APEC's evolving supply chain 2012

inspections or remotely when assets are operating. The collection of data remotely is generally facilitated by satellite and GPS technology.
- Use performance data to monitor and assess the safety, capacity and efficiency of asset deployment. This enables firms to evaluate ways to ensure safety, improve cost recovery, enhance customer responsiveness (such as cargo tracking or customer alerts about service delays), increase customer and cargo yields, and optimise competitiveness in new or existing markets.

Collection and use of business partner data
- Collect data from other firms with which they have alliances and partnerships, such as aviation code sharing arrangements where airlines provide services for each other to support seamless travel for customers between destinations. This data may be the personal or corporate information of shared customers and asset information transferred between partners to support the integrated management of their respective infrastructure.
- Use shared information to jointly design and offer improved and new customer services.

Nature of data being managed

All firms manage significant volumes of data. This includes:
- Information which customers directly provide when booking flights, shipping services, railway journeys, scheduled aircraft handling, and cargo management.
- Information which customers directly provide when booking ancillary services such as accommodation, car hire or leisure experiences offered via the airline websites in conjunction with flight bookings or rail journeys.
- Information about customers provided to the airlines and railway firms by third party booking services including travel agents, corporate account management services, and internet based travel booking engines such as Webjet and Expedia.
- Customer information collected and used to manage loyalty programs such as Frequent Flyer services and other reward programs, corporate service accounts, and cargo management accounts.
- Engineering and operational information collected about all aspects of asset and infrastructure performance. For example for airlines this can include aircraft fleet including data collected directly and remotely when aircraft are operating from airport terminals, when aircraft are flying between destinations and when aircraft are subject to maintenance in any location internationally.
- Information about cargo/luggage which they are transporting.

Firms were asked to describe the nature of their data use and provide examples of business activities dependent on or arising from this data use. Firms were also given options for data use which are based on the four common forms of digitalisation. Table 4 below illustrates the four kinds of digitalisation and examples provided by firms of business activities relying on this data use.

Table 4. Ways in which different kinds of digitalisation support business practices

Kinds of digitalisation	Examples
Principally online ordered and online supplied products/service	• Redemption of frequent flyer loyalty points online towards online travel booking or goods/services purchasing.
Principally online ordered products or services that are then supplied offline (i.e. physical products or services provided offline)	• Air travel or rail services purchased online but delivered offline via physical infrastructure services. • Parcel management ordered online but physically delivered.
Principally offline products or services	• Shipping services ordered offline and delivered by physical infrastructure. • Ground handling at airports ordered offline and delivered by physical activity.

Kinds of digitalisation	Examples
Online network, platform or matching service (i.e. enabling other entities that supply relevant products or services)	• Airline online booking services offer opportunities for customers to also purchase accommodation, care hire and leisure activities from third parties.

Source: Consultation with firms

How data flow enables the business

All firms consider that data flows are integral to their business operations. The collection and management of data is an enabler to support three key business activities in particular. These are:

- Customer relationship management;
- Operational efficiency; and
- Dynamic pricing of service offerings.

In competitive markets, such as the international airline and shipping industry, these business activities are critical to growing market share amongst customers and reducing costs of service without compromising safety.

All firms report that customer relationship management is a key focus of their data strategy because it is essential for business success. Customer relationship management includes:

- Understanding customer needs and preferences;
- Offering direct and ancillary services and promotions targeted to customer preferences;
- Rewarding customers for loyalty; and
- Securing repeat purchases from existing customers.

Cross border data flows enable some all-encompassing high-level business activities ranging from sourcing inputs and suppliers to customer relationship management, enterprise planning and monitoring the performance and use of services and products. These are described in the table below. Firms were asked to explain what these business activities mean in practice for their daily operations. Their responses are captured in Table 5 below and illustrate what kinds of essential business practices are enabled by data flows.

Table 5. Kinds of business practices relying on data flows

Kinds of business activities enabled by data flows	Examples
Sourcing and procurement of inputs and suppliers.	• Purchasing and managing fleet fuel, in-flight catering for airlines, railway carriage cleaning.
Logistics and management of your supply and distribution chain.	• Scheduling of services, management of services and scheduling of asset maintenance. • Management of warehouse capacity and distribution of goods.
E-commerce or other sales and supply to customers directly or via third party platforms.	• Customer journey bookings and other related customer ground travel arrangements.
Invoicing and payments.	• Customer and supplier payments.
Customer relationship management (CRM).	• Frequent flyer schemes to reward customer loyalty. • Corporate account management for cargo delivery.
Enterprise resource planning (ERP).	• Airline, railway and shipping crew scheduling across all travel routes. • Management of parcel delivery contractors.
Delivery of products/services such as media or communication services.	• In-flight entertainment provided by airline and/or support for passenger's entertainment on own devices.

Kinds of business activities enabled by data flows	Examples
Monitoring usage of services/products such as consumption of utilities and infrastructure.	• Fuel, inflight catering and aircraft, railway and vehicle fleet maintenance planning, safety management, and cargo and luggage handling.

Source: Consultation with firms

Data storage options

The firms store data in various ways including the following.

- Four firms store all information in the cloud . In this case two firms use cloud services provided by specialist third parties and two use cloud services built by them. All data is stored in this way regardless of its sensitivity.

- One firm uses a mix of cloud and firm server storage options depending on the data. It ensures that all personal information about customers is stored on firm-owned servers in the jurisdiction where they are headquartered and other international jurisdictions where they operate. This is to add a further level of data security beyond the normal protocols applying to cloud and servers storage.

- Four firms host information on their own servers and storage devices in both on-premise data centres and hybrid clouds regardless of the nature of the data.

The use of storage options does not appear to depend on the size of the business, although larger firms have greater capacity to invest in their own servers.

Use of artificial intelligence (AI) and blockchain

Three of the nine firms are either using or considering using AI and/or blockchain. For example:

- Firm A uses AI to gain efficiencies in disruption management and customer care and will continue to evaluate the opportunities for efficiencies and process improvements as AI gains further traction in their supply chain. They consider that AI will increasingly enable many tasks across the business to be simplified and produced at scale and pace.

- Firm D reports that "AI and blockchain technologies are more likely to have positive impact on our business, and we expect to utilize these technologies to enhance our business performance and reduce operational cost".

- Firm E reports that "we view positively the impact of new technologies such as AI and Blockchain and have actively engaged in Proof of Concepts in multiple areas of our business, to assess the feasibility and impact of adopting such technologies".

Data security and privacy governance

All of the firms suggest that they take a systematic approach to data security. Their methods include all or many of these activities:

- Ensuring their policies, procedures and practices are consistent with international quality assurance instruments governing data security and privacy. This is primarily achieved by firms ensuring they are compliant with ISO27001 and BS10012. The ISO 27001 is the international standard for

information security and provides a basis for achieving the technical and operational requirements necessary to comply with the European Union's General Data Protection Regulation (GDPR). The BS 10012 provides the core standards firms need to comply with when collecting, storing, processing, retaining or disposing of personal records related to individuals. The BS 10012 was updated in 2017 to incorporate the requirements of the GDPR.

- The systematic and regular review of local laws and regulations governing data security and management to ensure compliance. These local laws can include the personal data protection laws/regulations of economies such as Malaysia; Singapore; and Chinese Taipei.

- Applying a sophisticated and comprehensive data governance framework which consists of firstly classifying all data according to its sensitivity and secondly restricting access within the firm to data according to levels of sensitivity.

- Regulatory compliance and cyber security awareness and best practice training for all staff involved in handling business and customer data depending on the level of data staff members are authorised to manage. Various staff within each organisation are responsible for handling and managing data including its reporting, security and privacy. For example staff responsible for data management can include those taking customer bookings or handling complaints, managing customer accounts and loyalty schemes and overseeing the delivery of goods and services.

- Managing data flows within secure, transparent and auditable frameworks. This includes assessing the most secure and trusted hardware and location when choosing storage infrastructure; employing their own cyber protection teams which are heavily involved in the design and operation of selected hardware and the flow of data; and applying end-to-end encryption on all data flows across borders and over the Internet.

Most firms have governance structures where management must report against data security and privacy key performance indicators. In most firms this reporting occurs between layers of management and between management and the Board. Firms contain specific executives with ultimate responsibility for data security and privacy management. This is either the General Counsel or Chief Information Officer.

Key performance indicators that firms use to manage the compliance of their organisations and staff with data security and privacy regulations and standards tend to be based on indicators to support planning, doing, auditing and improving. These are described in Table 6 below.

Table 6. Common key performance indicators used by firms to manage data security

	Key indicator to meet regulatory standard	**Organisational information source**
Planning	Number of business activities needed to support compliance	Planning/scoping documents in business planning
	Number of security activities assessed against a risk/risk mitigation/business impact matrix	Risk management plan
	Inclusion of data security issues in commercial agreements the firm has with customers, suppliers, distributors and partners.	Non-disclosure agreements, service level agreements, customer contracts
Doing	Number of times security issues create service disruptions	Service level reports
	Duration of service disruptions created by security issues	Service level reports
	Time taken to resolve security issues	Service level reports
Audit	Frequency of security requirements are assessed	Risk management plan
	Sophistication of auditing	Risk management plan
Improvement	Number of identified improvements implemented	Risk management plan
	Timeframes for implementing improvements	Risk management plan

Source: Consultation with firms

Brand trust from good data management

All firms report that data security and privacy management is integral to their business values, competitiveness and growth. They believe that their "social contract" or "social licence to operate" is heavily defined by whether and the extent to which their customers trust them to both protect customer data and to deal with it appropriately.

This means that firms have a natural commercial motivation to ensure they design, implement and manage superior data governance and high levels of security to maintain trust in their brands and ongoing customer loyalty.

2.4. How policies and regulations are impacting their business models

Applicable data regulation and compliance costs

Because of the international nature of their business, seven of the nine firms are subject to various privacy legislation applied in individual member economies within APEC. Firms with EU residents amongst their customers are also subject to the EU *General Data Protection Regulation* (GDPR).

Direct costs

Firms report various significant direct costs associated with regulatory compliance of the kinds explained in the Table 7 below.

Table 7. Kinds of compliance costs reported by firms

Kinds of compliance costs	Examples
Recruiting specialised staff to improve compliance and/or reduce risk.	• Employment and/or contracting cyber security to oversee the design and management of hardware and processes to gather and store information.
Investing in new infrastructure and information technology architecture to improve compliance and/or reduce risk.	• Investment in compliant information management hardware and software, data programming and cloud based or local information storage solutions.
	• Amendment of online and offline processes to gather and retain personnel information during customer booking and relationship management processes.

Source: Consultation with firms

Firm reports that its need to comply with the GDPR has required it to invest millions of dollars in capital cost and commit to additional annual operational spending. The level of spending is related to the prescriptive nature of the GDPR which regulates the firm's data in these ways:

- The data it can collect;
- The permissions to access the data it collects; and
- The purposes for which it can use the data it collects.

Opportunity costs

In addition to direct costs there are a range of opportunity costs which firms experience as a result of data regulation and compliance requirements.

Some firms suggest that the complexity of new data laws have inhibited the ambitions of certain parts of its business to expand their customer services and products. This can impede development of new products and services that would have benefited customers.

Firms acknowledge that a large proportion of their capital expenditure to comply with data regulation would have been spent anyway to maintain customer trust in their brands. However some suggest that many laws, such as GDPR, far exceed reasonable protective purposes, and stray into legislating against normal and positive commercial exchanges/ bargains.

Beyond this impact, firms believe that data regulation has created the kind of opportunity costs for them described in the Table 8 below.

Table 8. Opportunity costs reported by firms

Kinds of opportunity costs	Examples
Reduced trading and diversification into international markets.	• This occurs when data laws in individual jurisdictions are not aligned and some impose mandatory requirements that exceed others, such as demands for local data storage or compulsory sharing of firm data with governments.
Decreased competitiveness in one or more markets.	• The cost implications of complying with data regulation are related to the scale of the business, the extent of its customer base, the specific features of its loyalty programs and the degree to which it partners with third parties to offer products and services. For example some airlines have global partnerships with hotel and car hire firms to enable customers to choose these ancillary services in conjunction with flight bookings. These airlines will be at a competitive disadvantage in markets where regulatory burdens add costs because of these partnerships.
Reduced their investment in and/or capacity for innovation.	• Capital expenditure envelopes for business are finite and the mandatory component of data regulation necessarily diminishes the commercial component. Capital expenditure programs can be subject to volatility in the price of fuel (a sunk cost for airlines, shipping lines and railways) and other inputs, and external shocks such as natural disasters, pandemics, economic slowdowns and terrorism.

Source: Consultation with firms

The benefits of regulation

All firms consider that the primary benefits of regulation which protects customer privacy are that it can:

- Support their social licence to operate. Regulation gives their data management increased legitimacy.
- Help to build customer trust of their services and their commitment to protect customer interests; and
- Level the playing field against/ between organisations that fail to take heed of their own "social contract" and breach customer trust. Enforcement against perpetrators assists to increase the legitimacy of firms who uphold the terms of their social licence to operate.

Firms also consider that regulation intended to protect intellectual property rights of data has benefits because it gives firms confidence to invest and trade outside their home jurisdictions.

Regulation which aims to promote frameworks for managing data security is less necessary because firms have strong commercial motivations to protect the integrity of their business data.

Concerns with current regulatory approaches

Regulatory scope

Some firms are concerned about regulatory over-reach which occurs when jurisdictions seek to regulate data collection, storage and use outside of their territorial borders. They cite for example the EU and some APEC economies as examples of jurisdictions which seek to claim extra-territorial control by using punitive measures to enforce alignment between practices in their own and other jurisdictions undertaken by entities.

Regulatory alignment

Some firms are concerned that individual divergent approaches to data regulation in a global trading environment can unnecessarily increase compliance costs. In the absence of an agreed common approach firms fear 'bracket creep' regulation where jurisdictions impose new compliance hurdles irrespective of the existence of thorough standards. For example significant new regulatory obligations imposed on them by the GDPR represents a comprehensive approach to protecting the data of EU residents. Nevertheless other economies outside the EU consistently seek to impose their own data protection regimes with little regard to whether this is duplicating the GDPR or adding unnecessary regulatory hurdles.

Firms also considers that the risk of bracket creep arises because jurisdictions take different views about the ownership of data. For example, some jurisdictions assume that all data is owned by and the property of the individual, while some assume that all data is owned by and the property of the corporation or the economy.

These competing views of data ownership give rise to different regulatory approaches with varying impacts on the capacity and liabilities of the firms to collect, manage and use data. The differences in regulatory approaches and associated compliance burden is one key factor firms evaluate when considering whether to enter new markets or diversify service offerings in markets.

In general most firms consider that there is a need for improved alignment between jurisdictions on the key common objectives and implementation of data regulation, particularly for firms whose customers and services are global. This alignment will assist firms to sensibly and cost-effectively navigate compliance requirements in different jurisdictions.

Firms were not aware of APEC's Privacy Framework, Cross Border Privacy Rules (CBPR) or the work APEC is doing to promote the interoperability between the CBPR and EU's GDPR.

Regulatory barriers

Firms were concerned with a range of regulatory barriers created by data regulation. The first is "behind the border barriers" such as lack of transparency or clarity of laws and regulations, that impede market access in economies. Firms reports that these occur and vary between economies. For example, they cite one economy's legal requirement for all data to be retained centrally and made available to the authority as an obligation that conflicts with the internal governance and customer proposition mandates of customers. This restricts access to the market.

The second relates to cross-border transfers of information or requirements to use locally controlled information management systems (such as cloud systems) and how this restricts business operations and trading and investment decisions. Firms reports that requirements for local data storage are significant impediments to market investment and service provision particularly where local data

storage is inconsistent with the cyber security policies and practices of firms. They suggest that APEC should carefully study the EU debate on data controller versus processor which has influenced the GDPR view that all data is owned by the individual.

The third concerns situations where intellectual property rights requirements or issues impede trade in digital services/products in local markets. Firms highlight that this is a significant problem in jurisdictions which do not enforce international intellectual property rights. Firms also suggest that requirements to disclose foreground intellectual property will be a concern as this is knowledge produced within a collaborative venture or an open innovation project that will turn into a competitive advantage for other firms if the IP owners cannot enter markets.

Preferred regulatory approaches

The firms had different views on a preferred approach. While some firms consider that prescriptive government regulation offered the most effective way to protect customer data, others suggested that light touch regulation was more effective to ensure that the management and enforcement of customer data privacy principles remained relevant as technology and business practice evolved. This approach assumes that to maintain brand trust firms will act in the best interests of their customers without the need for firm external regulation.

One firm cites emerging facial recognition technology as an example of business practice evolution which regulation must keep up with. It suggests for example that this technology has a positive impact because it improves travel security and safety and this is something that governments are also committed to. On the other hand the technology creates greater risks for personal liberty and privacy. The firm suggests that light touch regulation enables governments and firms to use such technology in ways that balance competing public policy outcomes.

Some firms suggest that the current model of one APEC economy, which is based on privacy principles, but largely leaving the detail of the execution of the policies and processes to businesses to define, is the kind of model that should be embraced globally. This approach embeds clear privacy objectives but also permits business to develop key differentiating features in their data governance and security practices that is fit for purpose and supports trust in their brand. This balance encourages competition and innovation which ultimately delivers consumer benefits. It should be noted however that this suggested approach would not be enforceable, much like the APEC Privacy Framework.

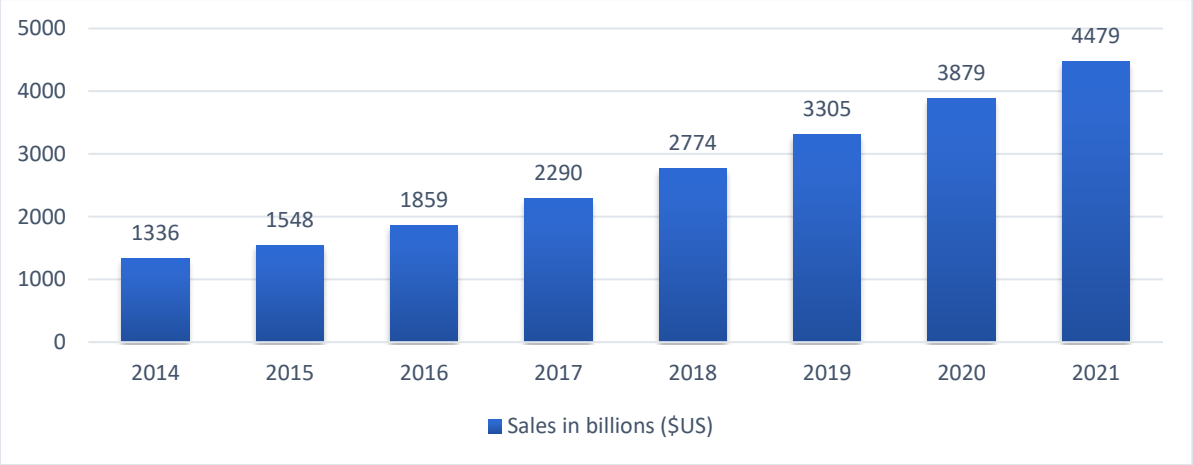
CHAPTER 3: DIGITAL SERVICES AND E-COMMERCE[55]

3.1. Sector overview

General economic contribution

There is little dispute that the internet and digital applications it supports has revolutionised the way goods and services are supplied and consumed and reshaped a significant proportion of economic activity around the world. Between 2014 and 2017 the value of global online sales (USD) has increased by an estimated 40 percent.

Figure 6. Global growth in the value of online sales 2014-2021[56]



It is estimated that retail e-commerce sales in the Asia-Pacific exceeded USD1 trillion in 2017, and its share of global digital spend represents 47.6 per cent of the world market[57].

Access to digital tools increases consumer welfare because it expands product choice and convenience of purchasing. These benefits can be especially important for consumers who are geographically isolated from conventional retailing, such as those living in regional areas, and people whose mobility is impeded by age and/or disability. Consumers who are less familiar with the everyday use of digital

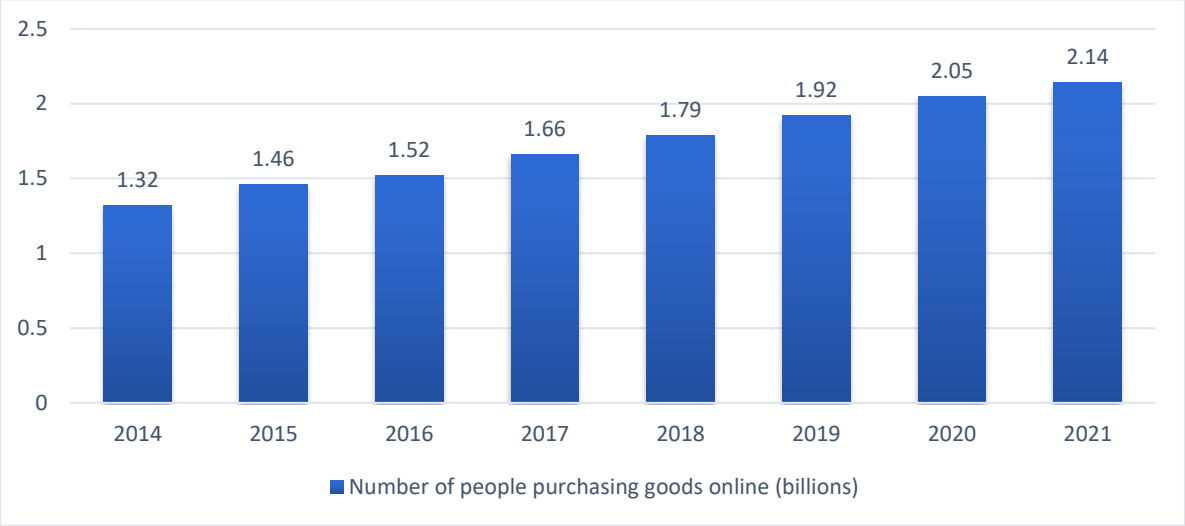
[55] This chapter discusses the collective views of fourteen firms consulted in the digital and internet services as well as e-commerce sectors. These are firms that themselves provide digital services and/or digital security services for other businesses and the wider public. The grouping of these industries has been selected because the firms consulted in these sectors are participating in the following common activities: 1) Providing platform services to business customers to enable those customers to trade. This includes for example online marketplaces where retailers can promote and sell their products; software and applications to support business planning, information security, certifications, operations, customer relationship management and payment solutions; and information technology solutions which improve the efficiency of business transactions and communication; 2) Developing and supplying digital technology solutions to business customers and individual consumers including internet integrated electronics to support connectivity for business and consumer practices and consumer devices; 3) Developing and supplying machine learning (artificial intelligence and blockchain) services to support business analytics and decision making including consumer profiling and preference management; and 4) Providing computer and internet management and support services for business customers to facilitate business practices.

[56] Statista 2017 at https://www.statista.com/statistics/251666/number-of-digital-buyers-worldwide/

[57] APEC PSU, Promoting E-commerce to Globalize MSMEs October 2017

technology, such as the elderly, may be more vulnerable to online fraud, and this increases the need for digital, internet and e-commerce tools and services to provide adequate security. Not offering consumers security of purchasing can have negative implications on a firm's brand. The number of consumers purchasing items online internationally is estimated to continue to increase over time.

Figure 7. Global growth of online consumers 2014-2021[58]



Use of digital services in the APEC region

The use of the internet varies for businesses in the APEC region, but research estimates that business uses online platforms to purchase goods and services more than they use it to sell goods and services.

Table 9. Comparative use of e-commerce by businesses in selected economies in 2015[59]

Economy	Purchasing via the internet (%)	Sales via the internet (%)
Australia	70	45
Canada	68	19
Indonesia	49	42
Japan	32	22
Korea	58	15

Productivity benefits of the digital economy

Research done by OECD across economies at firm and industry level showed that digitalisation increases labour productivity and promotes economic growth. This is despite wide variations in productivity gains across firms flowing from digitalisation[60]. Given this connection the OECD believes that governments should enhance business and consumer access to digital technology and applications, including to increase commercial opportunities for business. It considers for example that:

[58] Statista 2017 at https://www.statista.com/statistics/251666/number-of-digital-buyers-worldwide/
[59] OECD, Key issues for digital transformation in the G20, Report prepared for a joint G20 German Presidency/ OECD conference, Berlin, 12 January 2017, p24-25
[60] OECD, Key issues for digital transformation in the G20, Report prepared for a joint G20 German Presidency/ OECD conference, Berlin, 12 January 2017, p13

"*Digital technologies also offer new opportunities for firms, including in lowering important barriers to entry. For example, digital technologies can facilitate cross-border e-commerce and participation in global value chains (GVCs) (e.g. Skype for communications, Google and Dropbox for file sharing, LinkedIn for finding talent, PayPal for transactions, and Alibaba Group and Amazon for sales). Enhancing access to networks and enabling SMEs to engage in e-commerce can be an effective way for small firms to go global and even grow across borders where they can become competitors in niche markets. For example, M-Pesa, a Kenyan mobile-money service, is now active across Africa as well as South Asia and Eastern Europe*."[61]

One of the barriers to MSMEs capacity to participate in global markets is their ability to invest in digital technology, infrastructure and skills. Often their small scale can create barriers to this investment and underinvestment can impede their productivity growth. OECD finds that MSMEs trail lager firms in technology adaptation because they:

"*face a range of barriers in adopting ICTs and other digital technologies in their operational activities. SMEs tend to have limited financial resources, which makes adopting new technologies, including ICTs, difficult given these tools are often expensive. Another important barrier is related to human and organisational capital since investments in new technologies often require investments in complementary knowledge-based assets. SMEs do not often have the skilled people to operate new digital technologies in their teams, the resources to train these workers, or have the management that can help them make the most of the new technologies*".[62]

One of the key benefits of the digital economy is that it provides MSMEs with the opportunity to flexibly reach global markets without needing to invest significantly in digital technology normally required to do so. As noted by the OECD, MSMEs in economies that are more geographically isolated from trading partners are more reliant on e-commerce, and in these cases the productivity dividend offered by digital platforms is likely to be higher than the average[63].

The opportunity for this productivity dividend arises because the digital economy provides MSMEs with[64]:

- The capacity to reach international consumers including the ability to target consumer markets, which MSMEs could not achieve on their own;

- Research and the analysis of data about consumer spending, preferences, behaviour and other information which enables MSMEs to plan and execute their business objectives with certainty. This kind of data analytics is not something MSMEs could obtain on their own without considerable investment in market research and technologies to capture consumer data;

- Administrative support which lowers the cost of transactions, including for example, access to consumer market information which reduces the costs of decisions; decreasing the need for contracts between buyers and sellers thereby reducing bargaining costs; lower regulatory costs because the third-party marketplace provides business assurance; and providing secure forms of payment; and

[61] OECD 2017, p36
[62] OECD 2017, p116
[63] OECD 2017, 24
[64] Deloitte Access Economics, Platforms, small business and the agile economy 2017 and Aegis Consulting Group analysis

- A digital shopfront and related infrastructure which buyers and sellers can rely on. This includes for example, the capacity to disqualify sellers for poor performance; verification of the authenticity of sellers and buyers prior to use; and insurance covering buyers and sellers for any damage incurred while using online marketplaces.

These productivity benefits have more opportunity to be captured when MSMEs are able to receive the appropriate support for firms providing digital, internet and e-commerce services and tools such as consumer analytics, purchasing process security, business assurance and information system connectivity.

Variations in e-commerce retailing for regulation to consider

Retailing in the e-commerce sector takes various forms depending on the nature of the business doing the selling. This means that businesses rely to varying degrees on some digital services provided by other firms, but the need for e-commerce retailers to provide information security to support brand trust would be common.

Variations in retailing in e-commerce provides a good illustration of the need for data regulation to be fit for purpose for different firms and the different ways they rely on the internet to do business.

The variations in online retailing include:

- **Traditional largescale international retailers with physical and online shopfronts.** Some firms are international branded retailers operating across a range of retail market segments and offering consumers in multiple jurisdictions the capacity to purchase their goods online. These retailers can control the sourcing, manufacture, pricing, supply and distribution of goods offered under their brand and other branded products. The international British based department store, Marks and Spencer, is one example of this. It targets a range of markets including clothing, homewares, furniture and food, and controls the quality and the price of the goods it sells to consumers in those markets. It sells its own branded goods and other branded products. Marks and Spencer offers its goods for sale via fourteen jurisdiction specific websites[65].

- **Micro, small and medium enterprises with physical and online shopfronts**. In every segment for goods and services in the retail market there are MSMEs offering boutique products. This includes MSMEs who control every aspect of the products they offer from manufacturing to distribution, and MSMEs who simply trade other firms' brands directly to the market. Some MSMEs can own and operate their own online selling platforms and other MSMEs can use third party marketplaces like those offered by eBay.

- **Online only retailers**. It is not uncommon for some retail firms to have only an online presence. These firms can range from MSMEs to larger firms wishing to reduce their cost of service. These firms may control every aspect of the products they offer from manufacturing to distribution, or simply trade other firm brands directly to the market. Some can own and operate their own online selling platforms and others can use third party marketplaces like those offered by eBay. Larger firms may have their own websites and use third party marketplaces. One example of an online only retailer trading products manufactured and owned by other firms is Net a Porter which specialises

[65] http://www.marksandspencer.com/au/homepage

in selling designer fashion. It is registered in Hong Kong, China but via its single website sells and ships goods to over 170 economies[66].

