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.

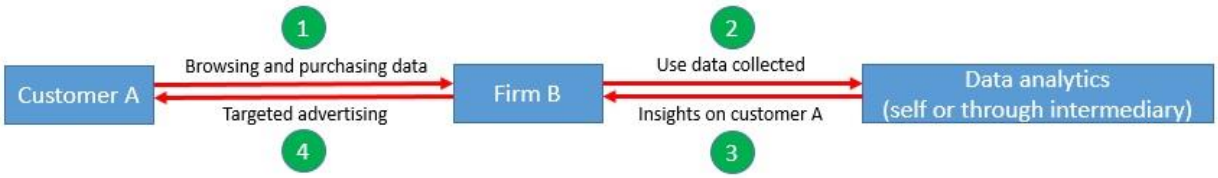
[9] Based on information from ITU, the fixed-broadband sub-basket is based on a monthly data usage of (a minimum of) 1 GB for comparability reasons. For plans that limit the monthly amount of data transferred by including data volume caps below 1 GB, the cost for the additional bytes is added to the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

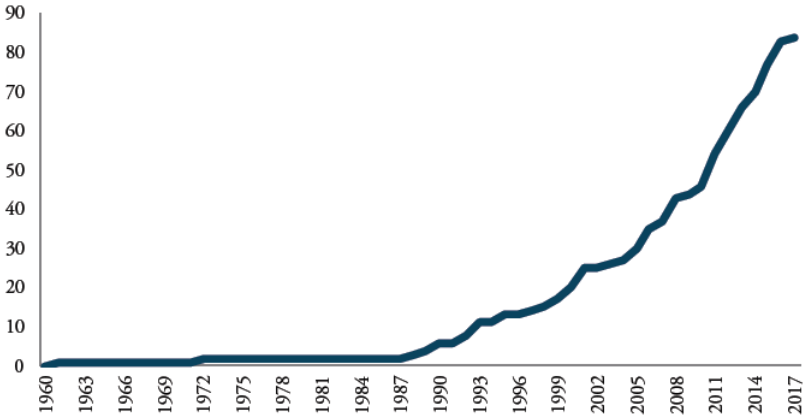
[22] BBC. 2018. "New Facebook bug exposed millions of photos." December 14. https://www.bbc.com/news/technology-46567131

[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)