- **Online marketplaces with product and pricing control**. The primary example of this kind of firm is Amazon. Its online marketplace offers branded products across a wide variety of market segments including books, clothing, accessories, travel goods, computers, and office supplies. The Amazon marketplace is one where it and other firms sell products. For example, in relation to clothing the Amazon marketplace sells over 50 recognised brands produced and owned by other firms, such as Calvin Klein. These brands and individual items are sold by over 50 sellers including Amazon itself. Beyond this the Amazon Basics range which includes electronic product accessories, homeware, kitchenware, pet supplies and fitness accessories are a mix of products with some carrying the Amazon Basics brand. Accordingly, Amazon is likely to control the pricing of third party goods that it sells as well as the goods that carries its brand. There is no consumer price bidding for goods sold via the Amazon marketplace[67].

- **Online marketplaces with no product and pricing control**. The primary examples of this kind of firm are eBay, Alibaba Group, Etsy and Rakuten. The marketplaces of each of these firms have some common features which are (a) none of these firms sell their own branded products via their marketplaces (unlike Amazon); (b) their marketplaces are purely to support the B2C or B2B connection between sellers and purchasers around the world;(c) they do not control the pricing of goods sold via their marketplaces (unlike all other kinds of online retailing); and (d) their business models do not include the warehousing of goods sold via their marketplaces to meet market demand and support delivery[68].

APEC economies' approach to market regulation

By and large firms operating in the digital/internet services and e-commerce sector are subject to three types of laws across APEC economies. There are:

- General privacy related rules found in domestic legislation like the Personal Information Protection Laws in Japan and Chinese Taipei or the Privacy Act in Australia. As discussed, the APEC Privacy Framework seeks to provide some common principles for economies to apply.
- Some economies also apply industry specific laws such as the various health sector privacy laws at the domestic level in Australia. These can vary between and within economies depending on the industry and whether they are federations or unicameral in nature.
- All economies impose domestic security and defense related rules to the use of digital data. The degree can vary between economies depending on the level of concern about the safety of digital data in their territories, cyber-attacks and how they are dealt with. This kind of regulation can place severe restrictions on firms in the digital and internet services and e-commerce sector.

3.2. Profile of firms interviewed

The fourteen firms whose views are reflected in this chapter are headquartered in Australia; Indonesia; Japan; the Philippines; Singapore; Chinese Taipei; and Viet Nam. Of the fourteen firms, twelve have international operations involving cross border trade. The largest firms employ over 100,000 staff and the smallest are start-ups employing less than 20 people.

[66] https://www.net-a-porter.com/au/en/content/about-us
[67] https://www.amazon.com/
[68] Aegis Consulting Group research 2017

The firms consulted provide a variety of digital and internet services and e-commerce. This includes the following:

- **Software services**. Firms A and B provide a range of software services to many industry sectors. Their customers are mainly large businesses for whom they provide enterprise solutions such as integrated and networked business systems, including payment services. They are involved in the development of fintech and other technologies such as AI.

- **Data analytics to support business services**. Firms C, D and E provide services to business clients to assist those clients maintain and improve the efficiency, capability, customer reach and security of their businesses processes. All three firms are start-ups and all three use machine learning (artificial intelligence) to provide their services to clients. Firm C helps customers with large digital databases to ensure against fraud. Firm D assists their clients to collect and process performance data of industrial assets to help increase reliability, improve efficiency, and prevent unplanned downtime in industrial facilities. Firm E helps clients understand how customers feel about services and products so that those clients can adapt and improve their offering. It provides real time information on customer responses by collecting relevant data from social media platforms like Facebook, and Instagram.

- **Internet support including storage**. Firms F and G provide cloud services and other internet support to business customers.

- **Information security**. Firms H, I and J provide data security services. This includes providing biometric technology for use in security applications and encryption services that protect against identity theft.

- **E-commerce**. Firms K, L and M provide online experiences for the consumer market. Firm K provides an online platform (marketplace) for retailing of a wide range of consumables. The platform enables various sellers including MSMEs to sell their products and connect directly with consumers. Firms L and M provide online gaming platforms through which consumers purchase experience and interactive games.

- **Business information services**. Firm N uses its own software and digital expertise to provide information which is essential for shipping and maritime activities. The information can be downloaded in real time via the firm's website and applications for devices which supports the use of its information by commercial and recreational maritime activities.

A number of focus groups were also undertaken in Taipei City, Tokyo and Singapore that included additional firms in the digital and internet and e-commerce sector. These firms delivered similar services to those listed above and expressed similar views to those reflected by the fourteen firms interviewed and consulted individually.

3.3. Role of data in firms' business models

The common ways in which these fourteen firms collect and use data to provide their services include the following:

Collection and use of consumer and business data

- Collect the business data of their clients to the extent necessary to provide required services. This can include the personal data of individual customers of their clients, such as consumers purchasing items via online platforms.

- Collect consumer data from third party providers in order to shape their advice to clients about preferred software, internet and technology solutions to support the business practices of their clients.
- Collect data from consumers purchasing their products (such as electronics) to identify suitable and preferred next generation features and devices to promote connectivity.

Collection and use of their own business data

- Collect performance data from their own products, computers, online platforms, devices, software and applications and technology to monitor and assess safety, capacity and efficiency of asset deployment. This enables firms to evaluate ways to ensure safety, improve cost recovery, enhance customer responsiveness (such as smart devices), and optimise competitiveness in new or existing markets.

Nature of data being managed

All the firms manage significant amounts of data, often running into the analysis of hundreds of millions of digital files.

The data managed ranges from personal information, starting with names and addresses, to biometrics including facial recognition. Further there is other very sensitive personal data like financial accounts that are stored and managed. This may be as simple as the data used for the online payments systems for a firm's own customers or as sophisticated as the firm operating international payment systems for third party marketplaces.

Firms were asked to describe the nature of their data use and provide examples of business activities dependent on or arising from this data use. Firms were given options for data use which are based on the four common forms of digitalisation. Table 10 below illustrates the four kinds of digitalisation and examples provided by firms of business activities relying on this data use.

Table 10. Ways in which different kinds of digitalisation support business practices

Kinds of digitalisation	Examples
Principally online ordered and online supplied products/service	• All firms accept orders for most of products/services via internet-based routs and provide the products and services online. This ranges from simple viewing of products online to sophisticated digital signatures to protect data.
Principally online ordered products or services that are then supplied offline (i.e. physical products or services provided offline)	• Firm B in this sector provides hardware that is placed in the customers‘ offices, but is ordered online. This includes biometric equipment.
Principally offline products or services	• Firms A and B in this sector provide hardware that is placed in the customers offices and is ordered offline. For example large customers use tender processes to purchase complex network solutions for their organisations.
Online network, platform or matching service (i.e. enabling other entities that supply relevant products or services)	• Firms K, L and M provide advertising products for online services. For example this includes the provision of platforms for third parties to advertise their products.

Source: Consultation with firms

How data flow enables the business

For all firms data flows are critical to their business models. One firm further added that "all of our main operations are not possible unless data flows and data sharing are enabled". This view is reflected in the responses of all firms interviewed.

Data flows enable some all-encompassing high-level business activities ranging from sourcing inputs and suppliers to customer relationship management, enterprise planning and monitoring the performance and use of services and products. These are described in the table below. Firms were asked to explain what these business activities mean in practice for their daily operations. Their responses are captured in the Table 11 below and illustrate what kinds of essential business practices are enabled by data flows.

Table 11. Kinds of business practices relying on data flows

Kinds of business activities enabled by data flows	Examples
Sourcing and procurement of inputs and suppliers.	• Firms A and B provide hardware products for the application of their software technologies.
E-commerce or other sales and supply to customers directly or via third party platforms.	• Firms K, L and M are involved in online payment systems.
Invoicing and payments.	• All firms use data to provide customer and supplier payments. This includes provision of payment platforms that facilitate financial transactions.
Delivery of products/services such as media or communication services.	• Firm M specializes in internet advertising.
Monitoring usage of services/products such as consumption of utilities and infrastructure.	• Firms A and B provide hardware products for the application of their software technologies.

Source: Consultation with firms

Data storage options

All the firms use cloud based computing. Given that they are in the digital sector, it is common for them to use their own servers. In some cases these firms provide cloud computing services as one of their product range. As will be noted later in this chapter, restrictions within economies on cloud computing is a major area of concern in this industry sector.

Use of artificial intelligence (AI) and blockchain

Firms C, D and E rely on artificial intelligence to provide the services they offer to clients. Firm D stated that "making use of data collection and machine learning allows us to adapt our system to many different applications. Because of this, we can scale to different assets in different industries".

It is useful to note that the three firms fully engaged with machine learning are all start-ups with limited resources and scale but providing innovative services in markets. Larger more established firms that were consulted during this research reported that they are planning to use or proving concepts for the adaptation of artificial intelligence in their current business practices but have not fully embraced it yet. Nevertheless, these established businesses consider that artificial intelligence can be a game changer for their business models.

The fact that start-up firms are more engaged with artificial intelligence suggests that machine learning offers new firms with the opportunity to offer and scale up services without the traditional level of business investment and resources. It also suggests that established firms with legacy infrastructure and practices will be slower to adapt to new systems based on machine learning.

Applications like blockchain are to some degree in their infancy, although firms report that the prospects of future developments are strong.

This sector is at the forefront of machine learning including the expansion of biometric analysis such as facial recognition technology; the use of artificial intelligence to analyse large amounts of data for audit and risk analytics purposes; and the use of digital signatures to track down and prevent cyber-attacks.

Data security and privacy governance

The firms in this sector rate data security and privacy governance at the top of their priorities lists. As the representatives of one firm noted "we think it is impossible to conduct business without data security and privacy management. ... We believe that proper security management and prompt response to changes will give us a competitive edge".

Firms manage the security and privacy of their client's and their own data in the following mix of ways:

- Ensuring their policies, procedures and practices are consistent with international quality assurance instruments governing data security and privacy. This is primarily achieved by firms ensuring they are compliant with ISO27001 and BS10012.

- The systematic and regular review of local laws and regulations governing data security and management to ensure compliance. These local laws include Personal Data Protection legislation in China; Japan; the Philippines; Singapore; and Viet Nam. It also includes industry specific legislation governing data management activities of their clients.

- Applying a sophisticated and comprehensive data governance framework which consists of firstly classifying all data according to its sensitivity and secondly restricting access within the firm to data according to levels of sensitivity.

- Regulatory compliance and cyber security awareness and best practice training for all staff involved in handling business and customer data depending on the level of data staff members are authorised to manage. Various staff within each organisation are responsible for handling and managing data including its reporting, security and privacy.

- Managing data flows within secure, transparent and auditable frameworks. This includes assessing the most secure and trusted hardware and location when choosing storage infrastructure; employing their own cyber protection teams which are heavily involved in the design and operation of selected hardware and the flow of data; and applying end-to-end encryption on all data flows across borders and over the Internet.

Brand trust from good data management

All firms report that brand trust from good data management is crucial to their business models. In this regard firms in this sector often go beyond the standard requirements in terms of government regulations on data protection. For example firms in this sector commonly adopt self-regulation practices in the form of ISO accreditation (eg ISO 27001) or other international standards setting compliance.

If there are higher level accreditation or certification opportunities that exist with government regulated rules these firms often are at the forefront of those processes. For example some have made the point of getting additional registrations under the domestic privacy legislation in their jurisdiction, like that under the Personal Information Protection Laws in Japan.

3.4. How policies and regulations are impacting their business models

Applicable data regulation and compliance costs

Firms in this sector are subject to all or most of the privacy legislation applied in individual member economies within APEC. Several firms are also subject to the European Union *General Data Protection Regulation* (GDPR) because EU residents are amongst their customers. A small number of firms abide by APEC Cross Border Privacy Rules (CBPR).

Direct costs

Firms report various significant direct costs associated with regulatory compliance of the kinds explained in Table 12 below

Table 12. Kinds of compliance costs reported by firms

Kinds of compliance costs	Examples
Recruiting specialised staff to improve compliance and/or reduce risk.	• Employment and/or contracting cyber security to oversee the design and management of hardware and processes to gather and store information.
Investing in new infrastructure and information technology architecture to improve compliance and/or reduce risk.	• Investment in compliant information management hardware and software, data programming and cloud based or local information storage solutions.

Source: Consultation with firms

Most firms do not believe that compliance with the GDPR is a particularly additional burden. Most firms report that their previously designed processes, often based on ISO 27001, have met the new rules with minimum change. However, that is not to say that the overall compliance costs are small. All firms regard compliance as a significant business cost.

Opportunity costs

Regulatory restrictions can create opportunity costs to firms in this sector. However as noted elsewhere in this chapter the firms believe that the benefit of much of the regulation to building trust is to their overall benefit. Nevertheless, there are significant concerns related to restrictions under various cyber security laws. Opportunity costs are described in the table below.

Table 13. Opportunity costs reported by firms.

Kinds of opportunity costs	Examples
Reduced trading and diversification into international markets.	• This occurs when data laws in individual jurisdictions are not aligned and some impose mandatory requirements that exceed others, such as demands for local data storage or compulsory sharing of firm data with governments.

Kinds of opportunity costs	Examples
Decreased competitiveness in one or more markets.	• The cost implications of complying with data regulation are related to the scale of the business, the extent of its customer base, and the specific features of online payment systems.
Reduced their investment in and/or capacity for innovation.	• Capital expenditure envelopes for business are finite and the mandatory component of data regulation necessarily diminishes the commercial component. For some of the firms in this sector there can be relatively large capital investment for the comprehensive networking of large corporations or government agencies

Source: Consultation with firms

The benefits of regulation

All firms regard government regulation as an overall benefit for them although they are well aware of the cost burdens. Recent worldwide concerns about the abuse of data ranging from the Cambridge Analytica scandal with Facebook and the lingering concerns about "fake news" allegations were repeatedly mentioned by participants in interviews as events that needed to be counteracted to rebuild/maintain trust in the use of digital data. There had been a noticeable increase in the overall concerns of their customers – not in their own products – but in the reputation of the whole digital/e-commerce sector. Good governance and processes were seen as critical in maintaining trust.

Concerns with current regulatory approaches

Regulatory scope

As a general proposition, firms were satisfied with domestic privacy rules. As it was noted by one firm - "we think that if regulations are tighter than the current one, businesses will have difficulty in meeting them. If the current regulations are relaxed, the reliability of them will fall below the level of regulations in other economies".

As another firm stated: "we actively follow domestic and international laws and policies and highlight [this] to [our] customers for improved confidence and the creation of business opportunities".

Having noted that, there is an overall concern with jurisdictional restrictions on such activities as cloud computing and the requirement that servers be located in "home" jurisdictions.

Regulatory alignment

Most firms expressed general concerns about the multiplicity of data protection rules. As one firm noted - "we hope that the laws of each economy, CBPRs, GDPR, ISO and other regulations will be unified as much as possible. It costs much and increases burdens on firms to investigate different regulation systems and find differences in order to satisfy them".

As another firm noted - "at a basic level we create our policies with the aim of ensuring compliance with all legal constructs. While keeping up with legal changes may be a challenge, compliance is vital. We simply have to take the necessary steps to maintain it".

As noted elsewhere in this chapter most firms are not troubled by the introduction of the GDPR. However that does not mean that there were no costs. As one firm reported - "we cancelled some transactions in order to ensure stricter policy compliance and proper contract performance, although the cancellations did not have a substantial overall impact on business".

Another firm stated that - "we want the authorities to standardize personal information protection measures to the fullest extent possible. Ideally the regulations would classify information by importance: [eg] 'important personal information' and 'less important information'.

Regulatory barriers

With respect to cloud based computing, some participants commented about the cyber security laws of an APEC economy. There are also some concerns that other APEC economies may follow suit. For those firms with customers in the financial services space, an equal concern about various laws in another APEC economy were also raised.

One firm stated that - "localization is gaining momentum in many economies around the world, creating the need for a variety of future countermeasures". What those countermeasures would be were not stated. But the worry is that they would escalate into some sort of tensions between economies.

Another firm also noted that they were "once required to disclose source code of our wireless communication devices by a [non-APEC economy] which caused us to stop customs clearance of our products".

A firm also mentioned about domestic promotion laws. It was noted that "in some cases we are not enjoying the same regulatory treatment as local business in some economies where government promotes policy of giving priority to buying products of their own economy over foreign ones.

Preferred regulatory approaches

Firms collectively supported strong privacy laws as they saw them as building trust in the business, and wider community, in digital data management. Without that trust firms consider that their market opportunities will narrow. Generally speaking there is an acceptance of the type of privacy principles set out by the OECD and subsequent rules by APEC and the EU. While it is acknowledged that such rules can impose costs, the value of these rules is largely seen as off-setting the cost burden.

There was a general concern about the restriction in some economies of cloud computing services. In particular there was concern about the demands in some jurisdictions that the geographical positioning of servers containing information on their residents be situated in their jurisdiction. This was seen by all firms interviewed as a major restriction on trade and a large red tape burden. In some cases it severely restricted firms' willingness to locate or conduct business in the relevant jurisdiction. There was a concern that a number of jurisdictions were adopting such rules and that there may be a cascade of increased regulation across APEC.

A number of firms looked favourably on APEC becoming more involved in ensuring that government regulation across jurisdictions were harmonised and that APEC may also assist in explaining cross-border differences to the business sector in member economies. There was also a view amongst a number of firms that the WTO had a similar role to play.

For those firms that were aware of it, there was particular mention of the recently agreed TPP 11 and its chapter 14 on Electronic Commerce. Amongst these firms there was agreement that this chapter was a significant and welcome development and that it should be replicated in future trade agreements.

There was not a significant awareness amongst firms about the APEC Privacy Framework and CBPR.

CHAPTER 4: PAYMENT SERVICES

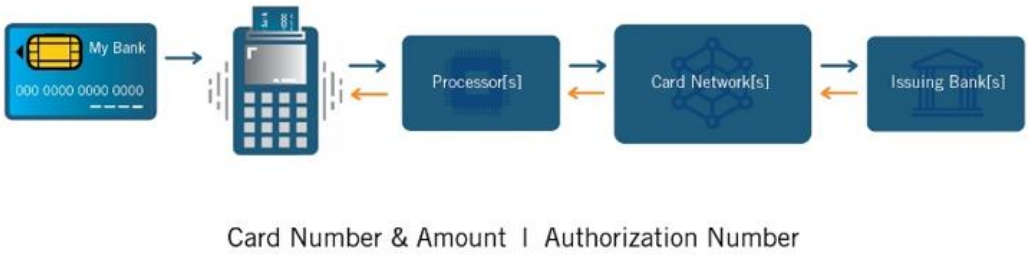
4.1. Sector overview

Technological innovation has dramatically changed the payment services sector. Established firms are developing and adapting new technology in order to defend and grow their existing business. For example, traditional banks are providing end-to-end services across the banking and payments value chain, including through new collaborative payments ecosystems with different industry stakeholders (Capgemini, 2017). Meanwhile, new market entrants (such as fintech firms) are competing to provide new means of payments, often as part of a broader set of digital services (McQuinn et al, 2016). Chinese payment companies offer the best examples of how payment fintechs are using consumer data in ways that differ significantly from established players (Chorzempa, 2018). At one end of the spectrum of new firms is the Chinese firm Tencent, which leverages a complete view of a consumer's behaviour from a broad ecosystem of services (including social, entertainment, news, literature, gaming, sports, and other fields). This gives its integrated payment service a considerable advantage as, on average, 55 percent of a typical Chinese consumer's mobile time is spent interacting with Tencent's services (Whitler, 2018). At the other end are many fintech payment providers (e.g., Stripe, Ayden, Square, etc.) that have developed a niche within the current system (i.e., hardware provider, acquiring services, gateway services, etc.) that have a much different view and use of data for payment services (as compared to Tencent).

Payments are no longer about physical interactions at the point-of-sale (POS). For example, by creating a wholly digital self-checkout, Amazon's physical stores allow customers to skip the traditional point-of-sale completely. Customers expect greater flexibility, functionality, and control over the point-of-sale, especially via smart phones. Overall, there is a clear trend in the payments space toward new partnerships and the use of agile technologies (such as application programming interfaces and web-based tools) and data analytics so that firms are able to provide a more personalized, secure, and seamless service to customers, who are using a growing range of devices and methods to manage payments.

Payment cards (debit, credit, and prepaid cards) continue to play a central role in digital trade given their wide acceptance and use for online payments. Basically, for payments to occur within a card network, an interbank processing platform connects payment card issuers and acquirers (typically banks), which allows the exchange of payment card transactions by a bank's cardholder with another bank's merchant, ATM, or other card-accepting device. Interbank settlement of cross-border transactions typically involves traditional banks relying on an international payment network establishing a multi-bank net/debit position (BIS, 2018). With payment cards, the business model is generally defined as being either a three- or four-party model, in terms of describing the relationship between card providers and banks, cardholders, merchants, and the payment networks. In the case of the four-party model (see Figure 8), the issuer (a payment service firm) provides the consumer with an account (debit, credit, or prepaid), which can operate via a physical card, a smart phone, or online only. The consumer selects products to buy from a retailer, who submits the transaction to the acquirer (mainly banks). The acquirer submits the transaction to the issuer for approval, who (if it approves) remits the retail price to the acquirer, less an interchange fee, who pays the retailer (less a merchant service charge). Finally, the consumer's account is debited the transaction amount.

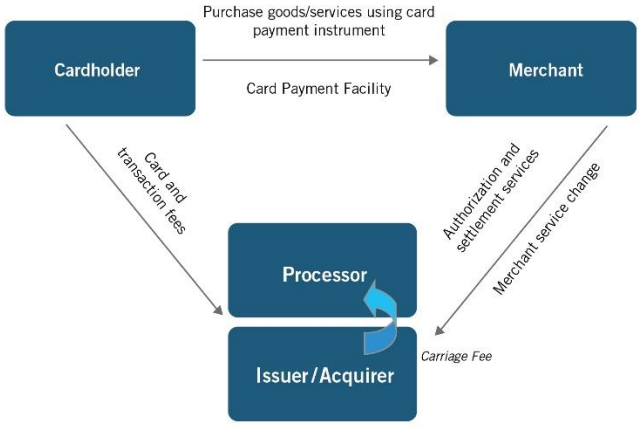
Figure 8. How a typical transaction flows through the four-party model for payment services, which involves merchants, acquirers, issuers, and schemes



Source: Firm A

In a three-party model, the payment service firm acts as both the issuer and the acquirer (see Figure 9). In both models, payment services data flows between these stakeholders as each seeks to play a specific role in facilitating a purchase. However, the sector is undergoing significant change. For example, many banks that issue cards are becoming more digital by offering virtual prepaid, debit, and credit cards for the first time, in order to give customer access to e-commerce solutions.

Figure 9. How a typical transaction works within a three-party payment model for payment services, where the payment firm is both the issuer and acquirer



Source: Firm A

Established payment service providers are coming up with new relationships with merchants in order to access a greater range of data. At the heart of payment providers' traditional business model was the basic service involved in facilitating payments, for which they earned interchange fees. However, the types of firms engaged in payment services, and what services they offer, is changing. A broad range of non-bank and fintech start-ups have entered the sector. This includes, for example, mobile money and financial services like Paytm in India, Stripe in the United States, Go-Pay in Indonesia, True Money in Thailand, Mynt in the Philippines, Toss in Korea, and Alipay in China (and beyond). Also critical for these payment/financial services providers is their integration within the broader digital ecosystem, especially e-commerce marketplaces, email platforms, and mobile apps and app stores. These services also go beyond payments and money transfers, to include a financial dashboard, credit score management, customized loan/insurance plans, and investment services. For example, Go-Pay, (part of ride sharing and on-demand services platform Go-Jek) in Indonesia, provides cashless payments via in-app services, peer-to-peer transfers, and QR code payments at brick-and-mortar stores (Fintech Ranking, 2018). At the same time, established firms are seeking to seize the opportunities through

innovation or partnerships with startups, which is happening all over the world and is seen as a win-win for both sides (Global Payment Innovation Jury, 2017).

Payment services and digital trade

Electronic payment services and digital trade have an intertwined, mutually supportive relationship as consumers want payment services to seamlessly handle the considerable challenges of managing cross-border payments across a diverse range of e-commerce marketplaces, while maintaining a high level of security and privacy (Gefferie, 2018). Payment services represent a critical part of the suite of online services (such as two-sided marketplaces, search functions, or customer review processes) that together make it much easier and cheaper for firms of all sizes to access customers and business partners from around the world, which in turn provides customers with greater convenience and choice. Ensuring that local firms have easy and cheap access to new, low-cost, and innovative electronic payment options is critical to connecting domestic firms with foreign customers. Innovation continues to change how this intermediary process takes place. While digital payments can be made via one of the established card networks (e.g., Visa, Mastercard, or American Express) and card-based point-of-sale devices, they are increasingly being made via mobile apps and devices provided by a growing range of online service providers, such as non-banking institutions and fintech start-ups (Marchetti, 2018).

Quantifying the growth of payment services and their impact on digital trade is difficult. Comprehensive and comparable data on cross-border payments are challenging to compile due to the absence of a common terminology and methodology and an absence of coordinated, large-scale data collection efforts (Marchetti, 2018). Regardless, a number of indirect measures which suggest the rapid global growth in international digital trade and e-commerce (and international remittances and other processes) indicate that the payments sector plays a large and growing role. In 2017, eMarketer estimated that global retail e-commerce sales reached USD2.3 trillion, a 24.8 percent increase from 2016. Of this, mobile-based e-commerce comprises an estimated 58.9 percent of all digital sales[69]. This is further supported by a surge in parcel volumes around the world, which increased 48 percent between 2011 and 2014 (WTO, 2015). There remains considerable room for payment services to drive further digital trade and e-commerce growth. An increasing number of developing economies are moving large numbers of people over to digital payments from their traditional use of cash. For example, formal banking reaches only about 40 percent of the population in emerging markets, compared with a 90 percent penetration rate for mobile phones (Beshouri and Gravrak, 2010).

4.2. Profile of firms interviewed

Firm A

Firm A is a U.S.-based, multinational financial services company involved in facilitating a significant number of transactions annually. Firm A has data centers in multiple regions around the world. Firm A's electronic payments services provide consumers with convenient and secure access to their funds, reduces cash and check handling for merchants, and expands the pool of customers able to engage in domestic and international transactions. Consumers can use Firm A to make electronic payments with credit, debit, and prepaid cards—and other devices, including smart phones.

[69] "Mobile Is Driving Retail Ecommerce Sales Worldwide," eMarketer Retail website, January 29, 2018, https://retail.emarketer.com/article/global-ecommerce-topped-23-trillion-2017-emarketer-estimates/5a6f89f5ebd40008bc791221.

Firm A's services are part of the changes that are blurring the lines between digital and physical commerce, with omni-channel experiences becoming the norm. Firm A is involved in data-driven innovation as payment services continue to change. For example, real-time payments are one part of the next wave of digital payments growth as on-demand services and new ecommerce platforms integrate sellers, hosts, drivers, freelancers, and developers needing fast, convenient and secure access to funds.

4.3. Role of data in firms' business models

Data is critical to each step in capturing, processing, and authorizing a transaction as electronic information (e.g., about the customer, the merchant, the purchase, etc.) is exchanged between the various stakeholders. Although the core function of the data is ensuring that a customer's funds are transferred to the merchant in exchange for a good or service, this is only one role of data in today's digital economy. Every interaction that Firm A's services are involved with generates data, which when analysed in aggregate can yield significant insights. This process at Firm A is indicative of the value chain associated with "big data," which can be generally described as: raw data, aggregated data, intelligence, insights, decisions, operational impact, financial outcomes, and finally, value creation.

For payment service firms, the first few steps of this process come from the traditional and structured data they provide to merchants that aggregates and summarizes their transactions (from a particular day or time period). Other common data used by financial institutions include: identity and demographic data (e.g., ID, age, nationality, address, education, professional details), transactional data (e.g., payment account movement (credits and debits)), payment obligations (e.g., to evaluate the debt service ratio and the remaining net income), behavioural performance data (e.g., credit incidents, debt falling due, potential debt), website, device, and mobile app usage, and the perception of the financial institution's service level (e.g., customer expectations and satisfaction/complaints) (Papp, 2019).

In the middle and final steps of this data analytics process, firms bring artificial intelligence and data science tools to bear in combining and analysing this traditional data with alternative and unstructured data sources, such as voice and message service usage data, social media, satellite imagery, emails, mobile applications, and personal devices. These data analytics processes also highlight the fact that for payment providers to be competitive, itis not enough to focus on lowering the cost of each transaction, but rather using the full spectrum of data and advanced data analytics to provide value-added services to customers, merchants, and others.

In the case of Firm A, it uses aggregated, anonymized data to help retailers understand a consumer's experience before and after visiting a retailer so as to better understand what needs are clearly being met and where the retailer may be missing opportunities. Firm A's use of AI is indicative of the broader trends in the financial services sector. For example, an estimated 53 percent of large merchants and banks in Latin America use artificial intelligence and machine learning technologies (Visa, 2019). Alibaba (which has extensive payment service operations) also provides an example that applies to Firm A's general approach in working with merchants to use technology and payment services to add value for their business. In exchange for a signup fee and a commitment to buy their inventory through Alibaba, the firm gives Chinese retail store owners extensive data collection infrastructure. For one local corner store merchant in China, it led to a 30 percent increase in revenue for the year. Alibaba has achieved a similar transformation, with over one million other small stores and a growing number of larger, "superstores."[70]

[70] Levine, Steve. "China's AI-infused corner store of the future," Axios, June 17, 2018, https://www.axios.com/china-alibaba-tencent-jd-com-artificial-intelligence-corner-store-df90517e-befb-40ca-82d5-f37caa738d54.html.

Personal data is central to data analytics and payments services at Firm A and throughout the sector. Payment services firms like Firm A may use personal data for a number of purposes, including to process payment transactions; to protect against and prevent fraud; and to provide the customer with personalized services and recommendations. Personal data is also shared, for instance, with third parties for fraud monitoring and prevention purposes, as well as those who provide auxiliary services with the customer's consent.

In a way, consumers' concerns over data privacy and protection affect the payment sector's use of data and hence service offerings. A survey for one of the world's leading payment providers showed that 27 percent of respondents stated that privacy and personal data protection was a key driver in trying a new payment method (Visa, 2019). What this highlights is that while consumers appreciate the ability to tailor every experience to suit their individual preferences, their concerns about personal data influence their decisions about whether to take advantage of these data-driven conveniences.

4.4. How policies and regulations are impacting firms' business models

Payment services are affected by several types of data-related laws and regulations:

- Regulations and restrictions about payment services data and its processing, transfer, and storage;
- Regulations about the collection and use of certain categories of data, including personal data;
- Regulations regarding government access to payment services data;
- Market entry requirements (e.g., licensing).

While the Internet may be global, domestic laws and regulations can seriously affect the role of payment services in digital trade. The cross-border payments process is complex, involving many different parties and underlying arrangements that all differ by jurisdiction. This is made all the more difficult as the financial services sector, which includes payments, is typically among the most heavily regulated areas of an economy. Divergent, restrictive and burdensome regulatory frameworks translate into costs, complexity, and lost economic opportunities for firms and customers to use cutting-edge payment services to access the global digital economy.

Rules and laws pertaining to data are critical to payment services, as the collection, processing, storage, and transfer of data is central to the delivery of the service itself and to the analytic processes firms use to improve customer service, drive market insights, and, ultimately, to extract economic value from data (IFC, 2017). This is evident in the fact that payment networks clear and settle transaction information, not funds. A central issue for payment services and global digital trade is that while technological innovation and changes in consumer preferences mean that payment services are rapidly changing, economies are at different stages in updating regulatory frameworks. Understandably, regulatory agencies that are responsible for consumer protection, financial stability, and other public interests are grappling with the legitimate challenge of updating policy frameworks to account for technological innovation and changes in consumer behaviour. For the purpose of this chapter, economies can generally be categorized into three main groups: those undertaking reforms which support the development, deployment, and use of payment services at home and across borders; those leaving legacy frameworks in place; and those undertaking reforms which may inadvertently undermine cross-border payment services and digital trade.

When economies do not update regulatory frameworks (i.e., legacy frameworks), this can potentially become a barrier to the development, deployment, and adoption of new payment services. Many modern barriers to payment services are due to institutions and regulatory frameworks which need to be updated, such as those pertaining to consumer protection, those restricting the establishment and operation of non-bank payment providers, and those which skewed playing fields towards certain participants in the payments system (WEF, 2018). For example, ensuring mobile money interoperability with the financial

system can be difficult when legacy policy frameworks discourage or complicate the use of new payment methods (WEF, 2018).

Data is already a major reason for existing bottlenecks in digital trade. As part of a Committee on Payment and Settlement Systems (CPSS) survey, respondents noted legal, regulatory, and compliance considerations as the most significant cost and challenge to their business, especially for cross-border payments. In particular, payment service providers cited anti-money laundering, know-your-customer, risk mitigation, and consumer protection requirements (BIS, 2018). Given the cost and complexity of cross-border transactions, respondents cited corresponding "de-risking" by some firms, particularly smaller firms, as they seek to reduce their exposure to certain types of customers and transactions. Furthermore, in terms of compliance costs, respondents confirmed that complying with several sets of rules and regulations as opposed to one added costs. The greatest challenge arose from conflicting jurisdiction rules and when the cooperation among authorities to resolve issues or areas of conflicting interpretation can be further improved (BIS, 2018). This highlights the more "traditional" data-related laws that payment service providers face when engaging in digital trade.

Data-related laws and regulations that support the role and flow of data

Depending on how they are implemented, regulations designed to allow government's access to payments data, especially by financial regulatory authorities, can be a significant impediment to the global provision of payment services. In particular, data localization requirements impede the free flow of data, with implications for the development of integrated, secure, and efficient payments systems worldwide, with consequences for innovation, competition, and economic growth.

At the heart of the issue is that many economies need to update domestic and trade policy tools to ensure that financial regulatory authorities have the confidence that payment firms are managing and protecting data in a responsible manner, and if needed by regulatory authorities, can provide data on request. The issue is that policymakers in many economies are focusing on the location of where payment service firms store data, rather than on the legal framework for ensuring that firms provide access to data in a timely manner (which is an example of regulatory best practice). In many cases, regulatory authorities are requiring local data storage because they believe that this is necessary to ensure government's access to the data. In the era of cloud computing, however, data can be provided with a few clicks of a mouse button.

The European Commission's (EC) efforts provide a useful example. As part of its efforts to build a digital single market, the EC is working to remove barriers to the transfer of company, tax, bookkeeping, and financial data, and asking that member states focus on mandating access[71]. For example, in 2015, Denmark changed its local data storage requirement for accounting data such that firms could store their data anywhere, as long as Danish authorities were given easy access to data on request[72]. This is where the focus should be: putting in place the legal framework to ensure firms provide data to regulatory authorities in a timely manner.

Similarly, the United States' experience with ensuring regulatory oversight of financial firms' IT systems and ability to provide data could serve as a good example for other economies dealing with concerns over access to data. The U.S. Treasury and financial regulators recently reconsidered a policy

[71] Julia Fioretti, "EU looks to remove national barriers to data flows," Reuters, September 29, 2016, http://www.reuters.com/article/us-eu-data/eu-looks-to-remove-national-barriers-to-data-flows-idUSKCN11Z19Q.

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

that would have allowed data localization for financial data, but instead enacted a policy framework that focuses on maintaining access to data. U.S. regulators' concerns were based on their experiences in the global financial crisis when they had issues getting access to data in key banks' (such as Lehman Brothers') IT systems during bankruptcy proceedings. The U.S. Federal Reserve and Federal Deposit Insurance Corporation's (FDIC) ability to use and analyze Lehman's IT systems and data was reportedly hindered as the bank's network became fragmented, overseas subsidiaries were sold off, some IT systems in overseas subsidiaries were turned off, some key IT staff departed, and restrictions on data flows were imposed due to insolvency filings in other economies—as was the case when the United Kingdom's financial regulator took over Lehman Brothers' European division[73]. This made it difficult for the regulators to access the data needed to unwind positions and ascertain what money was owed to whom[74]. However, subsequent legal reforms (e.g., the Dodd-Frank Act, enacted in 2010) have addressed these concerns by focusing on how companies disclose to regulators the way they manage their IT and data as part of regular prudential compliance activities..[75]

As it relates to trade policy, the United States-Mexico-Canada Trade Agreement's (USMCA) provisions on financial data flows and regulatory access to data show how economies can address legitimate issues raised by cross-border data flows while allowing the free flow of data as the default and predominant policy approach. In the USMCA, the opening section on the location of computing facilities for financial services (article 17.20.1) focuses on the underlying issue that financial regulators are worried about—access to data, not the location of data storage. USMCA parties agreed to recognize "that immediate, direct, complete, and ongoing access by a Party's financial regulatory authorities to information of covered persons, including information underlying the transactions and operations of such persons, is critical to financial regulation and supervision, and recognize the need to eliminate any potential limitations on such access." Modern cloud computing, which allows transfers of data with the click of a button, enables firms to provide such access, while still allowing firms to move financial data freely in order to provide secure, innovative, globally deliverable services.

---

[73] Rosalind Wiggins and Andrew Metrick, "The Lehman Brothers Bankruptcy: The Effect of Lehman's U.S. Broker Dealer" (Yale Program on Financial Stability Case Study 2014-3E-V1), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2588556; Administrative Office of the United States Courts, "Report Pursuant to Section 202(e) of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010" (Washington, D.C., July 2011); Lemieux, "Financial Records and Their Discontents"; "Lehman Brothers International (Europe) in Administration: Joint Administrators' Progress Report for the Period 15 September 2008 to 14 March 2009," PricewaterhouseCoopers, accessed April 4, 2016, http://www.pwc.co.uk/en_uk/uk/assets/pdf/lbie-progress-report-140409.pdf.

[74] "Lehman Brothers International (Europe)."

[75] "Resolution Plans," Board of Governors of the Federal Reserve System, accessed April 4, 2016, https://www.federalreserve.gov/bankinforeg/resolution-plans.htm.These "living wills" are required to provide a broad range of information relevant to resolution planning and implementation including, for example, detailed descriptions of organizational structures, credit exposures and cross-guarantees, and supporting data. The relevant section on IT and data states: "Management Information Systems; Software Licenses; Intellectual Property. Provide a detailed inventory and description of the key management information systems and applications, including systems and applications for risk management, accounting, and financial and regulatory reporting, used by the covered insured depository institution (CIDI) and its subsidiaries. Identify the legal owner or licensor of the systems identified above; describe the use and function of the system or application, and provide a listing of service level agreements and any software and systems licenses or associated intellectual property related thereto. Identify and discuss any disaster recovery or other backup plans. Identify common or shared facilities and systems, as well as personnel necessary to operate such facilities and systems. Describe the capabilities of the CIDI's processes and systems to collect, maintain, and report the information and other data underlying the resolution plan to management of the CIDI and, upon request, to the FDIC. Describe any deficiencies, gaps, or weaknesses in such capabilities and the actions the CIDI intends to take to promptly address such deficiencies, gaps, or weaknesses, and the time frame for implementing such actions."

The USMCA's central focus on ensuring access for legitimate financial oversight objectives is made clear (through partial repetition) with the subsequent balancing provision that prohibits parties from requiring financial firms to use local computing facilities as a condition of doing business "so long as the economy's financial regulatory authorities have immediate, direct, complete, and ongoing access to information processed or stored on computing facilities that the covered person uses or locates outside the Party's territory." This extends to third-party suppliers of cloud storage or other related services. Each economy also agreed to provide financial firms with a reasonable opportunity to make changes to their IT systems (i.e., shifting data storage from one jurisdiction or another) if they find that they are not able to provide regulators with immediate and ongoing access to data. Such a commitment makes sense if firms realize they are not able to assure access as part of prudential reporting requirements, such as in "living wills" (where firms have to detail how they manage their IT systems and data) which systemically important financial institutions in the United States need to prepare under the Dodd-Frank Act (Cory and Atkinson, 2016). Finally, highlighting the central focus on access to data, the USMCA details that even in the final resort whereby a financial regulator requires a firm to change where it stores data, it does not necessarily mean shifting it to computing facilities in the United States (for example), just to another (third-economy) jurisdiction where regulators know they would have requisite access.

Data-related laws and regulations that limit the role of data: Restrictions as to the analysis, storage, and transfer of payment services data

A growing number of economies are using data-related restrictions as a barrier to market entry and operations for payment service providers. Local data storage, processing, and transfer/routing requirements have a significant impact on payment services firms, especially foreign ones. Barriers that make it costlier, more complex, and/or illegal for payment service firms to export and use data as part of centralized data analytics platforms limit the ability of payment services firms to use data from the broadest range of sources to provide secure, innovative, and standardized services to customers around the world. This was a major impact of laws that have been enacted or considered in several economies including a few APEC members. At the same time, one APEC economy indicated that data localization should be a legitimate policy tool given the absence of global rules on privacy. The economy further added that it is necessary to protect its citizens' privacy and data as well as promote trust in the digital economy.

As an example, one APEC economy has put in place local data storage, processing and routing restrictions for payment services data, along with other market entry restrictions that make operations difficult for international networks. About five years ago, the economy enacted a new payment systems law that requires international payment providers to transfer their processing capabilities with respect to their domestic operations to a local state-owned operator.[76] Requiring firms to use a new, state-owned process raises a number of issues including data processing and security concerns considering that the operator is relatively new and may lack the technical and institutional capabilities to securely connect to and work with payment providers. At the same time, the economy explains that this measure is a response to the fact that the neutrality of international payment providers and their ability to deliver services irrespective of international political climate are called into question.

[76] Federal Law No. 161-FZ "On the National Payment System" dated June 2011 (the NPS Law) as amended in October 2014 by the Federal Law No. 319-FZ "On Amendments to the Federal Law on the National Payment System and Certain Legislative Acts of the Russian Federation."
https://www.dentons.com/en/insights/alerts/2017/march/2/major-russian-legislation-changes-for-2016-banking-and-finance#4

Another APEC economy is considering a law that would require payment services firms to route data through a local, state-owned, payment provider, hence forfeiting their role in delivering value-added services (ITI, 2017). Other economies also do this for certain types of transactions, such as debit card transactions. On the latter, these economies target debit transactions as this category of payment is often supported as part of broader efforts to improve the uptake of payment services.

Other examples of data-focused laws and restrictions that target payment services data include:

- The Law on Payments and Security Settlement Systems, Payment Services, and Electronic Money Institutions requires firms to maintain documents, records, data storage, and processing facilities in Turkey (Fefer et al, 2018).
- The Central Bank of Brazil proposed a cybersecurity policy that would require the local storage of financial data. The cybersecurity proposal would force firms to store their data locally (article 11). The law raises other concerns about the security of data given it required firms to indicate where the actual data centers are located (article 12:1) and that it included a requirement for cloud companies to provide the Brazilian Central Bank with physical access to the data centers (article 12:7) (Atkinson and Cory, 2017).

Some economies are indirectly creating local data processing requirements by using laws and regulations to require all transactions through a single, local "payment gateway," which is often a state-owned or connected firm. Payment gateways are essentially the stage of the e-commerce process where customers enter their personal and payment details to make a payment online (such as during the checkout process). It is equivalent to a physical point-of-sale POS terminal, where customers swipe or dip their chip-embedded card to complete a transaction. Economies are increasingly affecting this step in the processing of cross-border payments as they see it as a critical value-added step from a data analytics perspective which they want a local and/or state-owned firm to control.

Cases shared by Firm A include:

- One APEC economy is implementing a plan to develop its own local electronic payments industry by requiring that all credit and debit payment transactions be processed by a government-owned monopoly[77]. This makes the state-owned firm a direct competitor in the payments sector, while precluding foreign market access[78].
- About a year ago, another APEC economy enacted new rules that effectively prohibit foreign firms from playing a role in domestic payments, as part of its initiative to launch a domestic payment gateway[79]. The new rules require all domestic electronic (i.e., non-cash) transactions to be processed through the domestic gateway. Critical players in the payment network must be appointed or approved by the central bank, must store data locally, and must be 80 percent domestically owned. This includes the "standards institution," which is in charge of creating, developing, and managing the technical and operational specifications (including security and data protection) of the domestic gateway. It also includes the "switching" institution, which is in charge of processing domestic payment transaction data. Prior to this restriction, the economy allowed 100 percent foreign ownership. This is in addition to the Regulation on

[77] "National Payment Corporation of Vietnam," Banking Vietnam website, http://banking.org.vn/2016/national-payment-corporation-of-vietnam/.
[78] "Comments in Response to Executive Order Regarding Trade Agreements Violations and Abuses ," *The Information Technology Industry Council,* 2017, https://www.itic.org/dotAsset/9d22f0e2-90cb-467d-81c8-ecc87e8dbd2b.pdf
[79] "Regulation of Bank Indonesia No. 19/8/PBI/2017 on National Payment Gateway," Bank Indonesia website, November 1, 2017, https://www.bi.go.id/en/peraturan/sistem-pembayaran/Pages/pbi_190817.aspx

Information Technology Risk Management which requires foreign banks and payments networks to locate data centers and process payments in the economy[80].

The impact on data analytics

Firm A generally described how local data storage, processing, and transfer/routing requirements undermine data analytic processes. Furthermore, Firm A outlined how restrictions on payment processes have a similar impact to data localization given that such restrictions act as a de facto market entry and data processing restriction given they prevent foreign firms from accessing and processing payments data. Local data processing or routing restrictions have a significant impact as both policies effectively prohibit foreign firms from bringing to bear a key part of their competitive offering—their globally distributed data analytics platforms. The non-exhaustive description below is indicative of the general impact on data analytics.

A major impact is that these restrictions prevent Firm A from working with global datasets and providing quicker and more effective data-driven services. For example, Firm A outlined how these restrictive policies limit its ability to use data analytics to combat credit card fraud, which is a global problem for consumers, financial institutions, and regulators. Data analytics use behavioural, temporal, and spatial techniques to assess a consumer's behaviour and whether a transaction is out of the normal or not. When a transaction is initiated, hundreds of pieces of information (for example, about the customer, merchant, place, and time, all compared against years' worth of data about prior transactions) are gathered and sent for analysis by the payment processor's predictive model to determine if it is likely a genuine or fraudulent transaction. For Firm A and other large payment providers, this process happens tens-of-thousands of times daily, which ultimately involves billions of pieces of data. These data-driven systems are powerful and fast enough to detect fraud in real time by using models based on historical data (and deep learning) to proactively identify risks. Critically, these data analytic processes improve fraud detection without increasing the number of "false positives," which not only means that firms prevent more fraud, but that they spend less time and money doing it. Similarly, big data analytics is used to detect money laundering disguised as legitimate payments. Ultimately, requiring payment service firms like Firm A to use an artificially altered database for analysis means that they may not be providing the most accurate prediction for customers as it relates to fraud and other activities.

Quantifying the impact of these policies on Firm A and similar payment firms' data analytics in terms of cost is difficult given the diffuse nature of the processes and services affected. Firm A itself struggles to put a figure on the impact or even components of it, even though it can see the myriad ways these restrictions affect its preferred operational arrangements. It is difficult for firms to identify, isolate, quantify, and aggregate the financial (in terms of specifying extra labour, investment in IT systems) and non-financial costs associated with specific data-related regulations (in terms of indirect impact on operations and the provision and development of services). However, the impact of restrictions on data analytics differs from explicit local data storage (to a degree) in that differential costs between local and preferred data storage services provide a clear marker. However, the impact of data-related restrictions on data analytics for payments firms is clearly present. Furthermore, it is comparatively easy to see (from a conceptual basis) that the impact Firm A is grappling with would represent an even larger and costlier challenge for a small or medium-sized firm that does not have the resources or technical

[80] "Comments in Response to Executive Order Regarding Trade Agreements Violations and Abuses ," *The Information Technology Industry Council*, 2017, https://www.itic.org/dotAsset/9d22f0e2-90cb-467d-81c8-ecc87e8dbd2b.pdf

expertise to make the type of technical and operational changes, across multiple markets, that these restrictions entail.

The impact on digital trade

Firm A made the broader point that data-related laws discriminate against and potentially prevent market entry by foreign payment service providers as they affect the IT services used by foreign firms, but less likely to be used by local firms. Local mirroring or data storage requirements create costly and duplicative services, but requirements for local processing raise the cost and complexity to another level.

The impact can be described a sliding scale of restrictiveness and impact (from least to worst)[81]:

- Local "mirroring" requirements require foreign firms to either setup their own local data storage facilities and data processing services or pay a third-party provider for these services. In this scenario, foreign firms capture a first copy of the transaction data for local storage, before transferring it out of the economy for storage and processing in its global IT systems. Such mirroring requirements also affect data analytics processes depending on specific requirements, as they can extend to how firms are/are not able to use and update this local copy.
- Full and only local data storage requirements require foreign firms to either setup their own local data storage facility and data processing services or pay a third-party provider for these services.
- Local data processing or routing requirements (requiring firms to send transaction data to a designated firm) completely cuts off foreign firms from using data that is critical to providing modern services, such as global fraud monitoring and prevention. This can effectively be done in two key ways: when an economy designates a local firm (often state-owned) to be the only payment processor or when they require firms to route all payments through a local (often state-owned) firm. These requirements essentially act as a de facto barrier to market entry as they prevent firms from conducting core, value-added activities as part of their general service offering to customers.

Each of these categories provide an advantage for local payment service firms. As a service that relies on data and digital technologies, these requirements pose significant issues for payment service firms, especially foreign ones, which rely on the Internet to operate centralized, low-cost, and highly sophisticated IT systems. Payment providers leverage data analytics and cross-border data flows to be as cost competitive as possible and to help make transactions safer, more convenient, and overall, more valuable for the customer and the merchant, including through innovations such as contactless payments and electronic wallets.

In the scenario that an economy requires a payment services firm to only process data locally, it requires the firm to deal with the challenge (which may not be fully feasible) of seeing if it can download and replicate (to some extent) its global data analytics platforms into a local ecosystem (i.e., an IT system within an economy's borders). Such a scenario raises ongoing operational challenges as to the relationship between the local analytics platform and the global one and how to keep the former as updated (secure and effective) as possible (even though it will not benefit from the insights derived from a broader, global data set). These problems are compounded if the firm has to manage this issue across multiple economies.

These requirements tend to be discriminatory as local firms are more likely be only operating in their home economy and are therefore happy to comply with local data storage measures. Local firms are

[81] Based on information obtained during an interview with an industry expert.

also less likely to be concerned with the impact that local data storage and processing may have on business efficiency (e.g., spending more for IT services) as to their primary goal only be to capture local market share (rather than be globally competitive and innovative).

Local data storage and processing requirements act as a barrier to entry as payment service firms have to assess whether it is worthwhile for them to enter a market given the cost and complexity involved in making potentially costly and complex changes to global IT platforms and services. In some cases, a foreign payment firm may decide to enter or continue operations, but decide that data-related restrictions mean it cannot provide its full suite of services. For example, local data storage may mean that it cannot provide global fraud prevention services to a local market, as it is not able to integrate data from around the world to a local market. In other cases, a foreign technology firm may decide to not enter (or to exit, if already present) a market, as the initial and ongoing technical and operational costs simply outweigh the potential benefits. For many foreign firms, this type of regulatory assessment is becoming increasingly common, as they need to weigh up the aggregate cost and complexity that comes from making a number of iterative changes across individual economies.

The impact on local economies: cost and availability of best-in-class data services

The increased digitalization of organizations, driven by the rapid adoption of technologies such as cloud computing and data analytics, has increased the importance of data as an input to commerce, impacting not just information industries, but traditional industries as well. Beyond the impact on trade, localisation requirements which affect a key data-dependent service—such as payments—will ripple throughout a local economy in several ways[82].

Given their central role in facilitating economic activity, the effects of a less-efficient, competitive, and secure payments services sector will ripple through an economy in the form of reduced firm competitiveness and economic productivity. Local data storage and processing requirements are likely to result in some foreign firms not entering a market, not offering their full suite of innovative services, or inhibiting their ability to provide their best products/services given their inability to transfer or process data on centralized IT platforms (the section below examines cases involving fraud detection and cybersecurity). Companies may also be compelled to spend more on compliance activities, such as hiring a data-protection officer, or putting in place software and systems to get individuals' or the government's approval to transfer data.

Furthermore, localization requirements for payments data further complicates a service that firms in many economies already rank as a major challenge in terms of engaging in digital trade. For example, an International Trade Center survey identified international e-payments as the largest bottleneck in the process chain for e-services exporters, as compared with other elements such as establishing an online business (ITC, 2017). Furthermore, 23 percent of 2,200 micro, small, and medium-sized enterprise respondents engaging in e-commerce in more than 100 economies identified inadequate "links between third-party e-payment service providers and local banks" as a top e-payment obstacle (ITC, 2016 and 2017). Another recent survey of merchants in 15 emerging economies in Latin America, Asia, and Africa identified e-payments as a moderate obstacle to e-commerce, and one that was more problematic for small firms (Suominen, 2017).

[82] Based on information from discussions with an industry representative.

Measures that restrict payment services data may lead to digital platforms, such as e-commerce marketplaces, not entering certain markets as it prevents them from using their preferred payment service(s) they include as part of their broad suite of services, such as advertising and logistics. It is not hard to see the potential complications that arise for digital platforms that bring buyers and sellers together across dozens of economies having to re-evaluate their local operations if they have restrictions as to if/who they can use for payments in each and every market. Depending on the platform's decision to enter or not, this would mean local firms would be potentially prevented from accessing the enormous benefits that come from using platforms to easily and cheaply access customers around the world.

These additional costs are either borne by the customer or the firm, which undermines the firm's competitiveness (especially for foreign firms which are at some disadvantage vis-a-vis domestic firms) by cutting into profit margins. It also means that the broader economy will likely suffer as the local payments sector will be less competitive (in terms of price and service offerings) if foreign firms decide not to enter, as local firms will face less pressure. The cost to firms of complying with restrictive data governance arrangements are not limited to money, but extend to broader growth and expansion, as implementing operations to comply with local data storage requirements often requires lead time of months, even years. In addition to disrupting the broad shift from paper-based payments to electronic payments in economies around the world, these policies may undermine the significant economic benefits that research shows comes from this transition in payment methods[83]. For example, McKinsey & Company has estimated that the shift from cash to digital payments could increase GDP across developing economies by 6 percent before 2025, adding $3.7 trillion and some 95 million jobs (McKinsey Global Institute, 2016).

Firm-level competitiveness is also affected as local data storage and processing requirements may prevent local firms from accessing and using best-in-class data analytic services (wherever these may be based and whatever broader platform they may be part of, such as e-commerce marketplaces). For example, it may prevent firms from using data analytics to increase customer activity, such as through targeted marketing programs, predictive modelling of consumer behaviour, and other new customer targeting techniques. For example, at its broadest level, big data analytics allow payments providers to create a more detailed, comprehensive, and single view of a customer. For example, it can help firms improve their customer segmentation, targeting, and sentiment analysis. China's Ping An established a big data analytics platform in 2013 to improve cross-selling and customer migration, with the goal of "one customer, one account, multiple services, and multiple products."[84]

As the chapter on data analytics outlines, today's economy is increasingly dependent on how firms use data, and if local firms are prevented from using the best services, this will affect their success in today's increasingly data- and artificial intelligence-based economy (New, 2018). In a similar way, local data storage and processing requirements may also undermine data-driven innovation. Organizations use data to create better insights, which, in turn, lead to innovation. Businesses use data to enhance research and development, develop new products and services, create new production or delivery processes, improve marketing, and establish new organizational and management approaches (Reimsbach-

[83] For a literature review of the research which shows the economic benefits of electronic payments: Wilko Bolt and Sujit Chakravorti. Digitization of Retail Payments. (Amsterdam, De Nederlandsche Bank, December, 2010), https://www.dnb.nl/binaries/Working%20paper%20270_tcm46-243674.pdf.

[84] "Seven critical changes to payments industry as FinTech matures," Payments Cards and Mobile website, January 17, 2017, https://www.paymentscardsandmobile.com/seven-critical-changes-payments-industry-fintech-matures/.

Kounatze and Van Alsenoy, 2013). By making it harder and more expensive to access and use cutting edge data-driven services, economies may prevent local firms from extracting valuable insights from their data. Furthermore, it may affect the number and cost of data analytics services available in an economy, which may lead to fewer firms using such services (as cost is a key determinant of ICT adoption and deployment), which will affect data-driven innovation across an economy. In line with this, the OECD has found that the probability of innovation increases with the intensity of ICT use (OECD, 2010).

Similarly, by inhibiting competitiveness at home, economies may inadvertently cause their firms will be less competitive and innovative than those companies that compete without protection and at scale. Economies of scale for payment services, like many parts of the digital economy, are critical, as payment systems require considerable up-front investments in processing infrastructures, highly secure telecommunication facilities and data storage, and apply complex operational standards and protocols. As a consequence, it is critical for firms to achieve a large volume of payment transactions in order to reduce per unit costs (Bolt and Chakravorti, 2010). The Global Payments Innovation Jury Report of 2017 (a survey of 70 industry executives from around the world) shows how this is already a major issue in that it cites the inability to scale as the biggest reason payments start-ups fail (26 percent of respondents), followed by regulation (in third place with 15 percent). For policymakers who want to support local payment providers, it is critical they implement a policy environment that makes their firms competitive at home while also facilitating economies of scale by ensuring they are able to enter into and compete in foreign markets. Local firms in economies enacting local data storage and processing requirements will inevitably face the same disadvantages as foreign firms do in their local market if local data storage and processing rules for payments data become the norm around the world.

Ultimately, local data storage and processing requirements will likely lead to less efficient and less competitive local and regional payment markets. And this hurts all firms in an economy, because it raises their costs and/or forces them to use inferior services. In other words, when policymakers enact data localization laws to support one sector of their economy, they inadvertently end up affecting the other sectors of their economy. This issue is compounded by the fact that there are no significant regional initiatives to coordinate approaches to e-payments regulations (Cullen International, 2016). For example, in Latin America, e-payment solutions tend to be highly localized due to cross-border regulatory friction that in turn affects cross-border e-commerce. Likewise in South East Asia, cross-border bank payments among Association of Southeast Asian Nations (ASEAN) member economies remain complex due to reasons such as currency conversion costs, volatile exchange rates, significant variations in Internet speeds, and the absence of basic payments infrastructure systems in some economies and the lack of a common messaging standard[85].

The impact on local economies: detracting from foreign investment

In today's interconnected global economy, firms which have data at the center of their business model will take into account local data governance requirements as part of their regulatory due-diligence when considering global investment decisions. Local data storage or processing requirements signal to high-tech firms (whether in the payments sector or elsewhere) that an economy may not be truly committed

[85] HSBC. Payments in ASEAN post AEC. Available at: https://www. hsbc.com.my/1/PA_ES_Content_Mgmt/content/website/commercial/ cash_management/PDF_141107/5-Payments-in-ASEAN-post-AEC. pdf.

to supporting globally competitive and innovative data-driven firms[86]. Firms are less likely to commit the capital to invest in local research and development centers, global data processing centers, and other data-related facilities if they perceive that policymakers are likely to restrict the movement of data. Econometric modelling on the impact of data localization provides an indicative estimate as to the reduced level of investment that results from an economy that takes a restrictive approach to data flows. A study of potential data localization measures in several economies shows that the effects on GDP, investments, and welfare from data-related regulations are too considerable to be ignored in policy design (Bauer et al, 2014). If policymakers want to tap into foreign investment, technology, and know-how, they need to account for how their regulatory framework manages data-related issues, as these firms have the ability to setup operations in a broad range of economies to service foreign markets.

The impact on local economies: increased security risks

Economies requiring local data storage or processing affect the ability of payment service firms (and other tech firms) to use best-in-class technology and methods to protect and secure data and their IT systems[87].

Local data storage requirements means that all transaction data may only be stored in a single data center or only distributed over a small number of data centers. By requiring firms to use only local data services, economies enacting data localization may prevent firms from using best-in-class cybersecurity measures. This is a major potential issue, as cyber threats and fraud are on the rise with increased adoption of mobile payments and wearable devices leading to a loss of consumer trust as well as financial losses. Payment firms have to continuously invest in advanced authentication and enabling technologies (such as biometrics, secured element and tokenization, geo-location based authentication, and cryptographic keys) to stay ahead of hackers and cybercriminals (Capgemini, 2017). Local data storage and processing requirements may prevent firms from using modern techniques for storing data, such as "sharding," which involves breaking up data and storing it in multiple locations, or constantly moving it between different data centers in different economies.

Also, requiring firms to store data locally creates physical risks (and substantial costs) as firms may have to setup multiple data centers as part of a largely self-contained IT ecosystem within an economy in order to provide backup, redundancy capabilities to ensure data remains secure in the event of a natural disaster, power outage, or other such emergency which could take a data center offline.

Local data storage and processing requirements also prevent payment service firms from providing the best-possible fraud detection services to clients, as they are not able to feed local data into global systems that constantly monitor for fraudulent transactions, which are not limited by borders. It is now common for leading payment service accounts to have fraud management tools which score transactions based on insights from millions and billions of worldwide transactions. For example, if an odd transaction in New Delhi, India is found to be fraud, the global platform would learn from this. A similar transaction in Santiago, Chile the next day would be blocked (based on an assessment of a client's transaction history, it would lead to a higher fraud score that will cause the transaction to be declined). Firms use artificial intelligence to constantly assess transactions in real-time (Chakravorti et al, 2017). Firms are investing a growing amount of funds into developing machine learning solutions for fraud detection. Indicative of this, 68 percent of North American financial institutions (surveyed in a 2017

[86] Based on information from discussions with an industry representative.
[87] Based on information from discussions with an industry representative.

study) cite machine learning analytics as a high priority investment to help fight fraud. However, for firms to build fraud models and gain insights for fraud prevention, payment service firms need unimpeded access to their global platform and data sets from around the world. In a similar way, local data storage laws may prevent firms from being best prepared to defend against the full spectrum of cybersecurity attacks (in terms of being able to use data from global operations so that all systems reflect global best practices)[88].

4.5. Conclusion

Some data-related laws and regulations may add cost and complexity for payment services, which is a sector that already faces a significant compliance challenge from being subject to significant legal and regulatory requirements for financial services in multiple jurisdictions. This is why cross-border payments are generally more complicated and expensive than domestic payments. Adding data-specific issues adds a further distinction between domestic and foreign providers given that the latter tend to rely on centralized IT systems and data transfers to operate across multiple markets. By enacting policies which target cross-border providers as well as processing of payment data (including firms which are allowed to do so), these economies are affecting a key facilitator of digital and traditional trade.

[88] Based on information from discussions with an industry representative.

CHAPTER 5: ENCRYPTION SERVICES

5.1. Sector overview

Encryption supports digital trade as it protects the confidentiality and security of data, whether the data is in transit or storage. With encryption utilized in nearly all commonly used and globally traded ICT products and digital services, the adoption of policies that support encryption's role in protecting cross-border data flows supports digital trade, while discriminatory and restrictive policies could put digital trade and the large trade in ICT products at risk.

Encryption is a process to secure information from unauthorized access or use, mainly by changing information which can be read (plaintext) to make it so it cannot be read (cipher text)[89]. Over the last few decades, researchers and firms have gotten significantly better at using encryption to secure the privacy and integrity of data, which has been integrated into goods and services in order to improve security for consumers and businesses[90]. In particular, the development of public key cryptography, which allows users to communicate securely over an untrusted network, such as the Internet, has underpinned most modern ICT products and services. Whether consumers realize it or not, encryption is as ubiquitous as the many ICT devices they use in their daily lives. Even without a user's interaction, it is possible for devices to employ encryption when communicating to other devices to ensure that commands received from one device are authenticated before executing (US Department of Energy, 2011). Encryption is increasingly important as people and firms put more of their data online and engage with Internet-based services from throughout the world or use IT service providers from around the world.

Given this, encryption plays an important direct and indirect role in supporting digital trade. Encryption goods and services can be traded in-and-of themselves, such as through a software download. Encryption also plays a much broader role in supporting digital trade given it is embedded within many ICT goods and digital services. Encryption and other cryptographic tools can improve procedures for user authentication (preventing access from unauthorized actors) and guarantee the validity of instructions, as in the case of digital signatures[91]. As such, encryption allows consumers and firms to securely engage in a variety of online activities, such as access to services (e.g., logons, passwords, e-commerce applications) and privacy of communications (e.g., email, instant messaging, virtual private networks). Firms use encryption to protect the confidentiality of their research from competitors or hackers and to ensure the authenticity of their transactions with suppliers and customers. Essentially, strong encryption helps firms and consumers around the world securely communicate with the systems and individuals around the world, thereby facilitating the transactions that allow the global digital economy to grow (Jaikaran, 2016).

---

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

[90] Daniel Castro and Alan McQuinn, *Unlocking Encryption: Information Security and the Rule of Law* (Washington, D.C: The Information Technology and Innovation Foundation, March, 2016), https://itif.org/publications/2016/03/14/unlocking-encryption-information-security-and-rule-law.

[91] Digital Europe and The Information Technology Industry Council, *ICT Recommendations for Regulatory Cooperation in the Transatlantic Trade and Investment Partnership* (Washington, D.C and Brussels, February 2, 2015), https://www.bitkom.org/sites/default/files/file/import/ICT-Industry-position-on-TTIP-Regulatory-Cooperation.pdf.s

Trade in and use of encryption goods and services still has significant room for growth, especially since the growing importance of cybersecurity and data privacy and security means that advances in encryption are at the forefront of competition in IT goods and services. Indicative of this growing sector is a 2016 survey by researchers from Harvard University which identified 865 hardware and software encryption products (a figure the researchers considered indicative and a lower-bound estimate) from 36 economies, with 56 percent of these products available for sale and 66 percent proprietary (while 34 percent are open source). Of the 546 non-U.S. encryption products the survey identified, 47 were for file encryption products, 68 email encryption products, 104 message encryption products, 35 voice encryption products, and 61 virtual private networking products (Schneier et al, 2016). Showing the room for growth, the Ponemon Institute's "2018 Global Data Security Study" survey of more than 3,200 IT and IT security officials from firms around the world found that while 95 percent have adopted cloud services, only 40 percent of them use encryption and key management services to securely store their data in the cloud.

5.2. Profile of firm interviewed

Virtru

Virtru's encryption services ensure that protection travels with the data—wherever the data is transferred and stored—as part of a user-friendly and client-side protected encryption service. Virtru's end-to-end encryption services are used by over 8,000 organizations and hundreds of thousands of users around the world, including for leading providers such as Gmail and Google Drive, Microsoft Outlook/Office 365, for a range of system-as-a-service cloud platforms, and for encryption key management. Virtru has been Google's Recommended Application Partner for encryption since 2016, enabling users to add layered protections to Gmail messages and attachments.

Virtru uses the trusted data format (TDF), an open source data protection standard. Regardless of whether the file is an email message, an Excel spreadsheet, or a photo, the files can be encrypted and "wrapped" into a TDF file. This file then communicates with Virtru-enabled key stores to maintain access privileges. For example, when the email recipient attempts to open the message and the attachments, the TDF "wrapper" communicates with the Virtru server and verifies whether the receiver is verified as eligible to access the data, after which (if approved), the user can decrypt, open, and read the files.

When combined with Virtru's key management and access control systems, TDF provides persistent protection and granular control for emails, files, and other data types. Virtru allows administrators to easily revoke a message so that a user on the other end of an email will have access to the email or attachments. Virtru also has audit tools that facilitate reporting on when and where email and files have been accessed or shared. Virtru uses this encryption technology to remove the complexity and obstacles that encryption services create for end users. For example, it allows users to search encrypted email and attachments as easily as they search Google or Microsoft email inboxes (which contrasts with other traditional encryption services). Virtru provides end-to-end encryption at the client-side so that emails and files are encrypted on the client end to protect data even before it gets sent. In contrast, many other cloud-based services only encrypt the data with a key shared between the user and the service provider, creating a vulnerability for the data because it can be exposed by the service provider.

5.3. Role of data in firms' business models

Data is central to Virtru's service and what its customers use it for. As it relates to the movement and storage of data, Virtru's encryption service means that data seamlessly crosses borders as part of each process (described below), unless artificial legal/regulatory barriers prevent or distort this. Data is

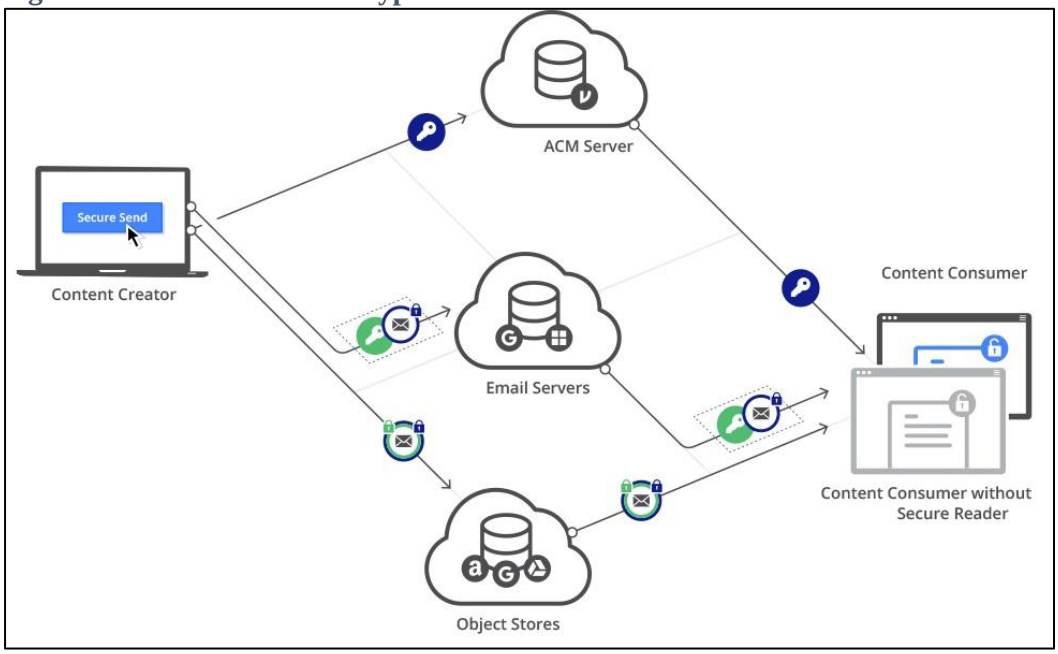
critical to the movement of the underlying data that Virtru's encryption services protect, the accompanying service a customer might be using it as a part of (such as any number of common email and data storage providers), and the functioning of Virtru's service (given it involves parallel processes for the data to be protected, transferred, stored, and accessed).

Data privacy and protection are central to Virtru's business model. Clients use its services to protect certain categories of data to comply with legal requirements for firms to use technical measures to protect data, such as for personal, health, and financial data. However, just as important to Virtru, is that its service is able to be used as part of a broader IT service that allows users to continue to reap the benefits of being able to share data, but as part of a controlled and auditable process. Virtru's Zero Trust Architecture uses a split-knowledge approach to content protection. Content and encryption keys are stored separately, so that only authorized parties can access unencrypted content. Only recipients authorized by the content creator can access and decrypt protected content.

A key feature of Virtru's business model is ease-of-use. For example, Virtru allows authorized parties to receive and decrypt protected content without installing its software. When using Virtru to secure emails, all messages and attachments are encrypted with access control keys on the content creator's client via a browser extension, Microsoft Outlook plug-in, mobile app, or other Virtru-enabled client. Access control policies may also be applied at this time, such as authorizing a party's access, setting expiration for this access, and enhancing content protection via PDF watermarking or download disablement. Once encrypted, emails are sent via Transport Layer Security (TLS, and its predecessor, SSL, a point-to-point encryption used across the Internet to send secure email, protect financial transactions, and provide for secure web browsing) to the email server that will eventually deliver this content to authorized recipients. Cloud providers cannot access unencrypted content or decrypt content on their servers because they do not have access to the keys stored in the Virtru access control management (ACM) server.

To allow recipients to read emails without installing its software, Virtru utilizes an external object store, such as cloud storage services, to surface encrypted emails. The sending client that uses Virtru creates a copy of the encrypted email and any file attachments, re-encrypts them with a separate key, and sends the re-encrypted content to the designated object store. Virtru's services do not have access to the sender's or the recipient's email servers, ensuring that encrypted content stored in the external object store cannot be decrypted outside of a Virtru client. For each object, such as the individual email bodies and attachments, an individual Access Control Key is created and sent to Virtru's ACM. The content and key remain separate until a content consumer requests access to the encrypted email content. After authenticating, the content consumer receives access to both the Access Control Key (from the ACM) and the Split Knowledge Key (from the receiving email server). The Split Knowledge Key decrypts the Access Control Key, which decrypts the original email content. For file storage, many similar processes take place in email encryption. This process highlights the many and varied ways that data and data flows play in Virtru's business model.

Figure 10. Virtru's email encryption



Source: Virtru's website

5.4. How policies and regulations impact firms' business models

Commercial encryption services relate to several laws and regulations that affect—both positively and negatively—its role in digital trade. Many of these are detailed below, but in summary, include:

- The use of encryption as a tool to protect data privacy and ensure data security as required by an economy's laws;
- The need for licenses, registration, local encryption key storage, and source code disclosure as a condition of import, sale, and use for commercial encryption services and products;
- The need for firms to use a government-mandated encryption standard; and
- Legal and administrative requirements to provide vague and arbitrary decryption support or technical support, without a transparent, predictable, and independent legal framework to manage such requests.

Commercial encryption directly relates to a growing range of domestic and sectoral data privacy and protection laws around the world as a technical tool for firms to prove that they have taken reasonable steps to protect data, especially certain categories of data, such as personal, health, financial, and justice-related data (elaborated upon below). In many instances, encryption is not explicitly required (it is simply mentioned as an example of what should be used), while in other cases, encryption is explicitly required as a form of data protection, as is the case in a recent regulation from Denmark. Either way, effective encryption policies should satisfy local legal requirements for firms to take technical steps to protect data, while still allowing data to flow freely (i.e., to be transferred and stored anywhere).

Data-related laws and regulations that support the role and flow of data

Data-related laws and regulations can have a major effect on the data involved in the use of encryption services and the broader role that encryption plays in digital trade. The case with Virtru shows that economies can enact laws and regulations that mitigate data-related policy concerns through the use of technology, without affecting the flow of data (such as through local data storage requirements). Firms can use encryption services, such as with Virtru's, to comply with privacy, financial, data security, and other regulatory requirements that several economies have which require firms to use technical measures to protect data, especially certain categories of data considered sensitive. These encryption-

related provisions (outlined below) focus on the firm using technological tools to ensure it protects certain categories of data, while still preserving its ability to transfer, share, and use data.

The United States

Health Data: Data encryption is a method to protect personal health information under the U.S. Health Insurance Portability and Accountability Act (HIPAA), which extends to all data that a covered entity creates, receives, maintains, or transmits in electronic form[92]. For example, HIPAA requires integrity controls (to ensure data is not improperly modified) and that organizations use a mechanism to encrypt electronic health information. For example, Omada Health uses Virtru's services to share sensitive data, including via email, whereas previously, it could not do this as its previous email and security arrangements were not secure enough. Furthermore, Virtru's service scans emails upon sending and matches them against specific rules to alert users that they may contain sensitive information and should therefore be encrypted. Similarly, Pitkin County in the United States and Massena Hospital both adopted Virtru's encryption services to ensure HIPAA compliance and better protect privacy and security.

Ultimately, this means that these organizations can send and share sensitive data with authorized third-parties, such as those involved in email, cloud storage, backup storage, mobile apps, tech support, and data analytics. Protecting healthcare data is critical as electronic health records can be worth even more to hackers than some financial data, such as credit card numbers, as the data (a person's insurance details, social security number, address etc.) can be used to create fake IDs to buy medical equipment or drugs (which can be resold) or used to file fraudulent insurance claims[93]. This healthcare data is often included in human resources data for foreign firms with U.S. operations. For example, Sony Pictures, which operates outside of the healthcare industry but still has human resources-related HIPAA requirements, has struggled to adequately secure healthcare data in the cloud. Following its 2014 email hack, Sony sent out a breach notification email admitting that info covered by HIPAA policy was among the leaked data[94].

Payments data: Encryption of cardholder data is an acceptable method of rendering data unreadable in order to meet the Payment Card Industry Data Security Standard (PCI DSS), which is a set of security controls that businesses are required to implement to protect credit card data. This is an industry-required standard (it is not required by U.S. law) managed by the Payment Card Industry (PCI) Security Standards Council. IT platforms need to be certified to manage this payments data, and while some popular cloud-based communications storage services have not been certified, when used in conjunction with Virtru's encryption services (which is certified), firms are able to use these popular platforms to manage cardholder data from the United States outside the economy.

The European Union (EU)

Privacy and Encryption – The EU's General Data Protection Regulation (GDPR) emphasizes data governance and accountability when firms manage personal data, requiring firms to assess the risk of data loss and data breach and requires them to consider technical—"state of the art"—measures to

[92] "Summary of the HIPAA Security Rule," U.S. Health and Human Services website, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
[93] Caroline Humer and Jim Finkle, "Your medical record is worth more to hackers than your credit card," *Reuters,* September 24, 2014, https://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924
[94] Steve Ragan, "Sony Pictures admits HIPAA data might have been compromised during breach," *CSO Online*, December 15, 2014, https://www.csoonline.com/article/2859822/business-continuity/sony-pictures-admits-hipaa-data-might-have-been-compromised-during-breach.html

mitigate those risks, including encryption. Because encryption is a common security measure and cybersecurity risks are increasing, it is likely that regulators and courts in Europe will find that encryption is necessary to comply with GDPR. The European Union Agency for Information and Network Security (ENISA) recommendation for end-to-end encryption for email supports this likely outcome[95]. Indicative of this assessment, Denmark's data protection agency announced in July 2018 that firms must encrypt all emails transmitting sensitive personal data[96]. This means that firms can use encryption systems, such as Virtru's, to transfer Danish personal data overseas (subject to other regulations).

Virtru's encryption services satisfy encryption-related requirements in the GDPR as they provide a level of protection and a range of access control features, such as protecting emails from creation (not once it reaches the email server), while allowing users and administrators to decide who can access content (and for how long). Relevant to the GDPR's governance and accountability requirements, email and file forwarding services using Virtru's system can be audited, limited, or prevented altogether. For example, Return Path (a leading email marketing firm) uses Virtru's encryption services to protect confidential human resources information and sensitive client communications in the European Union. In the past, the firm used Pretty Good Privacy, but it was not user-friendly, whereas Virtru's application can be turned on/off at the click of a button, is integrated with existing email providers, works with existing single sign-on processes, and provides protection for files and from a broader range of cyber threats. Again, this allows firms that use Virtru's services to transfer and use personal data from the European Union overseas (subject to other regulations).

Furthermore, while GDPR does not include specific rules for key management, Virtru's end-to-end key management services relate to requirements for technical security measures relating to encryption keys. Virtru allows customers to store encryption keys on-premise or in any cloud platform in order to give them exclusive control over encrypted content. This is in line with ENISA recommendations that "it is preferable, from a privacy perspective" that service providers do not have access to keys.

Multilateral engagement on commercial encryption issues

While commercial encryption services have existed for some time, international engagement to deal with domestic and international issues are limited. As of today, the most comprehensive international effort to establish recommended encryption policies took place in the Organization for Economic Co-operation and Development (OECD) in 1997 with the non-binding "OECD Guidelines for Cryptography Policy." Even back then, OECD members recognized that "due to the inherently global nature of information and communications networks, implementation of incompatible [domestic] policies will not meet the needs of individuals, business and governments and may create obstacles to economic co-operation and development; and, therefore, [domestic] policies may require international co-ordination."

Modern trade agreements have started including provisions to protect the trade in, and role of, encryption goods and services. For example, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) includes a number of provisions in the technical barriers to trade chapter, including ones that prohibit an economy from requiring a firm to transfer or to provide access to proprietary encryption technology and material, such as a private key or algorithm specification as a

[95] European Union Agency for Network and Information Security, "Privacy and Data Protection by Design" (Heraklion, Greece, January 12, 2015), https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

[96] Murtha Cullina, "Denmark Implements Email Encryption Requirement, What Countries Will Follow?" *JDSupra*, July 25, 2018, https://www.jdsupra.com/legalnews/denmark-implements-email-encryption-41045/

condition of market entry, sale, distribution, import, or use[97]. Furthermore, it prohibits signatories from requiring a firm from having to setup a joint venture or use a particular cryptographic algorithm, while providing exceptions for government networks, law enforcement access (via a legal process), supervision of financial institutions or markets, and for domestic security issues. The draft United States–Mexico–Canada Agreement also prohibits import restrictions of commercial goods that contain cryptography[98]. The European Union also views securing rules to protect encryption as a key component of its digital trade strategy[99].

Data-related laws and regulations that limit the role and flow of data

There are a range of laws and regulations related to encryption services that potentially inhibit or stop the flow of data. These include: requirements that firms store encryption keys locally; requirements relating to government access to data (such as requests for decryption or technical assistance), even though this may not be technically feasible given encryption key access issues; and requirements relating to government approval for market entry, such as source code disclosure and the use of mandatory encryption standards.

For example:

- Local encryption key storage would mean that the firm or its customer would have to setup a local server to facilitate the authentication and encryption process. For customers using their service outside their home economy, this would mean that the data allowing the encryption key authentication and use would flow back-and-forth across a border.
- Data localization would mean that use of encryption services would be limited to within that economy's borders. The only cross-border data flows involved in using encryption services would happen for categories of data that do not need to be stored locally.
- If economies require the disclosure of a firm's source code as a condition of market entry, it would limit market access as it would dissuade some firms from entering given the potential adverse impact of source code misappropriation. Similarly, government requests for technical assistance or encryption keys pose a similar potential barrier to market entry and operations as facilitating such requests may pose broader risks to the security and reputations of a firm and its IT products.

These types of rules would potentially affect the flow of data for firms like Virtru that focus on commercial encryption services. It should be noted that Virtru did not report that it or its clients have run into these issues. However, a number of economies have considered or enacted these types of requirements, which would affect data involved in its type of service. For example, as part of its broader strategy to control data within its borders, one APEC economy is increasingly requiring encryption keys and data access, with non-complying firms potentially being fined or having limited market access[100].

---

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

[98] United States Trade Representative, "United States-Mexico-Canada Trade Fact Sheet," United States Trade Representative Office website, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2018/october/united-states%E2%80%93mexico%E2%80%93canada-trade-fa-0

[99] Marietje Schaake, *Working Document on Towards a digital trade strategy*, (Brussels, Committee on International Trade, European Parliament, June 7, 2017), https://marietjeschaake.eu/media/uploads/posts/1497947344-Working%20Document%20Marietje%20Schaake%20Towards%20a%20Digital%20Trade%20Strategy%20INTA.pdf

[100] Josiah Wilmoth, "Russia May Unban Telegram…if it Shares Encryption Keys with the FSB," CCN, August 28, 2018, https://finance.yahoo.com/news/russia-may-unban-telegram-shares-133955770.html; Amy MacKinnon,

Similarly, other APEC economies have required local data storage and government access to data, which in effect requires breaking encryption[101]. Another APEC economy has also passed recent legislation that would require companies to not use end-to-end encryption in commercial products so law enforcement could gain access to data. Such efforts that mandate data access may effectively weaken security and privacy[102].

Market Entry or Operating Requirements

Commercial encryption services can also be affected through a range of other legal, technical, and administrative requirements, especially when the laws and legal framework for rules are broad, vague, intrusive, and implemented without a legal avenue for appeal.

Licensing and registration requirements can be used to limit which firms can enter, how they can operate, and what they can develop and use in terms of encryption products and services[103]. For example, some economies require an import permit or license for a range of encryption products and have an extensive certification regime to manage the development, distribution, use, and sale of encryption products[104]. As part of recent reforms in one APEC economy, firms need to obtain a certificate to produce encryption products, while distributors can only distribute certified products[105].

Similarly, requirements that firms provide source code disclosure for information communication technology (ICT) products (which have encryption embedded) as part of vague and broad security certification reviews can be used as a tool to discriminate against foreign products across a number of major commercial sectors, such as banking, finance, health, and other sectors[106]. Likewise, mandatory encryption key disclosure as part of law enforcement or domestic security investigations, such as under the Investigatory Powers Act of one non-APEC economy, raise trade concerns given the potential for users to see this as an indirect weakening of an encryption product/service. Another example, mandatory

---

"How Russia is Strong-Arming Apple," Foreign Policy, January 31, 2019, https://foreignpolicy.com/2019/01/31/how-russia-is-strong-arming-apple-data-security-icloud/; Maria Kolomychenko, "Exclusive: Russia plans stiffer fines for tech firms that break rules – sources," Reuters, November 26, 2018, https://www.reuters.com/article/us-russia-technology-security-exclusive-idUSKCN1NV09P.

[101] Campbell Kwan, "New Thai laws allow government to access information without warrants: Report," ZDNet, March 1, 2019, https://www.zdnet.com/article/new-thai-laws-allow-government-to-access-information-without-warrants-report/; Jeff Paine, RE: Additional Submission with comments on Thailand's Cyber Security Bill (Singapore, Asia Internet Coalition letter to Thailand's Ministry of Digital Economy and Security, November 29, 2018), https://www.aicasia.org/wp-content/uploads/2018/12/Final-AIC-additional-comments-for-Thai-CS-BIll_291118.pdf; Aekarach Sattaburuth, "Cybersecurity bill passed," Bangkok Post, February 28, 2019, https://www.bangkokpost.com/news/general/1636694/cybersecurity-bill-passed.

[102] Jamie Tarabay, "Australian Government Passes Contentious Encryption Law," New York Times, December 6, 2018, https://www.nytimes.com/2018/12/06/world/australia/encryption-bill-nauru.html.

[103] Global Partners Digital, *World map of encryption laws and policies*, website, https://www.gp-digital.org/world-map-of-encryption/

[104] Covington, *China Revises Rules on Commercial Encryption Products*, Covington law firm website, October 15, 2017, https://www.cov.com/-/media/files/corporate/publications/2017/10/china_revises_rules_on_commercial_encryption_products.pdf

[105] De Brauw Blackstone Westbroek, *Trends – China moves away from strict encryption regulations for foreign companies*, De Brauw Blackstone Westbroek website, February 15, 2018, https://www.debrauw.com/newsletter/trends-china-moves-away-strict-encryption-regulations-foreign-companies/#

[106] Michael Martina, "Business groups petition China's premier on cyber rules," *Reuters*, August 11, 2016, https://www.reuters.com/article/us-cyber-china-business-idUSKCN10M1DN

encryption standards, also constitute a technical barrier to trade as it prevents a firm from using its own proprietary encryption standard and process, which allows easier integration for the firm's global operations and may be more secure. For example, one APEC economy has mandated the use of domestic encryption products in telecommunications infrastructure, such as for 4G[107].

Intellectual Property

Commercial encryption services can also be affected through intellectual property-related laws and regulations that mandate that firms provide access to or a copy of their underlying source code. This poses a significant risk to a firm's business model, as source code lies at the heart of the patented technology that encryption companies develop to secure goods and services. For example, one APEC economy is considering mandatory source code disclosure as part of a new law for electronic systems and transaction operations[108]. While the details of industry-standard encryption algorithms are generally available, the implementation of these algorithms as part of a software or hardware product to deliver commercial goods and services may be proprietary. Sharing source code with government agencies risks poses a number of issues, such as potential source code misappropriation. In exceptional cases, such as in government procurement, there may be legitimate reasons to require source code disclosure, but a blanket requirement for encryption key or source code disclosure as a condition of market access is significantly disproportionate and trade distorting.

Concerns about source code disclosure also arise when economies mandate broadly defined requirements that firms cooperate or provide technical support to regulatory, law enforcement, and domestic security agencies, such as for security reviews as part of licensing and certification and for law enforcement and domestic security investigations. Beyond the risks from source code disclosure, the integrity of a firm's encryption products may be undermined by mandating that firms build so-called "back doors" into their products to facilitate government access. This can raise concerns such as defining technical requirements based only on an economy's subjective view of what is reasonable and practical, without due regard for how encryption is developed or how it works.[109] A weakness or opening provided for one stakeholder inevitably weakens the overall level of protection as it provides an opening for others, such as hackers. There have been calls for and draft laws mandating such cooperation and back doors in several APEC economies. In contrast, both Germany and the Netherlands have publicly disavowed backdoors in encryption products.[110]

Encryption key management is another area where economies can enact trade-distorting measures, such as requiring a firm to store keys within an economy (a so-called "key escrow"). Key management includes dealing with the generation, exchange, storage, use, and replacement of keys. In economic terms, it could be argued that an encryption key represents the aggregated value of all the information

---

[107] Adam Segal, *China, Encryption Policy, and International Influence.* (Stanford, Hoover Institute, 2016), https://www.hoover.org/sites/default/files/research/docs/segal_webreadypdf_updatedfinal.pdf; Stephen Ezell, *The Middle Kingdom Galapagos Island Syndrome: The Cul-De-Sac of Chinese Technology Standards* (Washington, D.C: The Information Technology and Innovation Foundation, 2014),

[108] "Letter: comments on Government Regulation 82/2012 on Electronic Systems and Transaction Operations," multiple trade association letter, hosted on the Software Alliance website, March 1, 2018, https://www.bsa.org/~/media/Files/Policy/Data/03012018BSAJointSubmissionOnGR82Amendment.pdf

[109] Aaron Tan, "Apple challenges Australia's proposed decryption law," *Computer Weekly*, October 15, 2018, https://www.computerweekly.com/news/252450584/Apple-challenges-Australias-proposed-decryption-law

[110] Kim Zetter, "Encryption is Worldwide: Yet Another Reason Why A U.S. Ban Makes No Sense," *Wired*, February 11, 2016, https://www.wired.com/2016/02/encryption-is-worldwide-yet-another-reason-why-a-us-ban-makes-no-sense/; "Dutch government says no to 'encryption backdoors'," *BBC*, January 7, 2016, https://www.bbc.com/news/technology-35251429. https://www.bbc.com/news/technology-35251429

that is protected by it, for example, all bank transactions.[111]. For example, Apple moved encryption keys for iCloud account users into one economy in response to a new cybersecurity law.[112].

5.5. Conclusion

Encryption services play both a direct role (given their growing use) and indirect role (as a facilitator of communications and other services) in digital trade. By acting as a technical tool to protect data and data-driven services, encryption services provide a clear example as to how the confidentiality of data does not generally depend upon its location, but the technical and administrative tools used to store and secure it. Yet, encryption services' role in digital trade can be limited by policies which restrict the free flow of data it relies on (through data localization), customer choice of services (through licensing and other market entry restrictions), the intellectual property it can be protected by (such as source code disclosures), and key technological processes which ensure its integrity (such as encryption keys and government-mandated backdoors).

[111] Sweden's National Board of Trade, *The Cyber Effect The implications of IT security regulation on international trade* (Stockholm, June 2018), https://www.kommers.se/Documents/dokumentarkiv/publikationer/2018/The-Cyber-Effect.pdf

[112] Stephen Nellis and Cate Cadell, "Apple moves to store iCloud keys in China, raising human rights fears," *Reuters*, February 24, 2018, https://www.reuters.com/article/us-china-apple-icloud-insight/apple-moves-to-store-icloud-keys-in-china-raising-human-rights-fears-idUSKCN1G8060; Robert McMillan and Tripp Mickle, "Apple to Start Putting Sensitive Encryption Keys in China," *Wall Street Journal*, February 24, 2018, https://www.wsj.com/articles/apple-to-start-putting-sensitive-encryption-keys-in-china-1519497574

CHAPTER 6: ELECTRONIC INVOICING AND DIGITAL TRADE

6.1. Sector overview

Governments around the world are embracing electronic invoicing (EI) as a way to combat fraudulent activities and improve tax and other business services. The main advantages of EI includes: it shortens processing cycles, including tax recovery; it lessens the risk of human error; it cuts transaction costs (such as printing and storage); it aids the fight against fraud; and it helps modernize the economy and strengthen the technology sector through the large-scale use of communications technologies, digital signatures, and services development (OECD, 2017). However, in order to maximize the benefits of EI, policymakers need to better understand the negative implications that some data-related policies may have on its utilization.

EI represents a major improvement for tax, trade, and other services, as traditionally, invoicing, like any paper-based process, is manually intensive (and therefore inefficient) and is prone to human error, resulting in increased costs. According to a study by Nixon (2017), the global e-invoice and enablement market is estimated to be worth 3.3bn euros in 2017 and will reach 16.1bn by 2024. The reason for this huge growth is that more than 90 percent of all invoices worldwide are still processed manually. Latin America is a global leader in the adoption of EI and the region is estimated to see a compound annual growth rate of 32 percent in the use of EIs in the 2017-24 period, with Mexico the regional and global leader in terms of adoption. Asia is expected to see a compound annual growth rate of 62 percent (Nixon, 2017).

Governments around the world are using EI as part of a broader push to digitize public services to improve service delivery and business operations. The use of such digital technologies in the tax, finance, and accounting sectors can improve the efficiency of public finances and tax collection services, which need to adapt to the digital nature of modern business to make compliance with these public services easier and cheaper. EI offers tremendous potential benefits for tax control, as the accumulation of invoices of credits and debits for a taxpayer—contrasted with the periodic tax returns covering the corresponding tax period—creates a control capacity that is much greater than any of the traditional mass control practices used. The traditional sampling of invoices as part of verification and scrutiny processes become obsolete when the administration's systems have an electronic record of all the documents. An Inter-American Development Bank (IADB) report (Barreix and Zambrano, 2018) outlines the positive impact that EI has in five economies in Latin America, showing that using EIs has a positive effect in value added tax (VAT) tax returns and payments. However, the benefits are much broader, and include spillovers into the private sector. Used correctly, this type of technology can create a virtuous circle for the benefit of society in that firms can use digital technologies to run their operations more efficiently and effectively, while also using these same technologies to make taxes easier to pay.

Furthermore, the digitalization of invoices opens a range of potential new services and processes for economies' tax administrators (TAs). Digitalization allows for automation, in that submitting data in standard formats facilitates data authorities to use tax, accounting, as well as other source data for compliance purposes. For example, as EIs are reconciled with a taxpayer's accounting records in Mexico, it is possible for taxpayers to be selected for income tax and VAT inspection based on digital information (EY, 2016). Digitalization allows tax authorities and other firms to use data analytics to uncover complex business relationships that they can use to trigger audits if necessary. For example, consistency can be checked by cross-referencing VAT return information with sales amounts claimed on income tax returns. In addition, a natural extension of EI are electronic payrolls (EP), which include information on salaried employees, which makes the determination of the payment of personal income tax and social security contributions easier and more transparent (Barreix and Zambrano, 2018).

In terms of other public-sector spillovers, EI opens up new avenues for economic and market analysis. For example, in Ecuador, the traceability of EI has allowed government agencies to better identify and analyze the local value-added contribution, and market composition, of production networks and entire

economic sectors. Emerging technologies like blockchain, automation, and machine learning will not only speed up adoption of EI, but open up other new, innovative ways in which to use and leverage EI. Overall, EI and related digital technologies will change the role of tax authorities from controllers of taxpayers' compliance to suppliers of services to taxpayers and to the public sector itself, with a more flexible relationship with firms, who are able to use EIs and similar records for other business services (Barreix and Zambrano, 2018).

For all of these reasons, EIs are a global phenomenon, but one where regimes differ by economy and region. In Latin America, Argentina, Brazil, Chile, Costa Rica, Ecuador, Guatemala, Mexico, Peru, and Uruguay already use EI, while projects are underway in several other economies, including Costa Rica, Colombia, Guatemala, Panama, and Paraguay. In Asia, Singapore has allowed EI since 2003. Since 2011, Chinese Taipei has made EI mandatory for all companies that submit invoices to the finance ministry. EI is used in private-sector settings in several European Union economies, such as Austria, Germany, Sweden and the United Kingdom. Since 2005, Denmark has made it obligatory to use EI for all transactions with the public sector. Italy will require the use of EI for all business-to-business operations as of 2019. In Africa, both Angola and Kenya are considering EI services.

The case of EI in Mexico is worth exploring given that the firm interviewed in this chapter operated in this economy. In 2004, EI was allowed when Mexico's Tax Administration Service (TAS, the government taxation agency) created the legal framework that defined the implementation of the "digital tax receipt" (an e-invoice, known by its Spanish acronym CFD or CFDI). Use was not mandatory, but a large number of firms adopted it, which led TAS to establish a new model—the Digital Tax Receipt by Internet (known by its Spanish acronym as Comprobante Fiscal Digital por Internet)—model in 2010. TAS gradually expanded the compulsory use of the DTRI, requiring any company that generates an annual revenue of more than 250.000 pesos (approximately EUR 11.000) to use a CFDI. The success of the system is evident by the fact that the volume of EIs issued between 2011 and 2017 increased from 1.7 billion to 6.5 billion.[113]

EIs are also increasingly popular for different reasons. They support global efforts toward improved tax transparency and cooperation on tax issues and have the potential to play a key role in improving the international exchange of tax information as part of multilateral efforts, such as those outlined under the Multilateral Convention on Mutual Administrative Assistance in Tax Matters (so far signed by 114 economies). The Convention allows for the periodic and systematic transmission of information between economies on a range of income, such as dividends, interest, royalties, salaries, and pensions.

EIs also provide another example of how digital technologies, such as online platforms, payment services, and encryption, can help overcome costs, complexity, and other barriers to international trade, such as uncertainty about local tax compliance and a lack of trust in cross-border transactions (WTO, 2018). As such, EI supports greater cross-border digital trade and e-commerce since it improves the perception of trust in transactions, and therefore interaction with clients. For example, EIs facilitate the development of more transparent, efficient, and secure 'factoring,' which allows suppliers to meet their working capital needs by selling their invoices, or accounts receivable, to lenders for cash (i.e., getting paid upon completion of work rather than waiting weeks or months for customers to pay their bills)[114].

Finally, EI improves the real-time control of freight. For example, Brazilian TA are using EI as part of an innovative customs and tax management tool, whereby a freight-vehicle tracking project using radio

[113] "CFDI: Mexico's Electronic Invoicing Model That's Become a Reference Across all of Latin America," EDICOM, accessed January 31, 2019, https://cfdi.edicomgroup.com/en/cfdi-al-dia-en/cfdi-mexicos-electronic-invoicing-model-thats-become-a-reference-across-all-of-latin-america/.
[114] "Factoring," United Nations Economic Commission for Europe Trade Facilitation Implementation Guide, accessed January 31, 2019, http://tfig.unece.org/contents/factoring.htm.

frequency is integrated with the EI related to transported goods. While the vehicles are on the move, antennas scan them each time they pass by goods-transport control units located along the highways. This allows the TAs to monitor goods traffic in real time, and the goods are matched to their respective tax documents. In addition to the tax control, it is expected that the exchange of information will also help reduce the theft of vehicles and their cargo (Barreix and Zambrano, 2018). In a similar way, the digitalization of customs operations in a way broadly similar to EIs would facilitate the efficient movement of goods.

6.2. Profile of firm interviewed

Founded in 2011, Gosocket is a mid-sized firm (total staff of 150) based in Santiago, Chile, but with offices and operations across Latin America (a total of 12 economies, including Brazil, Colombia, Cost Rica, and Mexico). It provides a range of EI services. For example, it provides a single platform to integrate and transform invoices from different enterprise resource planning (ERP) services into an electronic format, which is transferred to local tax authorities for validation and processing. It also provides a service for receiving and validating e-invoices that suppliers send to their clients, which means it also stores data of e-invoices not issued directly by them. Gosocket provides an application programming interface (API) so enterprise users and third-party vendors can offer additional solutions and capabilities to augment the platform, such as through accounting or inventory services. For example, its platform allows customers to analyze the information in their EIs to help them make better business decisions.

Gosocket has over 20,000 firms using its services, processing 5 million EIs daily. It has processed over USD $7 billion in EIs. Gosocket provides EI services for local and foreign firms that operate throughout Latin America. Their services are cloud-based, allowing customers to efficiently manage issued (sales) and received (purchases) documents remotely. In a first, Gosocket has set up a project (in cooperation with Microsoft) to provide its services for the Colombia government. Gosocket has support centers across Latin America.

6.3. Role of data in firms' business models

EIs are simply invoices that record an entity's commercial transactions in electronic form. Being digital, it means that there are no differences between originals and copies, but that there needs to be a common set of rules and defined processes that enable the standardized interpretation of this digital documentation. Each economy's TA regulates a single electronic format to be used by all certified tax-related firms and taxpayers. The data of an EI needs to be in a particular format so that it can be entered (integrated) into the TA's IT systems and the buyer's account payable accounting system without requiring any manual data input (from the buyer's own accounts payable administrator). Many TAs use Extensible Markup Language (XML) file formats (which is a plain text file that uses custom tags to describe the structure and other features of the document). For example, clients connect their ERP software to Gosocket's services in order to process their invoicing information into EIs. This transformation involves turning the data into an XML file format. Gosocket is then able to send EIs to the digital platform used by TAs for validation.

Gosocket stores, aggregates, processes, and transfers significant amounts of data from clients using its EI services. This data takes the form of the invoices themselves, encryption keys, and electronic signatures and communication that confirms an EI has been received, protected, decrypted, authenticated, and stored. Gosocket stores all its data on a cloud storage service (Microsoft Azure), given the low-cost, secure, and flexible services it allows them to provide clients in multiple economies. It is important to recognize that the data Gosocket manages has two owners—the issuer and the recipient involved in the transaction—so its platform has to be accessible to both parties. Gosocket helps improve communication between the parties as it allows the easy exchange of these digital documents. The data

Gosocket stores is confidential business data, and given it has two owners, it cannot be shared without explicit authorization or other legal requirements.

Gosocket has announced some world-first partnerships to provide quick and secure liquidity for clients via invoice financing. Gosocket believes that blockchain will be the next step in the digitalization of financial services. The goal is to launch the service in Mexico, Guatemala, Costa Rica, Colombia, Ecuador, Peru, Chile, Uruguay, Argentina, and Brazil.

6.4. How data-related policies and regulations impact their business model

Before analyzing how specific policies can affect the use of data by EI-related services, it is important to recognize that economies need to address a few fundamental issues if they are to be able to benefit from EIs. TAs must have the institutional capacity to perform their basic functions (e.g., registration, collection, auditing and recovery). TAs must also have sufficient data processing capacity, adequate ICT infrastructure, and a minimum degree of computer literacy among TA staff, the business community, and taxpayers. In particular, moving to EIs obviously entails investment in ICT infrastructure, as TAs will likely store and process more EIs in a few days than the total number of tax returns and other traditional documents they would receive in a year.

Once these key components are in place, economies can enact a system that uses EIs; however, in doing so, they can inadvertently enact policies which create barriers to the cross-border supply of EI services. As the interview with Gosocket shows, these typically arise as an economy's TA enacts and enforces economy-specific certification requirements that affect how/if firms can use a range of cloud-based data services and economy-specific cryptographic processes (both explained below). TAs in Mexico, Brazil, and elsewhere enforce these as part of their certification of third-parties to allow them to be the recipient of EIs and to conduct tax-related activities, such as tax collection and the processing of digital tax returns. For example, Mexico has authorized 70 or so third-party operators (known as Authorized Certification Providers (PACs)) to provide the service of the initial certification and collection of receipts. Other economies (such as Peru) are also considering this model. Gosocket's experience shows how certain TAs can enact requirements around electronic/digital signatures and cybersecurity that act as a barrier to data flows across borders. This is a major problem for firms like Gosocket which rely on cloud-based solutions to provide their services across markets. It also raises issues for customer support, as cloud-based firms like Gosocket tend to setup regional support centers to manage services across economies (which may be prevented from accessing and analyzing data as part of customer-support activities).

This chapter explains in detail how two specific policies—economy-specific cryptographic and e-signature requirements—affect Gosocket and its ability to use data. In general terms, as outlined in the table (below) of responses from Gosocket, these data-related measures negatively affect a broad range of Gosocket's business. Gosocket indicated that these barriers lead to increased operational and compliance costs and undermine cross-border sales of services, affiliate activities (such as after-sales service and research), and investment. Gosocket outlined that, generally, these measures have a varying, but significant impact on:

Table 14. The Impact of Data-related Barriers to Data Flows – Gosocket's Response

Function	Impact (Low/Moderate/High)
Efficiently managing firm's operational costs	Low
Gathering, transferring, analyzing, and otherwise using data	Moderate
Offering the full variety of or quality of products/services	High
Innovating products and services as well as conducting or assessing firm R&D	Moderate

Managing cybersecurity risks, including protecting firm's sensitive data	High
Investing in or acquiring competing or complementary technology/assets	High
Leveraging the value of customer and/or supplier networks (network effects)	High
Expanding customer base (scalability)	Low
Accessing financing/funding	High

Source: Author's own elaboration

The general impact these data barriers have is not unique to the policies outlined below, but extend to all types of data-related restrictions that affect foreign tech firms which rely on centralized global IT services to provide fairly standardized, cost-efficient, and secure services across markets. These behind-the-border restrictions on data and related digital technologies are often difficult to identify and may only have an indirect effect on (a specific type of) trade and economic activity. However, in an era where digital technologies allow firms to provide any number of services across borders, these barriers can act as a formidable barrier to firms trying to achieve economies of scale as they make it costlier and more complex to enter and operate across multiple markets. This is especially the case for SMEs, which are more likely to lack the resources and expertise to adjust to requirements in multiple local markets.

Data-related laws and regulations that support the role and flow of data

Electronic and digital signatures – Key building block to digital trade

In the broadest sense, every economy needs to ensure that electronic and digital signatures[115] are allowed, recognized, and enforced in order to allow firms to conclude contracts and agreements online. According to the United Nations Conference on Trade and Development (UNCTAD, 2015), 145 economies have enacted such laws, of which 104 are developing or transitioning economies. Almost half, 46.3 percent, of African economies have adopted e-transactions laws, compared to 72 percent of Asian, 81.8 percent of Latin American and Caribbean, and 97.6 percent of developed economies.

Latin America (Gosocket's home regions) have economies which have (generally) permissive and useful policy frameworks for EIs (exceptions are explained in the next section). For instance, Chile is considered a 'two-tiered' jurisdiction as it gives digital signatures the same status as handwritten signatures. At the same time, it recognizes simple e-signatures as legal and hence enforceable. Mexico is also considered a 'two-tiered' jurisdiction with digital and electronic signatures. While digital signatures are preferred under this system, parties are generally free to determine the form of acceptance for an agreement. Last but not least, Peruvian law also recognizes the legal status of electronic and digital signatures. The law specifies the minimum requirements for acceptable digital certificates and their issuers. A digital certificate must be issued by a certification provider who meets these standards

[115] The terms "electronic signature" and "digital signature" are often used interchangeably. An electronic signature is a process of signaling intent, including acceptance, as to the content of an electronic record, such as through email addresses, enterprise IDs, personal ID numbers, scanned copies of handwritten signatures, and clickable "I accept" boxes. A digital signature (also known as an advanced e-signature) is essentially the equivalent of an in-person notarized signature (where a trusted third party, known as a certificate authority, serves as the notary in terms of verifying a person's identity). The certificate authority binds a person's identity to a public key infrastructure (PKI, which manages public-key encryption), thereby allowing them to apply digital signatures to documents. When a person applies a digital signature to a document, this cryptographic operation binds the person's digital certificate and the data of the document being signed into one unique fingerprint. The combination of the two components is what makes digital signatures a viable replacement for wet-ink signatures.

for it to be considered as valid. While it recognizes the validity of digital certificates issued in other economies, these certificates must meet Peruvian standards (Adobe Inc, 2016).

Data-related laws and regulations that limit the role of data

Electronic and digital signatures – Differential policies with local technical requirements

The first issue that firms like Gosocket encounter is when economies do not have the legal framework in place for electronic and digital signatures, which thereby means that users must rely on paper documents. The second major issue is that there is no universal approach to regulating the exchange and authentication of electronic transactions (World Economic Forum, 2017). However, the United Nations Commission on International Trade Law (UNCITRAL) has taken steps to increase the uniformity of economies' legal rules governing e-transactions, e-signatures, and digital authentication, mainly through the development and deployment of model laws (with various versions – 1996, 2001, 2005, and 2017). Over 70 economies have enacted the 1996 model law, while more than 30 have also used the 2001 model law[116].

However, UNCITRAL model laws are not legally binding, instead being designed to guide economies in drafting their own legislation, which means that there are substantial differences between how economies enact their own e-signature laws. This creates friction and increases the cost of doing business. According to the OECD-WTO Global Review 2017 Aid for Trade Monitoring Exercise (OECD and WTO, 2017), e-signatures were ranked 4th among the top ten challenges facing firm and consumers when accessing and using Internet services. The World Economic Forum (2017) considers that the absence of mutual recognition and divergent rules between economies can create additional costs that may be particularly difficult for SMEs to manage.

For example, while local technology standards and use are not required for an e-signature to be considered valid under Brazilian law, there are exceptions for certain, government-regulated cases, such as when parties are engaged in foreign exchange transactions, factoring (accounts receivable), and transactions with the Brazilian government. In these cases, Brazil requires the various parties to use e-signatures that use Brazilian IT infrastructure and services, in the form of a local government-authorized certification authority, called ICP Brazil. ICP Brazil maintains the root certification authority and requirements that must be met for both government-recognized timestamping and PKI signature policies. The use of this local tech standard diverges from UNCITRAL model law.

Gosocket has found these local certification protocols to be a barrier to its use of a fairly standardized, region-wide IT system. Gosocket explained that many firms in Brazil have had to invest considerable capital in setting up redundant local IT operations, such as by setting up a local hardware security module (explained below). As DocuSign (a major electronic signature and digital transaction management company) explains, due to the difficulty of distributing and maintaining these digital certificates, use of ICP Brazil-backed electronic signatures in Brazil is generally limited to these few high-value, high-volume transactions (DocuSign, 2017). This limits the broader adoption and use of EIs in Brazil's economy.

This highlights the operational and technical complexity for firms like Gosocket who have to adjust to certificate authorities (which act as the guarantor of a digital signature) in different economies changing

[116] The United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce (MLEC) (1996), UNCITRAL Model Law on Electronic Signatures (MLES) (2001), United Nations Convention on the Use of Electronic Communications in International Contracts (ECC) (2005), and the UNCITRAL Model Law on Electronic Transferable Records (MLETR) (2017).

their requirements for approved digital certificate. A digital certificate contains the public key for a digital signature and specifies the identity associated with the key (e.g. the name of the organization). Digital certificates are required in order to create a digital signature. When a local certificate authority, such as a tax administrator, update their digital certificate requirements (e.g. so that they can apply the best security measures available at the time), all digital services providers need to revise their economy-level services to account for this, which can cause brief complications around compatibility. It also highlights security issues when tax authorities require the use of obsolete digital certificates.

Local Encryption and Security Requirements

Until recently, Mexico had a policy in place which created local data storage, protection, and encryption issues. Mexico's Tax Authority (known by its Spanish acronym—SAT) mandated that firms wanting to manage EIs in Mexico (known by their Spanish acronym—PAC) need to use a local Hardware Security Module (HSM)[117].Gosocket had to pay for a duplicative and expensive HSM in order to install and use SAT's digital certificate, which is mandatory to be able to provide EI services and submissions to the SAT in Mexico. A HSM is a dedicated crypto processor that is specifically designed for the protection of the crypto key lifecycle. HSMs act as "trust anchors" that protect the cryptographic infrastructure by securely managing, processing, and storing cryptographic keys inside a hardened, tamper-resistant device within the data center. This requirement acted as a de facto data localization requirement given the crypto key, and associated EI data, needed to be stored within Mexico in case of an SAT query or audit (FutureX n.d.).

Mexico's SAT recently decided to remove this local data storage and protection requirement and allow PACs to use cloud-based data protection and storage services. For example, Gosocket's cloud service provider (Microsoft Azure) offers a dedicated HSM service for clients. This service has been certified by the Federal Information Processing Standard (FIPS) 140 (Security Requirements for Cryptographic Modules). This is a U.S. and Canadian government standard that defines a minimum set of security requirements for products that implement cryptography. This standard is designed for cryptographic modules that are used to secure sensitive but unclassified information. Microsoft Azure's HSM is certified as a level 4 device (on a scale of 1-4, with 4 being the highest level)[118]. This certification allows clients to meet the most stringent security and compliance requirements of clients. As part of this service, clients have full administrative and cryptographic control over Azure's dedicated HSMs. Microsoft does not have visibility into its client's cryptographic keys. This service is provided directly on a client's virtual network on Azure and can be connected to on-premises infrastructure via a virtual private network (Tiwari, 2018).

What this shows is that data protection does not depend on the geography of data storage, as many leading data storage providers can provided audited, best-in-class cybersecurity protection.

6.5. Conclusion

EIs represent an innovative improvement in how firms and government authorities manage accounting and taxation services. The widespread adoption of EI-based taxation and accounting systems would support digital and traditional trade by facilitating easier accounting and tax reporting in multiple jurisdictions (through services such as Gosocket) and also help firms engaged in trade (such as through more efficient factoring). However, it also highlights how data and related processes (such as e-

[117] These firms are known as "Authorized Provider Certification" (known by its Spanish acronym PAC)
[118] "FIPS 140 Validation," Microsoft Windows IT Pro Center website, April 2, 2018, https://docs.microsoft.com/en-us/windows/security/threat-protection/fips-140-validation#ID0EWFAC.

signatures and cryptographic measures) can be affected by laws and regulations from a wide range of government agencies. It shows how indirect measures can affect data just as much as explicit, direct local data storage. Both cases highlighted by Gosocket (in Brazil and Mexico) entail significant costs and complications for firms using data related to these restrictions. Yet, in the case of Mexico's TA, it also shows how government agencies can replace these measure with readily available and reliable alternatives that satisfy concerns about cybersecurity which were not dependent upon local technical requirements and data storage. Similar to its efforts working with Mexico's TAs, Gosocket has worked with tax authorities throughout Latin America to share their examples of best practices, details about their operations and corresponding policy recommendations. For example, Gosocket and IADB provided formal advice to Colombia's tax administrator in 2012-2013 to help them design their EI system. Similarly, Gosocket is working with other economies (by using as an example the HSM issue it faced in Mexico previously) to show that there are secure alternatives to local key storage. This highlights a process that other economies should consider as they look at allowing electronic invoicing and expanding its use.

CHAPTER 7: ARTIFICIAL INTELLIGENCE

7.1. Sector overview

Today's economy is a data economy as organizations use data and analytics to drive productivity and innovation. But this is transitioning into the algorithmic economy, in which many more organizations invest in artificial intelligence (AI) to automate processes, develop new products and services, improve quality, and increase efficiency (New, 2018). AI represents a cross-cutting, horizontal issue that is relevant to all firms and sectors engaged in trade. Using data, AI has the potential to impact virtually every sector of the economy given its ability to make and test assumptions (without human intervention), allowing it to learn autonomously. AI's impact on economic productivity holds the potential to be much broader, as various aspects of it can be understood as being "general purpose technologies" (such as microprocessors) that have historically been influential drivers of long-term technological progress as they affect most functions in an economy (Cockburn et al, 2017). By extension, AI-based applications can benefit both trade in goods and services, for example by optimizing route planning and enabling autonomous driving, reducing logistics costs through cargo and shipment tracking, and using smart robots to optimize storage and inventory (WTO, 2018).

AI's emerging role in international trade is based on the transformative impact of the Internet and other digital technologies. The rapid growth in the volume and diversity of data produced by digital platforms, wireless sensors, billions of mobile phones, and other sources, when combined with low-cost, widely accessible, and increasingly sophisticated cloud-based data storage services provides a platform for firms (of all sizes) from around the world to develop and deliver or use AI-based services. AI will have its biggest impacts on more routinized information-based functions, which tend to be services, (e.g., making loans, processing accounts, or analyzing medical tests) (ITIF, 2018). It is in relation to services that there are both significant opportunities—the WTO (2018) estimates that the share of services trade could grow from 21 to 25 percent of total global trade by 2030—but also peril, in that services trade liberalization (in terms of new and meaningful services market access and addressing the non-tariff issues that affect services) has long taken a back seat to traditional trade goals of reducing tariffs on goods.

Likewise, the McKinsey Global Institute (2017) estimates that the potential for data analytics in digital trade is significant, in part, as many firms are (still) capturing only a fraction of the potential value of data. There is a large and significant gap in the degree of digitalization between certain sectors and within sectors, where a few leading firms often lead a large group of laggards in terms of developing and using advanced digital capabilities (McKinsey Global Institute, 2017). This gap is a major factor shaping competition in an economy as leading firms are more profitable and successful. Legacy firms face the challenge of adapting to new digital technologies, like AI, which opens up the opportunity for firms that have mastered these technologies to provide their services to help them close the gap. Likewise, it also presents opportunities for those firms "born digital" that have AI/ML at the heart of their business model to either disrupt the incumbent players or to provide their services to help them catch up.

As this chapter outlines, firms using AI as part of their business model (or even as their entire business model) depend upon the ability to collect, use, transfer, and share a large volume and diversity of data to train and deploy their services, and these firms need to maximize the value of their investments in AI expertise and systems by deploying them as widely as possible across sectors and borders. Absent regulatory, market, trade, and other artificial barriers, these firms should be able to leverage modern ICTs to do this remotely as a form of services trade. However, this is not the case in many scenarios, which raises trade policy concerns around the rules and regulations that affect data, intellectual property, and market access (for key service sectors and for the remote delivery of services).

7.2. Profile of firms interviewed

Mindbridge Ai

Mindbridge Ai is a small, but rapidly growing, data analytics firm based in Ottawa, Canada[119]. Established in 2015, Mindbridge Ai has around 70 staff (its staff doubled in size in 2018). More than 230 customers in seven economies use Mindbridge Ai's AI auditor tool. Mindbridge Ai's main target is the external auditor services sector. In its short history, Mindbridge Ai has developed an impressive track record. In 2018, the Canadian Advanced Technology Alliance gave Mindbridge Ai its outstanding product achievement award, Accounting Today said its AI auditor was the top new product of 2018, and Mindbridge Ai's CEO Eli Fathi was named AI Leader of the Year at the Canadian FinTech & AI Awards. Mindbridge Ai also won the Central Banking's FinTech and RegTech Global Award for Best Machine Learning Solution for Regulatory Compliance.

Mindbridge Ai uses a hybrid of techniques—from decision-based rules and statistical methods, to ML and AI—to perform real-time data analytics, pattern recognition, and anomaly detection in order to help various organizations investigate or audit past activity, detect active inadmissible behavior (e.g., fraud), and prevent potential transgressions. Mindbridge Ai has two core products/services: its cloud-based AI Auditor platform and AI Advisory, which provides custom data analytics services for clients.

Mindbridge Ai's main product, AI Auditor, is used by leading certified practicing accounting firms and governments worldwide to detect anomalies in financial data. Through the automated ingestion and analysis of financial datasets, AI Auditor detects anomalies. AI Auditor's results are presented through an intuitive interface that augments the capability of auditors and investigative professionals by allowing them to focus on anomalous transactions. This significantly reduces the risks associated with manually analyzing samples of the transactions, while also delivering deep insights on the financial datasets.

Mindbridge Ai's custom model for the Bank of England's Fintech Accelerator is an example of its tailored services. The Bank of England gave Mindbridge Ai approximately 100,000 data points of desensitized, historic regulatory credit union data (going back seven years) to develop an AI-based model for anomaly detection (e.g. reporting errors, compliance issues, and fraud). Mindbridge Ai combined AI and ML with more conventional data science techniques to produce a risk score for each data point, allowing anomalies to be easily identified. Mindbridge Ai's initial project with the Bank of England was successful and has been extended.

Pondera Lab

Pondera Lab is a three-year old data analytics firm based in Mexico City, Mexico[120]. Pondera Lab has 12 staff, with specialties in data-related law, econometrics, and data analytics and science. Its goal is to help private sector firms and government agencies use AI to better organize, analyze, and visualize data to help make better business decisions. As part of this, Pondera Lab provides a holistic suite of consulting and AI-based services in advising clients on how to incorporate new technology to collect and explore data, helping show clients how to plan and strategize using AI and data analytics (including capacity building of technical skills if needed), and providing either off-the-shelf or custom-built AI and ML models for clients. Pondera Lab serves clients in Argentina, Bolivia, the Dominican Republic, Mexico, Panama, Peru, and the United States.

[119] "About – Mindbridge Ai," Mindbridge Ai website, https://www.mindbridge.ai/about/.
[120] "Pondera Lab - about us," Pondera Lab website, http://ponderalab.com.mx/en/about-us-2/.

Data is at the center of Pondera Lab's business. However, Pondera Lab itself does not collect data; instead, it helps its clients develop and use technology to better collect, organize, and analyze their own data. In Pondera Lab's three years, it has found that its service is among the cutting edge and often ahead of where the actual market is in terms of firms and government agencies recognizing that AI and ML can be used to drive efficiency and innovative new services. Pondera Lab found that besides large technology firms, many other large Mexican firms and government departments are still at a relatively low level of awareness about the potential to use data and AI to help their businesses.

At the heart of Pondera Lab's business model and competitive position is proprietary AI and ML models. Pondera Lab uses these to provide either basic data-driven business intelligence models or advanced models that provide predictive abilities and learning processes to drive efficient business services (such as logistics and marketing). A generalized and indicative case for Pondera Lab is a client that already collects, or has the potential to collect (but lacks the technology), a significant amount of data from customers. However, the data is "messy" in that some parts of the firm may be collecting data, while others do not. Different parts of the same firm may use different platforms which do not connect to each other, which can lead to data that is not being collected, aggregated, and stored in a standardized manner. This often leads to data not being analyzed on a consistent basis or in a manner that provides actionable business intelligence.

Certn

Certn is a small (12 full-time staff) start up based in Victoria and Toronto, Canada, that has developed an AI (using proprietary AI and ML systems) and data analytics services (also based on proprietary AI and ML systems) that are focused on helping clients analyze prospective customers, employees, and renters (for example, individuals applying for a loan or bank account, prospective renters, and job applicants) [121]. Certn's AI and data analytics services are hosted on a cloud-based platform. Certn's services collect a wide range of data in order to create comprehensive profiles of prospective customers and applicants and provide (predictive) advice to its customers. At its founding in late 2016, Certn's focus was on helping customers evaluate people's credibility (especially those that do not currently have access to financial services) in order to help promote financial inclusion, while reducing risk for financial institutions, landlords, and employers. Certn's services allow its customers to effectively validate identity, and make better risk decisions while satisfying 'know-your-customer' (KYC) and 'anti-money laundering' (AML) requirements. At the moment, Certn works only in Canada, but it is expanding into the United States.

Certn's two main services are screening, through its main platforms ---"Basic eID" and "Softcheck." Certn provides the rapid screening of employees, contractors, taskers, and tenants by checking for criminal records from around the world, credit reports, and motor vehicle and driver records. It can conduct both basic and enhanced identity verification. For the former, this includes being able to use its "Basic eID" to instantly confirm a person's age and credit details, but extends to using a range of data sources to generate multi-choice questions and answers that only the true identity owner should know. For the latter, Certn allows customers to use any Internet-enabled devices (such as a smart phone) to take a photo of their physical ID and a selfie, which combined with Certn's enhanced e-ID, uses a proprietary mix of AI (including the subfield of computer vision, which focuses on training computers to interpret and understand visual objects) and ID experts to determine if an identity document is authentic and belongs to the user.

Certn's Softcheck identifies risk using real-time public information. It is designed to reduce the instances of high-risk hires, tenants, and customers by delivering automated, intelligent customer

[121] "Why Certn," Certn website, https://certn.co/.

screening, and to provide advice that helps businesses make decision about customers/applicants. Softcheck is updated daily and is curated using both natural language processing (NLP) and ML, with expert oversight from compliance personnel. Certn's API (a key function for software) allows it to provide a "plug-and-play" service to financial institutions, commercial property managers, financial technology companies, real estate technology companies, credit resellers, and others to assist with their risk management, identity verification, and compliance needs. Certn's API gives clients seamless access to their databases.

Softcheck uses data from a range of services, including:

- Criminal Record Searches: Public criminal and court records from around the world including PACER (USA), 350+ courts, boards and tribunals in Canada and records from 240 other economies (Interpol, economy-specific government and state agencies, and police forces).
- Adverse Media Scan: Softcheck uses AI to check over 200,000 sources of adverse media/negative news, sorts relevant articles for risks, and identifies individuals before they appear on a sanctions list or court record.
- Fraud watchlist: Softcheck scans thousands of watchlists dedicated to reporting fraud, including governing regulatory bodies (financial and securities commissions) from around the world.
- Known Affiliation: Softcheck searches police, government, and public databases for known affiliations to gangs, terrorist organizations, and other negative groups.
- Sex Offender Registry Check: Softcheck searches registries for every state, province, and territory in hundreds of economies.
- Public Profile Scan: Softcheck searches social media platforms for public social media profiles, positive news articles, and high-risk behavior.

7.3. Role of Data in Firms' Business Models

Each in their own way, the firms interviewed for this chapter both rely on data in their respective business models and show how they are all focused on specialized services to help other firms use data (and their AI) to help themselves. They are similar in that they are all outside parties offering their AI-based services to clients, rather than developing or otherwise applying AI-based services within established firms. As Certn put it: "business is data."

It is helpful to explain some background on AI and its connections to trade. AI is a branch of computer science devoted to creating computer systems that perform tasks characteristic of human intelligence, such as learning and decision-making. AI overlaps with other areas of study, including robotics, natural language processing, and computer vision.[122]

AI offers many functions:

- Monitoring: AI can rapidly analyze large amounts of data and detect abnormalities and patterns.
- Discovering: AI can extract insights from large datasets, often referred to as data mining, and discover new solutions through simulations.
- Predicting: AI can forecast or model how trends are likely to develop, thereby enabling systems to predict, recommend, and personalize responses.

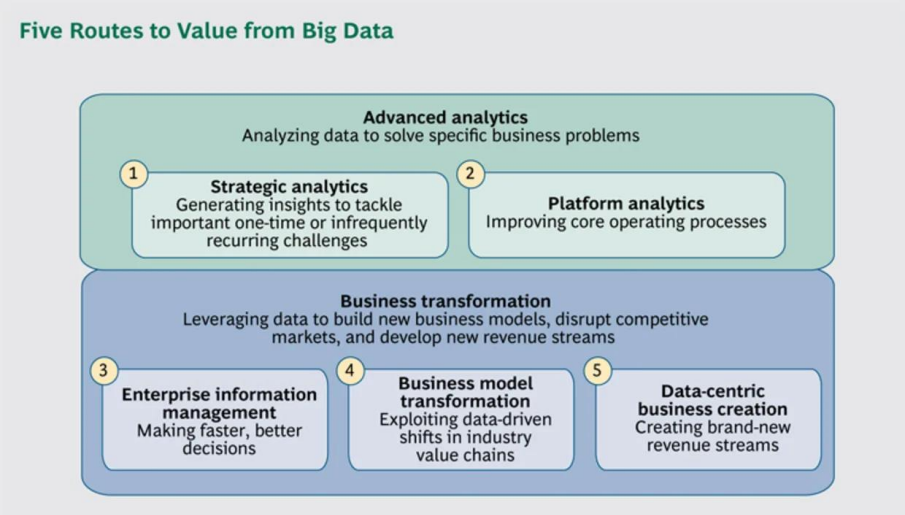
[122] The Information Technology and Innovation Foundation (ITIF). ITIF Technology Explainer: What Is Artificial Intelligence? (Washington, D.C, September 4, 2018), https://itif.org/publications/2018/09/04/itif-technology-explainer-what-artificial-intelligence.

- Interpreting: AI can make sense of patterns in unstructured data such as images, video, audio, and text.
- Interacting: AI can enable humans to more easily interact with computer systems, coordinate machine-to-machine interactions, and engage directly with objects.

Machine learning is an important subfield of AI. It focuses on building systems that can learn and improve from experience without being explicitly programmed with specific solutions. This compares to traditional data analysis, where software aggregates, organizes, and performs basic analysis of historical data for a human to interpret and use as the basis for predictions, insights, or programming feedback. Within ML, an important development is deep learning. Deep learning involves processing multiple layers of abstractions of data and using these abstractions to identify patterns—much like the way people learn through changes in the configuration of the neurons in their brains in response to various stimuli. Obviously, a benefit of ML systems is that they are able to analyze data at a speed, scale, and depth of detail that is beyond human analysis (Reavie, 2018).

These firms all show that AI can be leveraged in a variety of ways to: generate new business insights; improve core operating processes; enable faster, better decision making; take advantage of changing value chains; and create new data-centric businesses. As BCG (2013) points out, competing through lower cost, better products, and innovation are not new, but driving all these with data and AI is now central to a firm's success, especially as data processing and storage costs have decreased by a factor of more than 1,000 over the past decade. While more and more firms are realizing that there is value to be extracted from the massive amounts of data being generated every day, only a few are truly incorporating AI into their business. These firms are some of the latter. Their strategic and tactical application of AI shows how it can affect all aspects of a firm, as Figure 11 below shows.

Figure 11. Example on how Firms Can Extract Value from Data.



Source: BCG (2013)

Furthermore, the broad application of AI by these firms shows that business models and capabilities in virtually every sector of the economy are being reshaped by AI's use of data, with applications that will impact a wide range of sectors from education, travel and leisure, and finance to media, retail, and advertising. Incumbent firms may rely on certain standardized data to make decisions, whereas new firms (such as those profiled here) are using new data sets (such as orthogonal data), which leads to reshaped competition in and between sectors. A general example is that insurance companies are using telematics data (i.e., location/GPS data) to derive insights into customer behavior (such as driving), which is beyond the usual demographic data used for insurance underwriting (McKinsey & Company, 2017). Another example is in marketing, whereby firms use behavioral characteristics to engage in

micro-segmentation[123], in addition to other key demographic characteristics (e.g., breaking a person's geography down from economy to state to city to neighborhood or for behavior that could mean frequent purchases, seasonal-only purchases, or window shoppers).

Interviewed firms' business models differ in terms of where data comes from and how it is used. For Mindbridge Ai and Pondera Lab, they are not data collectors (i.e., not data controllers) themselves but rely on clients to provide access to their data to either help develop or to use as part of their AI and data analytics services. For example, Mindbridge Ai's data-driven business model is indicative in that clients use AI Auditor to process their data, so that they receive benefit from the insights that the platform is able to provide about their data. AI Auditor allows clients to learn at three levels: at the local level in "unsupervised" learning; at the "tenet level" in how clients respond to insights and use it to change business operations; and at the "service level" through curated learning through the insights provided by ML and AI.

Certn is also not a data collector, but a data aggregator in that its services are based around identifying, accessing, and analyzing data from established third-party sources. Certn's value-add derives from accessing a broad range of databases and sources to identify the right person and to correctly attribute information about this person to them when undergoing assessment by a customer.

For all firms, a major challenge is not only collecting data, but in how they organize and analyze it. Their experiences are indicative of the fact that for every firm, in every sector, "big data" means something different in terms of how the data comes from various sources and how it appears in multiple formats. In many cases, data arrives unstructured, which requires firms to develop algorithms to analyze and organize it into useful information. This process lies at the heart of their data-driven, value-added services.

7.4. How Policies and Regulations Impact Firms' Business Models

Firm interviews revealed two main types of rules and regulations that affected their use of AI for digital trade: (i) the rules on data, and (ii) source code protection.

Laws and regulations on data collection, transfer, storage, sharing, and use affected how all of these firms were able to use AI to engage in digital trade. The impact of these laws and regulations, such as for privacy and regulatory oversight, can be either direct or indirect depending on whether the firm is a data controller (i.e., collector and manager of data) as opposed to simply providing data analytic services for clients to use with their own data. However, a clear point that came out of each interview is that AI-based firms need to be supremely vigilant in reviewing the legal and regulatory environment in each market in which they operate to assess compliance-related risks.

Data protection and privacy rules are central to how AI-based firms operate. How economies set the rules about collecting, sharing, and using personal data can have a major impact on AI. In some cases, firms outlined how it reduces the availability of data that AI can use.

Beyond mandatory compliance activity (due to local laws and regulations), policymakers also need to recognize that there is significant pressure from clients about how firms manage and protect data. Many of the firms interviewed mentioned that much of their compliance activity, and parts of their delivery

[123] Micro-segmentation involves layering hundreds or even thousands of data points to identify granular clusters of individuals. See: https://blogs.oracle.com/oracledatacloud/targeting-in-the-age-of-micro-segmentation

of business services, was done to satisfy their clients' perception of compliance risks, even if it was not legally mandated.

All firms mentioned the importance of protecting their AI/ML, whether this is through source code protections, the use of contractual arrangements, and/or the use of technical and administrative controls to manage access and use. This meant avoiding certain markets due to the risk of hosting their AI-based services on local cloud services, due to the unacceptable risk this would pose to their system as they could not trust local cloud providers. Some economies have formal or informal rules/practices that make source code disclosure a requirement for market entry.

Data-related laws and regulations that support the role and flow of data

Data privacy laws

For all firms, data privacy laws and regulations are central to their use of data in the economies in which they operate. Data privacy laws define who is legally authorized to collect, store, and use one's personal information, and they are intended to protect individuals from three types of injuries: harm to one's autonomy (such as involuntary disclosure of sensitive information); discrimination (such as denied access to housing, credit, or employment); and economic harm (such as in the case of identity theft or fraud) (McQuinn, 2018). The starting point for firms in their decision to provide services in other economies (i.e., engaging in digital trade) is conducting a legal review of local laws and to compare these against laws in their home economy and major "benchmark" economies, such as the United States and the European Union. This analysis considers how local laws would impact how the firm typically uses data at home and whether it can (generally) deploy existing data analytic services with no changes.

Pondera Lab uses legal services specializing in data-related issues, especially those related to privacy and the legal framework for how the firm will access and use their clients' data as part of their services (the latter will be addressed below). Pondera Lab manages this for all its clients, whether based in Mexico or elsewhere in North or Latin America. On privacy, Pondera Lab develops individual legal contracts to account for any privacy-related legal requirements of a client's home economy, but this is often built on Mexico's privacy framework, which Pondera Lab considers to be robust. This tailored approach works for most clients given their home economies have compatible and comparable privacy frameworks. If clients have specific privacy concerns, they are able to specify these as part of the contract they sign with Pondera Lab.

Mindbridge Ai builds to a "high water mark" in terms of meeting the strict privacy framework in which it operates, and complements this with externally audited compliance measures, which are then demonstrated to clients in product use and customer service. Given it is the strictest, Mindbridge Ai considers the GDPR to be the "high water mark" of data-protection regulations. The focus on GDPR is also driven by the fact that non-compliance penalties are huge. Beyond Europe and the GDPR, Mindbridge Ai has to manage the challenge of differential privacy protections, such as different state-level requirements in the United States.

Certn's use of data is mainly affected by Canada's federal privacy law as well as some provincial privacy laws (especially in British Colombia, Alberta, and Quebec). Furthermore, Certn keeps updated (and where necessary, makes adjustments) on the latest interpretations of the law, as issued by the Canadian Office of the Information Privacy Commissioner. Certn finds Canada's privacy framework to be generally supportive of data-driven innovation. Certn's internal data privacy and protection procedures are regularly audited by Canadian government authorities. In the case of an audit, Certn's cloud storage provider (Amazon AWS) makes it easy by providing all the relevant documents and certifications about how it stores and protects Certn's data.

From its launch, Certn has worked with Canada's privacy regulators and other government agencies and leading privacy compliance professionals from across North America to ensure its data-

management processes are both legal and ethical. Certn has worked with the U.S. Federal Trade Commission (Fair Credit Reporting Act), the U.S. Department of Housing and Urban Development (Fair Housing Act), and the Canadian Office of the Information Privacy Commissioner. Certn never looks at race, religion, sexual preference, family status, or any other characteristic protected by any economy's human rights legislation. Certn does not analyze photos, nor does it review content that is not public. For example, Certn never looks at social media profiles that are set to "private."

Data storage, data protection, and data accessibility

All firms stressed the importance of understanding data governance issues as part of their daily engagement with customers in their home economies and overseas. Highlighting (again) the importance of cloud services, all firms emphasized that their AI-based services are designed for the cloud, in part, as it provides ready and dependable access, good cybersecurity protections, and scalability to meet client demand. However, as with Pondera Lab, the firms need to tailor these cloud services for each client given local legal requirements, which affect cost, complexity, and accessibility of their services.

Many firms go beyond the strict legal requirements in how they manage and protect their data. For example, Mindbridge Ai stated that their broader approach to data protection emphasizes a focus on both administrative and technical compliance with data protection requirements. Administrative compliance relates to contractual controls about data access, use, and protection a firm sets with its client. Firms use technical controls for data access and protection, such as two-factor authentication and monitoring and logging of data access and use. Furthermore, many firms mentioned their use of third-party certifications to prove that their firm's IT systems, or that of their provider (in the case of cloud storage services), are designed to keep its clients' sensitive data secure.

Pondera Lab relies on globally distributed cloud services. Regarding data access and use, Pondera Lab needs to develop a legal framework with each client to govern how it will access and use their data and how it can deploy or develop AI-based platforms as part of its services. A key question for clients is how to manage cloud service arrangements so that Pondera Lab can access its clients' data. For example, can Pondera Lab use its preferred cloud provider to host its AI/ML platforms, which then needs a legal and technical framework to access data in the client's cloud service provider to develop or provide AI-based data services. Otherwise, Pondera Lab needs to develop a legal framework to manage its access to and use of a client's own cloud service provider in order to develop customary AI/ML platforms and/or upload off-the-shelf data analytics platforms.

Mindbridge Ai uses cloud services with data centers in Canada, the United States, and the European Union as these are the three core markets in which the firm operates. From this base of operations, for every client that operates in another jurisdiction, Mindbridge Ai conducts a review of a client's regulatory environment (at the state/provincial and federal level) to check whether its services comply with local requirements. If Mindbridge Ai does not find any regulatory issues, it will offer to provide its solutions from cloud services from data centers based in Canada. Mindbridge Ai stipulates for these clients that its services will be governed by Canadian law, and if the client does not accept that, then the service is not provided. Thus far, Mindbridge Ai has not had to decline services based on this jurisdictional clarification. Beyond ensuring its services are compliant with (mandatory) local laws, Mindbridge Ai uses voluntary, externally accredited and audited certification measures to demonstrate its commitment to best practices in terms of data protection and security.

Intellectual Property Protections - Mixed

There is no single template for firms involved in AI/ML in how they seek legal protections for their inventions and the underlying data they use.

Given that the intellectual property laying at the heart of their business model is intangible (in the form of source code), it is susceptible to exposure and theft. There are several potential scenarios that pose a risk to source code. There is the threat posed by hackers gaining unauthorized access to the software

hosted on a foreign cloud service provider. At the other end of the spectrum are mandatory source code disclosures, as considered by a number of economies. Mindbridge Ai and Pondera Lab mentioned the importance of implementing specific measures to protect their AI-based services, involving legal, technical, and administrative arrangements.

Mindbridge Ai pursues strict internal control over the intellectual property that lies at the heart of its AI- and ML-driven data analytic services. However, it has not run into IP-related issues that negatively affect its operations. Yet, Mindbridge Ai is aware of the potential risks to its IP in certain markets that it does not currently operate in. The source code at the heart of Mindbridge Ai is largely protected in how its software is developed and deployed. Mindbridge Ai only does service development on data centers based in Canada, and therefore, is protected by Canadian law. Mindbridge Ai also employs internal controls to carefully manage product development so that source code is not inadvertently exposed and therefore copied or reverse engineered. Furthermore, Mindbridge Ai files relevant IP filings to ensure its products are protected from hostile filings. As with most cloud-based platforms, the compiled form in which its product/code is deployed to cloud services in Canada, the United States, and the European Union for clients to use and feed data into means that it is largely protected from reverse engineering.

Pondera Lab recognizes that the custom models it develops and uses are the result of its intellectual capital, so it needs to ensure that it uses IP protections to maximize the value from them. To protect its algorithms, Pondera Lab registers relevant IP in the United States. While U.S. law explicitly mandates copyright protection for software[124], actual protection of software has been significantly limited due to case law (i.e., the U.S. Supreme Court's Alice Corp. v. CLS Bank case). Copyright protects against literal infringement of the text of the program. In this regard, source code can be protected under copyright as literary work.[125] Pondera Lab registers its IP in the United States and sees the provisions on source code protection in new trade agreements (The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the United States-Mexico-Canada Agreement (USMCA)) as holding the potential to change this situation in some economies.

Data-related laws and regulations that limit the role of data

Privacy

When considering providing services in a particular economy, firms outlined how they each assess whether the new market has privacy rules which require changes to their systems. Each firm then weighs up the market opportunity against the impact (technical and financial cost) of having to modify its core services to account for these local laws. The latter may be higher than the former, especially in the case the contract is likely to only be a one-off.

AI-based services are a highly competitive sector and so having to modify fairly standardized cloud-based analytics platforms for each and every economy may not be viable for every firm given the 'back end' cost in terms of ICT services, data engineering, and other activities that are related to providing the firm's services. This highlights the importance of economies of scale to AI-based models and the incremental impact that differential data-related laws and regulations have on a firm that provides AI-based services, in that major requirements (such as local data storage and source code disclosure) obviously entail significant costs, but that smaller requirements in aggregate can be just as significant a barrier to entry.

[124] https://www.law.cornell.edu/uscode/text/17/101
[125] https://www.law.cornell.edu/uscode/text/17/101

Mindbridge Ai's strategy is to essentially develop its AI-based services so that they are compliant with the strictest privacy framework in the market in which they want to target—i.e., to build to a "high water mark." However, Mindbridge Ai does run into privacy legislation that can be problematic to comply with, so it sometimes avoids working with clients in certain sectors. For example, America's HIPAA requirements have constrained its ability to provide its solutions in America's health services sector. In some cases, Mindbridge Ai has provided its Auditor AI service to clients that are covered by HIPAA, but in order to do this, the client has requested that Mindbridge Ai not use its U.S.-based cloud services, but instead deploy its AI-based platform onto the client's on-premise data center. These types of requests are not strictly required by law, but are based on how the client chooses to be compliant with HIPAA. These custom deployments add initial costs to deployment (as opposed to using cloud services), but the real costs and complexity come after deployment, when Mindbridge Ai has to provide software updates and customer support services, as it does not have remote access to the client's platform, for example, to check the access logs and other details when something goes wrong. This adds considerable technical difficulties, especially if Mindbridge Ai were to accept such requirements from a growing number of clients, as it would effectively remove a major benefit of using a centralized, cloud-based service.

Certn's general view of data privacy at the domestic level in Canada and the United States is that it is generally supportive of data-driven innovation. At the broadest level, data privacy across both economies is similar in that they mention similar things, but in slightly different ways, which is where complications arise. The big difference is that managing these differences across the 10 provinces of Canada is much easier than across the 50 states of the United States. For example, two Canadian provinces require local data storage for personal data (outlined below). In the United States, different state laws and regulations affect fairly standard employee data in very different, often complicated, ways. The challenge in navigating these differences is that it is quite common for customers to be considering people/applicants who have lived in multiple states, therefore meaning the (same or similar) data for a single person can be simultaneously governed by multiple laws/regulations. Furthermore, U.S. states manage access to data in very different ways, which also complicates integrating the same data sources into a single platform. For example, criminal records in California require a manual application process for Certn to gain access, while in Colorado, the same data is available online and is accessible to automated services (such as Certn's cloud-based platform).

Certn does not provide services in the European Union as yet. However, Certn has made the up-front investment to build procedures into its AI-based services with the goal of eventually being GDPR-compliant. This has required a significant investment of time, money, and effort, including seeking outside legal and privacy consultants and expertise[126]. GDPR sets a high bar that is (at least initially) difficult for a small start-up like Certn to meet. During its early, formative stage, accounting for GDPR compliance was challenging and costly as it required Certn, as a start-up, to have the compliance regime of a big firm. This extended to physical security requirements at Certn's office and doing extensive background checks on its own staff. Furthermore, it required Certn to have full-time staff dedicated to

[126] For example, the GDPR calls for the mandatory appointment of a data protection officer (DPO) for any organization that processes or stores large amounts of personal data, whether for employees, individuals outside the organization, or both. In terms of potential the potential cost and impact of having a DPO, one study from the University of Milan Biocca, Ca' Foscari University Venice, and the Denver-based Analysis Group estimated that if the data protection officer provisions of the European Union regulation are implemented as written, it would cost each effected European small- and medium-sized enterprise as much as €7,200.00 in additional compliance costs per year. See: Lauritis R. Christensen, Andrea Colciago, Federico Etro and Greg Rafert, *The Impact of the Data Protection Regulation in the EU* (Denver: Analysis Group, 2013).

data protection and security at an early stage, which is a major cost. In essence, GDPR increases the up-front cost of entry for a start-up AI-based firm like Certn. However, in making an assessment of the market risk and opportunity, Certn judges that making this investment will eventually pay off in being able to target bigger clients by being able to show that the company complies with the GDPR. Certn's long-term strategy in aiming for GDPR compliance is that meeting such a "high water mark" standard will make it easier in expanding to other economies with a similar, but less burdensome, privacy framework, such as Australia and New Zealand.

Data storage, data protection, and data accessibility

Requirements to store data locally pose a major risk to AI-based firms as they cut them off from the data that lies at the heart of their business model. A growing number of economies are enacting data localization, for a variety of reasons, such as privacy, cybersecurity, digital protectionism, and guaranteed government access to data. AI benefits from the quantity of data (e.g., merging of data sets from different economies etc.), but also the diversity of data, in that AI predictions will be better if the algorithms have access to a greater range of data. Economies which enact data localization policies limit the ability of foreign AI firms to achieve economies of scale, while protecting the ability of local AI firms to exploit local economies of scale, but at the cost of lower-quality AI predictions and services.

A major issue for Certn is that two Canadian provinces have implemented laws mandating that personal data held by public bodies such as schools, hospitals, and public agencies must be stored only in Canada. The British Columbia Freedom of Information Protection of Privacy Act and the Nova Scotia Personal Information International Disclosure Act apply to personal information in the custody or control of public bodies. This requires Certn to store personal data locally in these two provinces, which it does through its primary cloud provider (Amazon's AWS), which happens to operate data centers in these two provinces. Therefore, Certn is fortunate in that this local data storage requirement does not disrupt its IT systems in a significant way. However, as it expands, it does raise the issue of cost and complexity from using multiple data centers (even if via a central provider) and not being able to aggregate all its data.

Mindbridge Ai uses cloud services based in Canada, the United States, and the European Union as these are its three core markets. Mindbridge Ai stipulates that for clients outside these economies its services will be governed by Canadian law, and if the client does not accept that, then the service is not provided.

Pondera Lab uses a global cloud storage service. In limited circumstances, Pondera Lab's clients (mainly some Mexican government agencies and financial firms) require that their data only be stored in Mexico. Local data storage requirements disrupt Pondera Lab's use of its preferred (in terms of cost, accessibility, and security) cloud service provider.

Furthermore, in limited circumstances, clients will specify that Pondera Lab will only be able to access their data from their premises, which is a major operational barrier to its services, given it relies on remotely accessible cloud services. The framework the client wants has a significant effect on the cost and complexity of the service Pondera Lab provides. Many of Pondera Lab's clients, at least initially, are concerned about sharing data with the firm. This is understandable, as these firms need to ensure their data (whether personal, operational, or transactional) is protected and secured (e.g., not disclosed to competitors). Clients need a clear understanding about how Pondera Lab will use and protect their data.

7.5. Conclusion

As this chapter shows, there are a range of data-related laws and regulations that can affect how firms using or offering AI provide their services. AI-based firms stand to be major players in digital trade as technological change reshapes economies. It holds enormous potential to drive productivity and

innovation in service sectors, which comprise a growing share of many economies. Being based on low-cost, scalable global platforms means that AI-based services can basically be delivered from, and-to, anywhere. These interviews are indicative of the fact that just because a technology or service may be globally deliverable and accessible, does not mean that it ends up being that way due to government laws or client perceptions of regulatory risk. As this chapter shows, there exists a range of data-related laws and regulations that can affect how AI-based firms approach digital trade in providing their services and products across borders. At its heart, this chapter shows how certain laws affect the critical concepts of economies of scale and scope that are critical to the use of AI in digital trade.

A key theme in the interviews is that in cases where there are local data requirements, firms need to weigh up whether the compliance risk and cost is less than the market risk (in terms of bringing its service into line with a jurisdiction's laws and regulations in order to serve clients in that market). As one of the firms stated: there are two demands for data protection and security requirements, to be secure and to feel secure. Firms do the former as a matter of fact, but also have to do a range of things for the latter that may not be strictly necessary, as there is a market risk in clients not willing to take on additional perceived risk. But this highlights the broader impact that data-related rules and regulations can have on how firms manage data in that even if economies do not call for explicit local data storage requirements and call for the free flow of data, barriers to data flows may be the de facto result due to compliance risks. The indirect impact leads some firms to specify requirements above-and-beyond what is legally required, which affects how firms use data.

Designing data privacy and protection frameworks involves a complex process that must address a wide range of legal and regulatory issues. Economies of all sizes and levels of development are grappling with this challenge, which is understandable given the impact digital technologies have had on our societies and economies. The challenge for policymakers is to fully understand digital technologies and balance various competing goals, such as consumer privacy, productivity, and innovation.

The interviews highlighted that getting this balance right is a major challenge. Despite the significant benefits to companies, consumers, and economies that arise from the ability of organizations to use, share, and analyze data, including through AI-based technologies, a growing number of economies have enacted or are considering policies which may act as a barrier to AI-based digital trade.

Another key issue is the impact of data protection laws. A number of firms mentioned that they often have to work with policymakers, especially outside their core markets, who may misunderstand data privacy and data protection. Some policymakers justify restrictive data privacy laws and data localization requirements on the premise that they want their citizens' data to be protected by the laws of the economy. But as interviews with these firms demonstrate, the location of personal data storage is separate to holding the firm responsible for its management of personal data originating from an economy. If a firm has a legal nexus in an economy, the laws and regulations of the economy apply. That was most definitely the case for each firm interviewed. Similarly, for data protection, many policymakers associate the geography of data storage with cybersecurity. But the confidentiality of data generally does not depend on the geographical location where information is stored. Data security depends very much on various factors including the technical, physical, and administrative controls put in place by the service provider. For the firms interviewed, they relied on global, best-in-class providers in part as they recognize their ability to provide a high level of cybersecurity protections.

Firms also mentioned the cumulative impact of data-related laws and regulations. Due to the APEC members covered (those of North and South America), the firms interviewed detailed issues (mainly) about North America, Latin America, and the European Union. However, they also referenced the impact of policies they had encountered outside these regions, especially when considering expansion to new economies. This highlights the importance of adequate IP protection, especially source code protection. This is important, as most economies in North America and the European Union have a predictable and stable business environment, including a strong rule of law. When dealing with sensitive and potentially significant technologies, firms are understandably reluctant to enter into non-core

markets where they are not assured of the same degree of control and predictability. What this means is that firms may decide not to enter certain markets or take on one-off clients from economies outside these regions due to the regulatory uncertainty and risk and due to the corresponding cost and complexity involved in tailoring (often global) IT systems for local conditions. This highlights the broad spectrum of considerations that AI-based firms face in deciding whether to engage in digital trade—explicit vs. implicit requirements, regulatory compliance vs. market opportunity, client vs. government-driven requirements.

At the strategic level, given the critical role of data and emerging competition in AI, it is also worth considering the longer-term implications of divergent data-related policy frameworks in the key markets. Different laws and regulations can advantage AI firms in some economies, given the impact they have on economies of scale and local externalities, while disadvantaging foreign firms. The central role of data to AI means future trade policy will likely focus on these points of friction and/or interoperability. Where it is the former, current literature already shows that policies which limit services trade, for example by restricting market entry and foreign investment in services markets, or by impeding online cross-border supply, constrain the development of the digital economy (Roy, 2017). But a growing number of economies have started the process of enacting rules that protect data flows and address other AI-related trade issues, such as source code protection. Which side prevails in setting the global standard on data and digital trade will play a part in determining the impact of AI and other data-driven technologies in driving economic productivity and innovation.

CHAPTER 8: CONSUMER SERVICES[127]

8.1. Sector overview

Services dominate the general economic output of APEC economies representing about 70 percent of total APEC output. The different levels of economic development within APEC means that the share of services in economic output varies across economies[128]. However, the share of services in APEC trade is small compared to manufacturing. In 2016 services represented about 17 percent of total APEC exports below the world average of 19.8 percent[129].

Energy

Energy services are often locally produced and consumed with minimal trade in the generation, distribution and retailing of energy between economies. This is because of the often natural geographic barriers to supplying energy from one economy to another. Nevertheless energy services that are tradeable between economies include those of a digital nature such as the provision or smart metering services in homes and businesses which enable consumers to control their energy use; platforms which facilitate trade in energy based securities such as hedge pricing; and software and systems providing transparent information on comparative retail pricing which consumers can rely on to choose energy suppliers in their local markets[130].

Healthcare

Data and data flows underpin a range of healthcare activities. These include for example:

- General practitioners and specialists collect and store patient data to assist ongoing patient management. Usually this data is stored locally within a practice for access by an individual doctor or group of doctors treating a patient within that practice.
- Patient data can be shared by medical professionals and allied health workers who are involved in treating the same patient. For example, a patient with diabetes may be treated by a general practitioner, endocrinologist, and allied health workers such as a podiatrist or home nurse. Each practitioner would generally collect and store their own information about the patient and share relevant information with other practitioners where necessary to assist patient management.
- Laboratory and imaging centres which are involved in conducting a range of patient tests collect data which the store locally and share with medical practitioners who have requested these tests.
- Where jurisdictions have developed an electronic health record system, patient information is stored centrally in data centres and can be shared amongst any medical practitioner who may be treating the patient for any type of medical condition. Electronic health record systems are often promoted as beneficial to patients because they allow medical treatments to be fully informed by the complete record of a patient's health, thereby reducing the risks of inaccurate diagnosis and treatment. These systems also improve efficiency because they relieve the patient and doctor of the need to discuss the patient's medical history each time the patient seeks new or ongoing medical treatment.

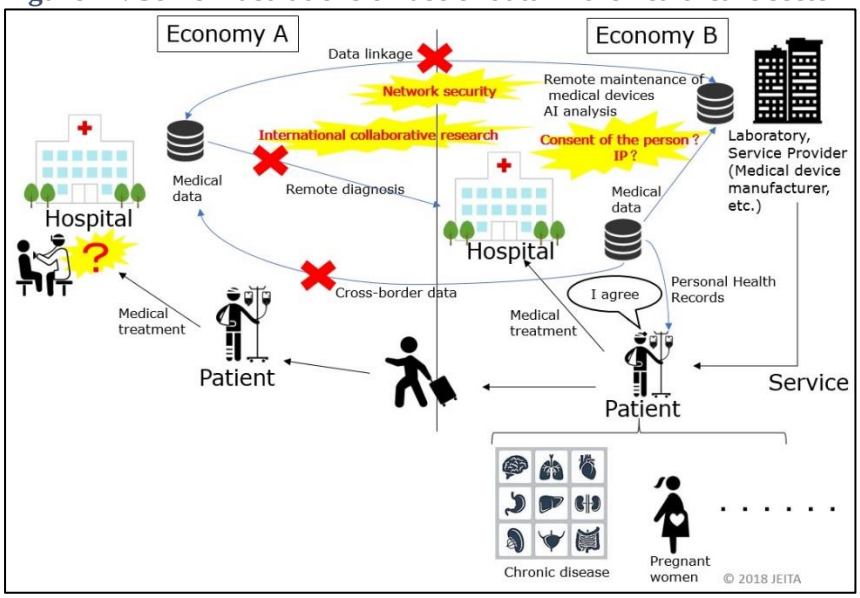
[127] This chapter discusses the collective views of four firms consulted in the consumer services sectors (energy, healthcare and education publishing). This grouping has been selected because: 1) There were not a sufficient number of firms in each sector to justify separate chapters on each; 2) The firms did not express different views to those reported in the other chapters in this report.
[128] APEC Committee on Trade and Investment, Report to Ministers: Collective Strategic Study on Issues Related to the Realization of the FTAAP 2016, p75
[129] Ibid
[130] Aegis Consulting Group

Electronic health records tend to be more acceptable to patients if there are strict regulations governing access to their data, including the requirement for their consent to any data sharing.

- Hospitals rely on effective data sharing within clinical settings to ensure the accurate and efficient management of patients. For example, patients admitted to the emergency department of a hospital with life threatening injuries or conditions may need to be managed through surgery, an intensive care unit, a recovery ward and when the patient returns home. Simple solutions can often improve data management and deliver benefits. For example, studies have estimated that the use of laptops at patient bedsides by medical staff to record and monitor patient information can deliver a 30 per cent improvement in clinical productivity including reduced staff time and increased accuracy in treatment[131].
- Pharmaceutical companies collect patient data through clinical trials and via the clinical research conducted by medical practitioners prescribing their drugs. This data is critical to the research and development of new and improved pharmaceuticals. The costs of pharmaceuticals to individual patients in private medical systems and the taxpayer in government subsidised systems can increase when patients are prescribed drugs to which they have adverse reactions such as heightened side effects. Costs rise because patients may have to be prescribed numerous versions of medication before they find one that suits them. To avoid these risks, pharmaceutical companies are investing in DNA testing systems to assist medical practitioners target suitable medications to patients. This will require the sharing of highly sensitive and unique patient data and regulators will need to develop sophisticated regimes to govern this.
- Governments and private health insurers need to access and analyse high level data from clinical contexts to monitor and develop appropriate policy and insurance solutions to existing and emerging healthcare and health system priorities. The efficiency of healthcare funding in private insurance or government subsidised systems relies on insurers and governments understanding the capacity and limitations of funding to influence patient behaviour, prevent illness, manage chronic disease, and deliver improved clinical outcomes in hospital and non-hospital settings.

Some of the ways by which data are used in the healthcare sector and their potential implications if restricted are illustrated in Figure 12 below.

Figure 12. Some illustrations on use of data in the healthcare sector



Source: JEITA

[131] Aegis Consulting Group, work conducted for Cisco, IBM and Dimension Data in Australia

The future use of AI in healthcare will rely fundamentally on the availability of high-quality data in standard formats that can be collected and shared in the different clinical contexts referred to above. The specific and sometimes conflicting interests of participants in the healthcare sector can be barrier to the standardisation of data collection, analysis and sharing to achieve this. For example, health practitioners can be resistant to efforts by insurers and governments to understand funding flows to improve efficiencies. Attempts to standardise data collection and centralise storage in integrated databases can be resisted by health consumers and practitioners if they are not satisfied with privacy controls and data security measures.

Education publishing

Data and data flows in education publishing can take various forms. These include for example:

- The investment in technology such as computers and other devices to improve student access to educational material published on networks or online. For example, " EdTechXGlobal and Ibis capital estimated that schools spent nearly $160 billion on education technology, or ed tech, in 2016, and forecast spending to grow 17 percent annually through 2020. Private investment in educational technology, broadly defined as the use of computers or other technology to enhance teaching, grew 32 percent annually from 2011 through 2015, rising to $4.5 billion globally"[132].
- The use of the internet to distribute educational material across the globe. The internet has created two critically new opportunities for producing and circulating educational material. Firstly, it has enabled the production of digital material that can be updated on a regular basis for all users simultaneously. This has benefits for producing text book material used by primary, secondary and tertiary students as well as material used by professionals undertaking continuing education. Secondly, it has transformed access to education material by making information available to students with internet access, no matter how remotely they live and regardless of the existence of any other educational institutions or infrastructure. Accordingly, the internet has enabled the most current educational information to be accessible almost universally and in real time.
- Data gathered within teaching environments on student and teacher performance can be used to quickly improve the production and distribution of educational material to maximise learning outcomes.
- The availability of data on industry and business needs in economies can better inform educational material and tailor coursework to increase the employment opportunities for graduates.
- Algorithms within AI can be used to assess the local, domestic and global data on student performance and the contribution of available educational material to comparative results.
- AI is likely to increase the opportunities for virtual and personalised learning, thereby expanding the opportunities for the production of tailored educational material.

8.2. Profile of firms interviewed

The four firms whose views are reflected in this chapter are headquartered in Australia; Japan; and the Philippines. Of the four firms, three have international operations involving cross border trade. The largest firms employ over 20,000 staff and the smallest employ about 20 people.

Firms A and B provide energy-related services:

[132] McKinsey Global Institute, Artificial Intelligence, The Next Digital Frontier, June 2017, p.65

- Firm A supplies smart meters and provides metering services. These include meter installation, monitoring and collection of energy use data and provision of that data to energy retailers for customer billing purposes and network providers for the purpose of network load management.
- Firm B collects real time pricing data from energy retailers and converts that for provision to energy consumers to assist their choices about energy supply and tariffs. Energy retailers participate in this scheme because it provides an alternative distribution model to their business marketing and therefore expands their reach to potential consumers.

Firms C and D provide other consumer-related services:
- Firm C provides healthcare consulting such as policy planning to support the establishment of medical institutions.
- Firm D is a publisher of education material which provides digital content worldwide.

8.3. Role of data in firms' business models

The common ways in which consumer services firms collect and use data include the following:

Collection and use of customer data
- Collect personal data of individual customers via processes customers use to purchase services.
- Collect the business data of suppliers/customers upstream and downstream in the supply chain.
- Use personal and corporate data of customers to develop, tailor and offer account management and loyalty scheme services including the design and promotion of price discounts, service consolidation, improved service convenience, new services, and ancillary benefits to reward customer loyalty.
- Collect customer data to facilitate regulatory compliance with trading requirements.

Collection and use of their own business data
- Collect performance data from infrastructure assets such as energy smart meters and manufactured goods. This generally occurs remotely when assets are operating. The collection of data remotely is generally facilitated by satellite and GPS technology.
- Use performance data to monitor and assess the safety, capacity and efficiency of asset deployment. This enables firms to evaluate ways to ensure safety, improve cost recovery, enhance customer responsiveness and optimise competitiveness in new or existing markets.

Nature of data being managed

All firms manage significant volumes of data. This includes:
- Business data of clients which is analysed and used to provide consulting advice.
- Business data of corporate clients which is analysed, transformed and transmitted for public consumption.
- Personal data of consumers which is analysed, transformed and transmitted to upstream and downstream businesses in a supply chain.
- Personal data of consumers which is assessed for use to promote and tailor products to those consumers based on their preferences.

Firms were asked to describe the nature of their data use and provide examples of business activities dependent on or arising from this data use. Firms were given options for data use which are based on the four common forms of digitalisation. Table 15 below illustrates the four kinds of digitalisation and examples provided by firms of business activities relying on this data use

Table 15. Ways in which different kinds of digitalisation support business practices

Kinds of digitalisation	Examples
Principally online ordered and online supplied products/service	• Provision of e-books.
Principally online ordered products or services that are then supplied offline (i.e. physical products or services provided offline)	• Supply of energy smart meters where consumers order meters online but meters are physically installed.
Principally offline products or services	• Provision of healthcare consulting services.
Online network, platform or matching service (i.e. enabling other entities that supply relevant products or services)	• Provision of energy pricing and product information to consumer markets to support sales by retail energy firms. • Remote monitoring of energy smart meters and provision of data to energy firms for customer billing and network control purposes.

Source: Consultation with firms

How data flow enables the business

All firms consider that data flows are integral to their business operations. The collection and management of data is an enabler to support three key business activities in particular. These are:

- Customer relationship management;
- Operational efficiency; and
- Dynamic pricing of service offerings.

In competitive markets, these business activities are critical to growing market share amongst customers and reducing costs of service without compromising safety.

All firms report that customer relationship management is a key focus of their data strategy because it is essential for business success. Customer relationship management includes:

- Understanding customer needs and preferences;
- Offering direct and ancillary services and promotions targeted to customer preferences;
- Rewarding customers for loyalty including; and
- Securing repeat purchases from existing customers.

Data flows enable some all-encompassing high-level business activities ranging from sourcing inputs and suppliers to customer relationship management, enterprise planning and monitoring the performance and use of services and products. These are described in the table below. Firms were asked to explain what these business activities mean in practice for their daily operations. Their responses are captured in Table 16 below and illustrate what kinds of essential business practices are enabled by data flows.

Table 16. Kinds of business practices relying on data flows

Kinds of business activities enabled by data flows	Examples
Sourcing and procurement of inputs and suppliers.	• Provision of client business data to inform healthcare consulting services. • Provision of client business data to inform energy consumer market.
E-commerce or other sales and supply to customers directly or via third party platforms.	• Sales or published material including e-books for education purposes.
Invoicing and payments.	• Customer and supplier payments.

Kinds of business activities enabled by data flows	Examples
Customer relationship management (CRM).	• Corporate account management. • Consumer market management.
Enterprise resource planning (ERP).	• Supply of energy smart meters in line with planned roll out to customers by energy retailers.
Monitoring usage of services/products such as consumption of utilities and infrastructure.	• Remote monitoring of consumer energy use to inform energy retailers and distributors for customer billing and network management purposes.

Source: Consultation with firms

Data storage options

Three firms shared that they store all information in the cloud outside of its head office. In this case two firms use cloud services provided by specialist third parties and two firms use cloud services built by them.

Use of artificial intelligence (AI) and blockchain

None the firms are using AI and/or blockchain. However they all view these technology developments as a positive one for their businesses and future customer relationships. In the energy sector, firms view AI as an important tool to assess the impact of appliances on the load in energy networks and best practice pricing.

Data security and privacy governance

All of the firms suggest that they take a systematic approach to data security. Their methods include all or many of these activities:

- Ensuring their policies, procedures and practices are consistent with international quality assurance instruments governing data security and privacy. This is primarily achieved by firms ensuring they are compliant with ISO27001 and BS10012.

- The systematic and regular review of local laws and regulations governing data security and management to ensure compliance. These local laws can include the personal data protection and privacy legislation in Australia, Japan and the Philippines. In the energy sector it can also include industry specific regulations including domestic energy network rules in Australia.

- Applying a sophisticated and comprehensive data governance framework which consists of firstly classifying all data according to its sensitivity and secondly restricting access within the firm to data according to levels of sensitivity.

- Regulatory compliance and cyber security awareness and best practice training for all staff involved in handling business and customer data depending on the level of data staff members are authorised to manage. Various staff within each organisation are responsible for handling and managing data including its reporting, security and privacy.

- Managing data flows within secure, transparent and auditable frameworks. This includes assessing the most secure and trusted hardware and location when choosing storage infrastructure; employing

their own cyber protection teams which are heavily involved in the design and operation of selected hardware and the flow of data; and applying end-to-end encryption on all data flows across borders and over the Internet.

Most firms have governance structures where management must report against data security and privacy key performance indicators. In most firms, this reporting occurs between layers of management and between management and the Board. Firms contain specific executives with ultimate responsibility for data security and privacy management. This is either the General Counsel or Chief Information Officer.

Key performance indicators that firms use to manage the compliance of their organisations and staff with data security and privacy regulations and standards, tend to be based on indicators to support planning, doing, auditing and improving.

Brand trust from good data management

All firms consider that consumer trust in their brand is integral to their business operations and capacity to compete effectively in domestic and international markets. They all implement data privacy and security policies and practices to preserve consumer trust.

8.4. How policies and regulations are impacting their business models

Applicable data regulation and compliance costs

All firms report being subject to the relevant privacy and personal data protection legislation in their host economies and other APEC markets they operate in. Some are also subject to the EU's GDPR if they provide services to EU residents.

Direct costs

Firms reported a range of direct costs associated with regulatory compliance, although these were accepted as part of doing business. Some costs that were highlighted were:

- Development and operating costs associated with the need for separate data management systems in economies. This can lead to some information functions being disabled and services being unequally provided depending on the requirements in economies.

- Administrative costs of providing compliance documentation which can be a burden for MSMEs.

- Energy services need to comply with various regulatory measures such as customer frameworks, market conduct rules, and network regulation. The provision of smart meters must also comply with regulation in other markets which regulate hardware and software used by meters. For example energy smart meters contain 3G microchips and therefore must also comply with telecommunications regulations.

Firms indicated that regulation creates a range of costs of the kinds explained in Table 17 below

Table 17. Kinds of compliance costs reported by firms

Kinds of compliance costs	Examples
Recruiting specialised staff to improve compliance and/or reduce risk.	• Employment and/or contracting cyber security to oversee the design and management of hardware and processes to gather and store information.

Kinds of compliance costs	Examples
Investing in new infrastructure and information technology architecture to improve compliance and/or reduce risk.	• Investment in compliant information management hardware and software, data programming and cloud based or local information storage solutions.
Legal review of applicable regulation.	• Review local and international legal requirements and plan a compliance strategy with firm legal affairs, public relations, and IT departments and the use of external expertise. • Tighten in-house rules and monitoring of compliance. • Review agreements associated with data transfer. • Reform systems to obtain the consent of data providers and protect data (servers need to be locally installed or added if data transfer is not allowed).

Source: Consultation with firms

Opportunity costs

In addition to direct costs there are opportunity costs which firms experience as a result of data regulation and compliance requirements. For example, capital expenditure envelopes for business are finite and the mandatory component of data regulation necessarily diminishes the commercial component.

The benefits of regulation

All firms report that regulation protecting consumer data is of benefit because it assists them to preserve trust in their brands and commercial reputations. This is because they can rely on their regulatory compliance to assure their customers that their collection and use of customer data meets best practice.

Concerns with current regulatory approaches

Regulatory scope

The primary concerns of firms was the regulation of data collection, storage and use which promoted localisation as this created additional costs and impeded competition.

Two firms expressed particular concern about cyber security regulation in an APEC economy which requires them to share data with the government and store all information locally. These firms considered that this kind of regulation hindered their trade in the said market because it was inconsistent with their other regulatory obligations and own firm policies.

Regulatory alignment

All firms favoured greater regulatory consistency between economies and increased regulatory alignment within economies particularly when the management of data is subject to variations in domestic and industry specific rules. Firms that were subject to the GDPR were not troubled by it.

Firms were generally not aware of APEC's Privacy Framework, Cross Border Privacy Rules (CBPR) or the work APEC is doing to promote the interoperability between the CBPR and EU's GDPR.

Regulatory barriers

Firms did not express any concerns with regulatory barriers created by data regulation other than those already discussed in relation to direct and opportunity costs.

Preferred regulatory approaches

Firms considered that regulation was important to maintain brand trust and there was no strong view expressed for the need for self-regulation. Firms emphasised the need for regulatory consistency within APEC.

CHAPTER 9: MANUFACTURING

9.1. Sector overview

Manufacturing plays an important role to economic growth in the APEC region, particularly due to its important role in trade. Manufactured goods represent the largest share of APEC's intra-regional and inter-regional trade. Since 1996, intra-APEC trade in manufactured products has increased by about 6 percent per annum and represented about USD4.5 trillion in 2017.[133] Despite its position as one of the main drivers of economic growth in some economies, however, the manufacturing sector can hardly be perceived as stable. Firms have seen the need to continually reinvent themselves as they seek to maintain their competitive advantage and ensure the viability of their businesses. For example, the increase in labour cost in some economies, coupled with improvements in telecommunications and logistics services among others, have led to the internationalization of production such that a significant share of world trade takes place within the framework of global value chains (GVCs). Nowadays, a product is likely to be made up of parts and components sourced from across the world.

Increasingly, firms also have to adapt to producing more high mix, low volume parts, components and products, as opposed to those that are low mix and high volume. This is particularly so for some industries such as consumer electronics where the upgrade cycle is relatively shorter (i.e. about once or twice a year). For firms who face challenges in responding fast to the changing demand, they have preferred to focus on B2B instead of B2C businesses since the lead time is relatively longer.

The competition from different players have also meant that manufacturing firms often have to utilize and/or offer the whole spectrum of services from R&D and engineering to leasing and after-sales such as maintenance, repair and overhaul (MRO) services in order to stand out from the rest. Indeed, the boundaries have blurred that some manufacturing firms have been asked if they can still be categorized as such firms considering the range of services that they provide and the corresponding revenue that can be attributed to them. One way of looking at the critical role of services in manufacturing is through the OECD Trade in Value Added (TiVA) database. Based on the latest year where data is available (2011), it can be observed that services made up between 20.7 and 58.6 percent of the value-added share of gross exports of manufacturing in APEC economies covered by the database[134]. Advancements in and introduction of technologies such as cloud computing, Internet of Things (IoT) and artificial intelligence (AI) are likely to further increase the share of services value-added in manufacturing.

Different types of data are believed to contribute significantly to the daily operations of these manufacturing firms, including ensuring that services are utilized and offered optimally. These can range from ensuring the smooth functioning of the global value chains (GVCs) operations to increasing the demand for products among others. Specifically on the former, examples include making sure that parts and components are delivered on time and that downtime on factory floors are minimized, while on the latter, examples include employing data for targeted advertising and utilizing usage statistics for product improvements.

[133] Data for Papua New Guinea are not available and the latest data for Viet Nam and Thailand are from 2016. Data can be accessed from StatsAPEC Bilateral Linkages Database http://statistics.apec.org/index.php/bilateral_linkage/index.

[134] The total value-added share of services in gross exports is obtained by adding the domestic and foreign value-added of services in gross exports. Data for all APEC economies are available except for Papua New Guinea.

For instance, coordinating the activities of its suppliers without relevant information being exchanged between them would have been close to impossible for Apple[135]. The same can be said for Volkswagen, where its 55 strategic suppliers are based in different economies including Japan, Korea, Mexico and the United States[136]. In fact, there is very close collaboration between Volkswagen and its suppliers to synchronize and refine their strategic goals. In some cases, Volkswagen involved their suppliers early in the innovation process. To allow its supply chain to respond more flexibly to increasingly complex markets, one Japanese firm shared that it employs the supply chain management system developed by a data solutions company. Essentially, the system allows demand information, actual results, constraints and other data inputs to design a single production, marketing and inventory plan globally. Bain and Company shared that one firm streamed data from stores the moment shoppers purchased the products so that they can quickly restock popular items and minimize lost sales. Some leading firms such as Fast Radius[137] and Adidas[138] are already deploying 3D printing in locations that would enable them to reach customers within shorter lead time.

Manufacturers are indeed starting to realize the value of data, specifically big data[139] on their businesses. In a reference to a joint survey conducted by SCM World and MESA International, Forbes (2015) noted that 47 percent of manufacturers expect big data analytics to have a major impact on their performance. 49 percent also expect advanced analytics to reduce operational costs and utilize assets efficiently[140]. Additionally, the same survey noted that 49 percent of manufacturers are either piloting or planning to invest in big data analytics. On the most likely use cases of big data analytics in the factory, those identified by respondents include real-time factory performance analysis, real-time re-planning (material requirements planning and factory scheduling), real-time supply chain performance analysis, as well as production quality and yield management.

In terms of impacts, a publication by McKinsey Global Institute (2017) focusing on Artificial intelligence (AI), which is heavily reliant on data as inputs for decision-making, showed that using AI to improve R&D process has led to 10 percent yield improvement for integrated-circuit products[141]. Employment of AI to determine timing of goods transfer and to predict sources of servicing revenuers have also led to 30 percent increase in terms of timeliness of material delivery and 13 percent improvement in earnings before interest and tax, respectively.

---

[135] https://www.apple.com/supplier-responsibility/pdf/Apple-Supplier-List.pdf.
[136] https://www.autocarpro.in/news-international/vw-picks-55-strategic-supplier-partners-fast-initiative-20039
[137] https://www.ibm.com/blogs/think/2019/02/how-future-factories-will-change-manufacturing-and-supply-chains/
[138] https://www.bain.com/insights/build-a-digital-supply-chain-that-is-fit-for-the-future/
[139] There is currently no agreed definition of big data. However, one general understanding is that it is a collection of large datasets obtained through a wide range of online and offline sources. The data collected may be unstructured, structured and/or both and organizations are able to analyse them to predict patterns and trends among others depending on their ability.
[140] Columbus, L. 2015. Big Data Analytics, Mobile Technologies and Robotics Defining the Future of Digital Factories. Forbes. https://www.forbes.com/sites/louiscolumbus/2015/02/15/big-data-analytics-mobile-technologies-and-robotics-defining-the-future-of-digital-factories/#d458e367e9d8
[141] McKinsey Global Institute. 2017. Artificial Intelligence: The Next Digital Frontier? https://www.mckinsey.com/~/media/McKinsey/Industries/Advanced%20Electronics/Our%20Insights/How%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/MGI-Artificial-Intelligence-Discussion-paper.ashx

This chapter seeks to better understand how data are used in various aspects or process of the manufacturing sector. It has been structured as follows. Section 2 provides the profile of firms interviewed, section 3 provides the role of data in firms' business models, while section 4 discusses on how policies and regulations are impacting their business model.

9.2. **Profile of firms interviewed**

Firm A is a multinational manufacturing company based in Japan. For fiscal year 2017, its consolidated revenue reached USD10 billion. It has over 20 manufacturing and R&D subsidiaries and over 80 sales and services subsidiaries with 80,000 employees in six continents. Firm A provides a wide range of products from home and commercial printers, projectors, smart glasses and watches, to industrial robots and semiconductors.

Firm B is a Fortune 500, Japan-based company with over 250,000 employees and 600 subsidiary companies globally. Its net sales in fiscal year 2018 (which ends in March 2018) reached USD70 billion. Firm B produces a wide variety of products across multiple manufacturing industries, including consumer electronics such as televisions, home communication and entertainment products, kitchen appliances, air conditioners, beauty and living product; energy and electronic devices such as automotive batteries and semiconductors; avionics such as inflight connectivity and entertainment systems; mobile and camera products such as laptops, projects, displays and cameras and etc.

Firm C is a Japanese manufacturer producing products across a wide range of industries for public sectors, businesses, as well as general consumers. Examples of the products include firefighting command and emergency radio systems, traffic control systems, satellite communications, mobile phone base stations, biometric solutions such as facial recognition products, as well as computers, projectors and cameras. Its annual net sales averages USD20 billion and it hires over 100,000 employees globally.

Firm D is a Japanese automotive manufacturer which has established R&D, design and production sites in around 20 economies, and offers automotive products to above 160 markets worldwide. With more than 100,000 employees, it produced over 5 million vehicles globally and achieved over USD100 billion in net sales in fiscal year 2017.

Firm E is also a Fortune 500 Japanese manufacturing company. Its annual revenue is more than USD80 billion and it employs over 300,000 staff. Its businesses range from large social infrastructure products such as elevators, railways, power generation systems, to small electronic components such as semiconductor chips, magnetic materials, wires and cables, and consumer goods such as home appliance, refrigerators and air conditioners.

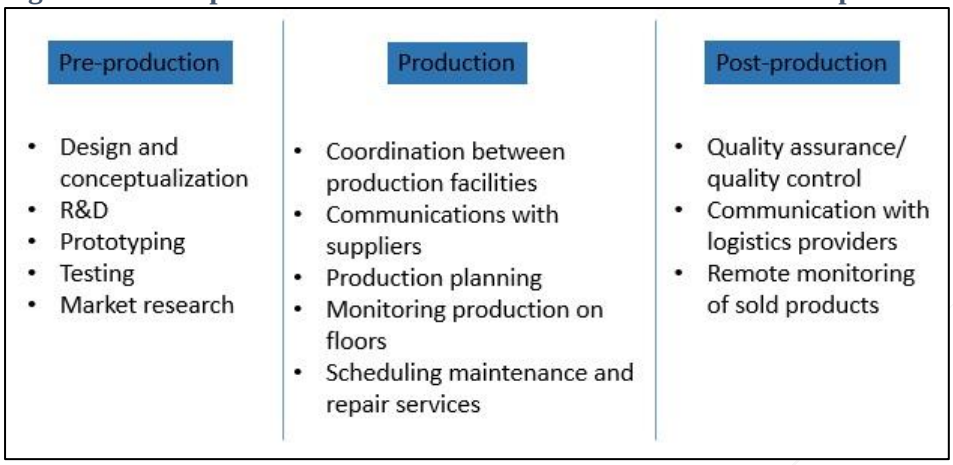
Firm F is a Japanese construction machinery manufacturer producing a wide range of machinery and transportation equipment such as excavators, wheel loaders, trucks, cranes, compaction and demolition equipment. It has manufacturing facilities in Europe, the U.S. and Asia. With more than 50 overseas subsidiaries, firm F hires over 20,000 employees globally and enjoys an annual revenue of over USD8 billion.

Firm G is a terminal solutions provider based in Japan. It produces bank branch terminals, ATMs, cash recycle machines, as well as various card reader products for financial, retail and security industries. With around 1,000 employees, its products are widely deployed in many economies such as India, Thailand, Indonesia, Chinese Taipei, and China.

9.3. Role of data in firms' business models

Depending on the products, value chains within the manufacturing sector can vary from one another in terms of structure and complexity. One way of categorizing the different parts of a value chain is to group them into pre-production, production and post-production (including post-sales) (Figure 13). Interviewed firms shared the critical role of data across various parts of the value chain.

Figure 13. A simplified illustration of a value chain and some examples of activities



Source: Authors

Pre-production

In the pre-production stage, firms indicated that they collect and use data to facilitate product design and conceptualization. Since firms have facilities in different economies, data collected in one economy often has to be shared with that in another economy. As several firms also involve some of their suppliers in the product design stage, data often has to be shared with these external partners as well and they may not always be located in the same economy where data was generated. It is worthwhile to point out that cross-border data transfer is usually not unidirectional. In fact, data have to be sent back and forth between the facilities involved throughout the entire process.

The same can be said for R&D activities which tend to be scattered across different economies for reasons including availability of talent and supporting ecosystem. Firm D shared that its R&D activities can generally be divided into two main groups: a) one works very closely with the design and conceptualization team to come up with new technology and parts; b) another undertakes activities to improve on existing technology and parts as well as ensuring that products function optimally in different regions (e.g. thermal insulation, tire tread depth, etc.). Both groups collect and have to share data across the borders since the different teams involved are usually located in different economies.

Production

In the production stage, firms use data collected from different manufacturing facilities to better exercise control and coordination activities. For example, several firms including Firms A, B and D shared that its HQ in Japan analysed the data provided by different facilities and used them to allocate production plan such as the models and corresponding quantity to produce over the next quarter or so. One of these firms indicated that it is in the midst of consolidating the production planning system across different facilities into a single platform. Once completed, it would allow the HQ to live monitor production in these facilities (which are located in different economies) and better coordinate activities across them.

On the production floor, data are used for a broad range of activities. For example, data are used by production planning software to identify machines which are available for the next production run. Data are also used to determine if a particular production run is operating efficiently and if not, where the bottlenecks are so that they can quickly be rectified. Pertaining to this, Firm E shared that while it has always relied heavily on the skills of its experienced master engineers (known as meisters) to keep production going, it has never really get around to complete understanding of what these meisters did correctly until very recently. With the advent of big data, firm is now able to measure things such as the cutting angle, speed and force that these meisters apply to the materials. This leads to better monitoring of such activities and the collected data can also be used to train new meisters. Furthermore, the same firm indicated that the ability to share live data from its regional facilities to its HQ in Japan has allowed it to reduce the need to dispatch engineers to these facilities where possible. The data centre of Firm C which is located in Japan remotely monitors data generated by its facility in India and provided technical assistance when necessary. Data are also used to monitor machines and therefore minimize unplanned downtime through predictive maintenance.

Particularly on communications with their suppliers, firms including Firms F and G noted the importance of being able to share data with them to ensure that parts and components are delivered on time. Firm C shared that since it obtained 70 percent of parts and components for its products from overseas suppliers such as Chinese Taipei and China, its procurement activities rely heavily on unimpeded cross-border data flow. The importance of communications with suppliers is even more pronounced for firms which have put in place just-in-time manufacturing system and only have a small warehouse to store parts and components for a short period of time (e.g. maximum of one day). Too early or too late a delivery would have negative implications on the firms' production plan.

Post-production

Once production has been completed, data from quality assurance/quality control activities are collected and analysed to ensure that products adhere to certain standards and are ready to be shipped out and/or delivered to the customers. Data would also need to be shared with logistics providers to schedule pick-up and delivery.

In the past, with the exception of the provision of warranty services, it can be argued that the responsibility of the manufacturers ends once the products have been sold and are in the hands of the customer. Increasingly, however, this is often not the case anymore. To ensure that they remain competitive relative to other players in the sector, firms have to provide more than just the products. Provision of maintenance and repair services is becoming the new normal and in some cases, could generate more revenue for the firms than the products themselves. Effective maintenance and repair services necessitates that products can be monitored and data can be shared remotely with the manufacturers so that predictive and preventive services can be provided before they break down.

Value-add can also be generated by collecting and analysing usage information to a greater extent. For example, knowing the features that are more commonly used by customers and their corresponding feedback can enable firms to enhance them and hopefully build loyalty. Linking the features used to customer profile can enable firms to promote the availability of these features to potential customers of the same profile and garner more purchases. Likewise, a better understanding of customer profile can allow firms to target new markets whose potential customers have similar profile.

Firm D shared that it is currently working with insurance companies to analyse usage data of its vehicles and in doing so, can enable them to set premiums which are more in line with the behaviour of individual drivers. This could act as a strong incentive for drivers to be more careful when on the road.

Ensuring data protection and security

Considering the importance of data in their business models, firms recognized that their policies pertaining to data should be clear, transparent and designed in such a way to ensure that data in its possessions are kept secure and private. One firm noted the current predicament faced by Facebook and would like to avoid the same situation. As a start, the same firm shared that it seeks customers' permission to collect any data from the electric vehicles purchased by them. If customers do not give the permission, no data are collected from the corresponding electric vehicles. Once data are in the possessions of the firms, strict rules have to be followed when using and analysing them. As an illustration, data are anonymized before they are transferred for further use and analysis by another team. Firm B also shared that access to data within the same firm are restricted based on sensitivity level. Furthermore, senders are recommended to encrypt sensitive data before they are sent to the recipients. The same firm indicated that it has a strong cyber protection team which would do its best to ensure that data are kept secure and private. Firm F indicated that they also ensure that their suppliers are also compliant with the information management regulations, privacy information management rules and agreement that it abides to, including the GDPR. It also has protocols in place to allow for steps to be taken promptly by the relevant units and departments in the event of a problem. Moreover, all employees are regularly provided training in these areas.

9.4. **How policies and regulations are impacting their business model**

Pre-production

Similar to the approach taken to describe the role of data in their business model, firms were also asked to indicate if data-related policies and regulations are impacting the various parts of their value chains and elaborate on them. On pre-production which includes R&D activities, firms shared that none of the data-related policies and regulations in the jurisdictions where they operate are affecting them negatively at the moment. They have been able to transfer and share data such as technical specifications across the borders within their companies and also with other stakeholders such as their suppliers. However, one firm noted that uncertainty with regards to implementation of an upcoming intellectual property (IP) law in one economy had led it to consider moving its R&D operations to another economy because it may not be able to transfer data as freely as the current situation. In addition to the cost of relocating its operations, firm may also lose access to the existing pool of talents.

Production

Firms also did not express any specific concerns about policies and regulations that are currently affecting the production stage of their value chains. For those that coordinate manufacturing activities across different facilities from several centralized locations, they have been able to receive data from these facilities and likewise, send data back to these facilities. Indeed, one firm shared that since its production planning software currently differs between regions, it is trying to synchronize the software and may be able to coordinate activities from a single centralized location in the near future. For those that need to send data to their suppliers to ensure that parts and components are manufactured and sent to their facilities in time for assembly, they have also been able to do so without any challenges. Similarly, firms have also not encountered any difficulties in sharing machine-generated data to schedule maintenance and repair services of its production machines.

Post-production

While firms do not encounter any issues sharing data on product quality across the borders, the insights provided by firms on post-sales activities appear to indicate that data-related policies and regulations have more implications here. As shared in the previous section, firms are increasingly tapping on customer data to improve their products and offerings. In some cases, firms are re-sending the data that they have analysed back to the consumer to recommend certain course of actions such as maintenance and repair among others. Since many of these data are personal data and/or can be associated with an individual, firms would technically face more barriers in sending such data across the borders. For example, if these data belong to citizens of the EU, firms would have to adhere to strict GDPR requirements before transferring data across the borders. The good news for the interviewed firms is that Japan has been conferred adequacy status pertaining to GDPR and therefore, data can generally flow freely between the borders. Nevertheless, one firm shared that it has had to hire extra lawyers to ensure compliance with GDPR requirements.

While firms have not encountered any specific issues in other economies and are still able to transfer data freely, they are concerned that they would be at some point. If this happens and Japan has no adequacy status with these economies, then they may face difficulty transferring data in the future. Firms opine that the implications of this are likely to be greater than the situation of not having adequacy status with the EU because these are relatively larger markets than the EU. Moreover, firms have the perceptions that data-related policies and regulations in some economies are unclear and discretionary in nature.

Preferred regulatory approaches

On the ideal situation, firms hope that there could be a single data-related policy that is applicable across the region so that they do not face challenges in finding and adhering to different regulations which may tend to be duplicative in nature. Recognizing that aligning different data-related policies and regulations between economies would be an onerous process, firms noted that the CBPR is a step in the right direction. It allows a firm fulfilling the data privacy regulations of one economy to be regarded as meeting those of other economies which are part of the mutual recognition system. Interestingly, despite knowing the existence of CBPR, none of the interviewed firms are currently part of the system. Reasons can include the limited number of economies currently participating in the CBPR and firms not encountering much issues transferring data between these economies.

REFERENCES

Adobe Inc. 2016. Global Guide to Electronic Signature Law: Country by country summaries of law and enforceability. San Jose. Accessed January 31, 2019. https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/document-cloud-global-guide-electronic-signature-law-ue.pdf

Air Transport Action Group. 2016. Around the world – APEC. https://aviationbenefits.org/around-the-world/apec/

APEC Policy Support Unit. 2015. Services in global value chains: Manufacturing-related services. http://publications.apec.org/Publications/2015/11/Services-in-Global-Value-Chains-Manufacturing-Related-Services

Atkinson, R.D. and Cory, N. 2017. ITIF Filing to the Central Bank of Brazil on Cybersecurity and Data Processing Requirements. https://itif.org/publications/2017/11/14/itif-filing-central-bank-brazil-cybersecurity-and-data-processing

Bank of International Settlements. 2018. Cross-border retail payments. Basel: Bank for International Settlements, February 2018, https://www.bis.org/cpmi/publ/d173.pdf.

Barreix, Alberto and Zambrano, Raul. 2018. Electronic Invoicing in Latin America. Washington, D.C: The Inter-American Development Bank. Accessed January 31, 2019, https://webimages.iadb.org/publications/english/document/Electronic-Invoicing-in-Latin-America.pdf.

Bauer, M., Lee-Makiyama, H., van der Marel, E, and Verschelde, B. The Costs of Data Localization: Friendly Fire on Economic Recovery. (Brussels: The European Center for International Political Economy, 2014), https://ecipe.org/wp-content/uploads/2014/12/OCC32014__1.pdf.

BCG. 2013. "Big Data's Five Routes to Value: Opportunity Unlocked". https://www.bcg.com/en-us/publications/2013/information-technology-strategy-digital-economy-opportunity-unlocked-big-data-five-routes-value.aspx

Beshouri, Christopher, and Gravrak, Jon. 2010. "Capturing the promise of mobile banking in emerging markets," McKinsey and Company website, February 2010, https://www.mckinsey.com/industries/telecommunications/our-insights/capturing-the-promise-of-mobile-banking-in-emerging-markets.

Bolt, W. and Chakravorti S. Digitization of Retail Payments. (Amsterdam, De Nederlandsche Bank, December, 2010), https://www.dnb.nl/binaries/Working%20paper%20270_tcm46-243674.pdf.

Capgemini. 2017. "Top 10 Trends in Payments in 2018." https://www.capgemini.com/wp-content/uploads/2017/12/payments-trends_2018.pdf.

Castro, D. and McQuinn, A. 2016. Unlocking Encryption: Information Security and the Rule of Law. http://www2.itif.org/2016-unlocking-encryption.pdf?_ga=1.192038954.1045463480.1471968194

Chakravorti, B., Bhalla, A., and Chaturvedi, R.S. Which Countries Are Leading the Data Economy? Harvard Business Review, January 24, 2019. https://hbr.org/2019/01/which-countries-are-leading-the-data-economy.

Chorzempa, M. "China Needs Better Credit Data to Help Consumers" (The Peterson Institute for International Economics, January, 2018), https://piie.com/system/files/documents/pb18-1.pdf.

Cockburn, I., Henderson, R., and Stern, S. The Impact of Artificial Intelligence on Innovation (Cambridge: The National Bureau of Economic Research, December 16, 2017), https://www.nber.org/chapters/c14006.pdf;

Cory, Nigel. 2019. The Ten Worst Digital Protectionism and Innovation Mercantilist Policies of 2018. Washington, D.C: The Information Technology and Innovation Foundation, January 28, 2019, https://itif.org/publications/2019/01/28/ten-worst-digital-protectionism-and-innovation-mercantilist-policies-2018.

Cory, N. and Atkinson, R.D. 2016. "Financial Data Does Not Need or Deserve Special Treatment in Trade Agreements."

Cullen International. 2016. Building a Digital Single Market Strategy for Latin America. http://scioteca.caf.com/bitstream/handle/123456789/980/DigitalMarketStrategy-7dic.pdf

Deloitte Access Economics. 2017., Platforms, small business and the agile economy. https://www.aph.gov.au/DocumentStore.ashx?id=b459be7e-2d6e-4e35-b7d0-82be74e88b11&subId=510227

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

EY. 2016. "Tax administration is going digital: understanding the challenges and opportunities." London. Accessed January 31, 2019, https://www.ey.com/Publication/vwLUAssets/EY-tax-administration-is-going-digital-understanding-the-challenges/%24FILE/EY-tax-administration-is-going-digital.pdf.

Fintech Rankings. 2018. "Why Ant Financial-backed Dana may struggle to catch up with other Indonesian payments apps," Fintech Rankings, July 2, 2018, http://fintechranking.com/2018/07/02/why-ant-financial-backed-dana-may-struggle-to-catch-up-with-other-indonesian-payments-apps/.

Fefer, R.F., Akhtar, S.I., Morrison, W.M. 2018. Digital Trade and U.S. Trade Policyhttps://fas.org/sgp/crs/misc/R44565.pdf

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

Gefferie, Dwayne, "The Top 3 Trends that will impact the Payments Industry in 2018," The Startup page on Medium.com, January 2, 2018, https://medium.com/swlh/the-top-3-trends-that-will-impact-the-payments-industry-in-2018-3bed3588f98f.

Global Payments Innovation Jury. 2017. An Insider's View to Payments and Fintech. London: Global Payments Innovation Jury, 2017, https://www.aciworldwide.com/-/media/files/collateral/trends/payments-innovation-jury-report.pdf.

Grosso, M.G. 2010. Air passenger transport in APEC: regulation and impact on passenger traffic. OECD: Paris. http://www.oecd.org/tad/services-trade/46329349.pdf

HSBC. Payments in ASEAN post AEC. Available at: https://www.hsbc.com.my/1/PA_ES_Content_Mgmt/content/website/commercial/cash_management/PDF_141107/5-Payments-in-ASEAN-post-AEC.pdf

International Trade Centre (ITC). 2016. Bringing SMEs onto the E-commerce Highway.

International Trade Centre (ITC). 2017. New Pathways to E-commerce: A Global MSME Competitiveness Survey.

ITI. 2017. Comments in Response to Executive Order Regarding Trade Agreements Violations and Abuses. https://www.itic.org/dotAsset/9d22f0e2-90cb-467d-81c8-ecc87e8dbd2b.pdf

ITIF. 2018. "What Is Artificial Intelligence?" ITIF Technology Explainer Series. http://www2.itif.org/2018-tech-explainer-ai.pdf?_ga=2.156402939.190190766.1544733053-713678332.1542814788

ITIF. 2018. "ITIF Technology Explainer: What Is Blockchain?" Washington, D.C. https://itif.org/publications/2018/10/03/itif-technology-explainer-what-blockchain.

Jaikaran, C. 2016. Encryption: Frequently Asked Questions. https://fas.org/sgp/crs/misc/R44642.pdf
Marchetti, Juan. 2018. Addressing E-Payment Challenges in Global E-Commerce. Geneva: World Economic Forum, May 2018, http://www3.weforum.org/docs/WEF_Addressing_E-Payment_Challenges_in_Global_E-Commerce_clean.pdf.

Lemley, Mark A. 2008. The Surprising Virtues of Treating Trade Secrets as IP Rights, 61 STAN. L. REV. 311, 332.

McKinsey & Company. 2017. "Time for insurance companies to face digital reality" https://www.mckinsey.com/industries/financial-services/our-insights/time-for-insurance-companies-to-face-digital-reality

McKinsey Global Institute 2016. How Digital Finance Could Boost Growth in Emerging Economies. https://www.mckinsey.com/global-themes/employment-and-growth/how-digital-finance-couldboost-growth-in-emerging-economies, 9.

McKinsey Global Institute. 2017. "What's now and next in analytics, AI, and automation" https://www.mckinsey.com/featured-insights/digital-disruption/whats-now-and-next-in-analytics-ai-and-automation

McQuinn, Alan. "Understanding Data Privacy," Realclearpolicy, October 25, 2018, https://www.realclearpolicy.com/articles/2018/10/25/understanding_data_privacy_110877.html.

McQuinn, Alan, Guo, Weining, and Castro, Daniel. 2016. Policy Principles for Fintech. Washington, D.C.: The Information Technology and Innovation Foundation, October 18, 2016, https://itif.org/publications/2016/10/18/policy-principles-fintech.

New, Joshua. Why the United States Needs a National Artificial Intelligence Strategy and What It Should Look Like (Washington, D.C: The Center for Data Innovation, December 4, 2018), http://www2.datainnovation.org/2018-national-ai-strategy.pdf.

Nixon, Patrick. 2017. "Latin America becoming world leader in e-invoicing," BNAmericas. https://www.bnamericas.com/en/news/ict/latin-america-becoming-world-leader-in-e-invoicing/.

Null TX. 2018. "Blockchain Invoice Financing Platform Hive Project Inks Deal with Social Business Gosocket to Secure Presence in Latin America." https://nulltx.com/blockchain-invoice-financing-platform-hive-project-inks-deal-with-social-business-gosocket-to-secure-presence-in-latin-america/.

OECD. 1997. OECD Guidelines for Cryptography Policy. http://www.oecd.org/sti/ieconomy/guidelinesforcryptographypolicy.htm

OECD. 2010. Measuring Innovation: A New Perspective, 84-85.

OECD. 2017. Key issues for digital transformation in the G20 - Report prepared for a joint G20 German Presidency/ OECD conference. https://www.oecd.org/g20/key-issues-for-digital-transformation-in-the-g20.pdf

OECD. 2017. Technology Tools to Tackle Tax Evasion and Tax Fraud. Accessed January 31, 2019, https://www.oecd.org/tax/crime/technology-tools-to-tackle-tax-evasion-and-tax-fraud.pdf.

OECD. 2018. Economic Outlook for Southeast Asia, China and India 2018: Fostering growth through digitalization. https://www.oecd-ilibrary.org/development/economic-outlook-for-southeast-asia-china-and-india-2018/overview_saeo-2018-5-en

OECD and WTO. 2017. Aid for Trade at a Glance 2017: Promoting Trade, Inclusiveness and Connectivity for Sustainable Development. Paris/Geneva. https://doi.org/10.1787/aid_glance-2017-en.

Papp, Noemie. 2019. "Discussion Paper on innovative uses of consumer data by financial institutions," European Banking Authority website, accessed January 31, 2019.

Ponemon Institute. 2018. The 2018 Global Cloud Data Security Study. http://www2.gemalto.com/cloud-security-research/

PricewaterhouseCoopers. 2012. APEC's evolving supply chain. https://www.pwc.com.au/about-us/apec-ceo-summit/assets/apec-supply-chain-sep12.pdf

Schneier, B., Seidel, K., and Vijayakumar, S. 2016. A Worldwide Survey of Encryption Products https://www.schneier.com/academic/paperfiles/worldwide-survey-of-encryption-products.pdf

Reavie, Vance. "Do You Know The Difference Between Data Analytics And AI Machine Learning?" Reuters, August 1, 2018, https://www.forbes.com/sites/forbesagencycouncil/2018/08/01/do-you-know-the-difference-between-data-analytics-and-ai-machine-learning/#323414be5878.

Reimsbach-Kounatze, C. and Van Alsenoy, B. "Exploring Data-Driven Innovation as a New Source of Growth" (Paris: Organization for Economic Co-operation and Development, June 2013), http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP(2012)9/FINAL&docLanguage=En.

Roy, Martin. "The Contribution of Services Trade Policies to Connectivity in the Context of Aid for Trade", (Geneva: World Trade Organization, Staff Working Paper No. ERSD-2017-12, 2017), http://dx.doi.org/10.2139/ssrn.3036946.

Statista. 2017. Number of digital buyers worldwide from 2014 to 2021 (in billions). https://www.statista.com/statistics/251666/number-of-digital-buyers-worldwide/

Suominen, Kati. Ecommerce Development Survey and Index. USAID, April 2017.

The MasterCard Foundation and IFC. 2017. Data Analytics and Digital Financial Services Handbook. https://www.ifc.org/wps/wcm/connect/22ca3a7a-4ee6-444a-858e-374d88354d97/IFC+Data+Analytics+and+Digital+Financial+Services+Handbook.pdf?MOD=AJPERES

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

UNCTAD. 2015. "Cyberlaws and regulations for enhancing e-commerce: Case studies and lessons learned." Geneva: UNCTAD secretariat. https://unctad.org/meetings/en/SessionalDocuments/ciiem5d2_en.pdf.

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

Visa. 2019. Global Commerce Unbound. Foster City: Visa, accessed January 31, 2019, https://usa.visa.com/dam/VCOM/global/visa-everywhere/documents/innovations-cashless-report-digital.pdf.

Whitler, Kimberly "How Tencent Is Using Closed-Loop Data To Drive Better Insight And Engagement," Forbes, January 9, 2018, https://www.forbes.com/sites/kimberlywhitler/2018/01/09/how-tencent-is-using-closed-loop-data-to-drive-better-insight-and-engagement/#7dc55bc61f0d.

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

World Economic Forum. 2018. Addressing E-Payment Challenges in Global E-Commerce. http://www3.weforum.org/docs/WEF_Addressing_E-Payment_Challenges_in_Global_E-Commerce_clean.pdf

WTO. 2015. International trade statistics highlights 2015. Geneva: World Trade Organization, 2015, https://www.wto.org/english/res_e/statis_e/its2015_e/its15_highlights_e.pdf.

WTO. 2018. World Trade Report 2018: The future of world trade: How digital technologies are transforming global commerce. Geneva. https://www.wto.org/english/res_e/publications_e/world_trade_report18_e.pdf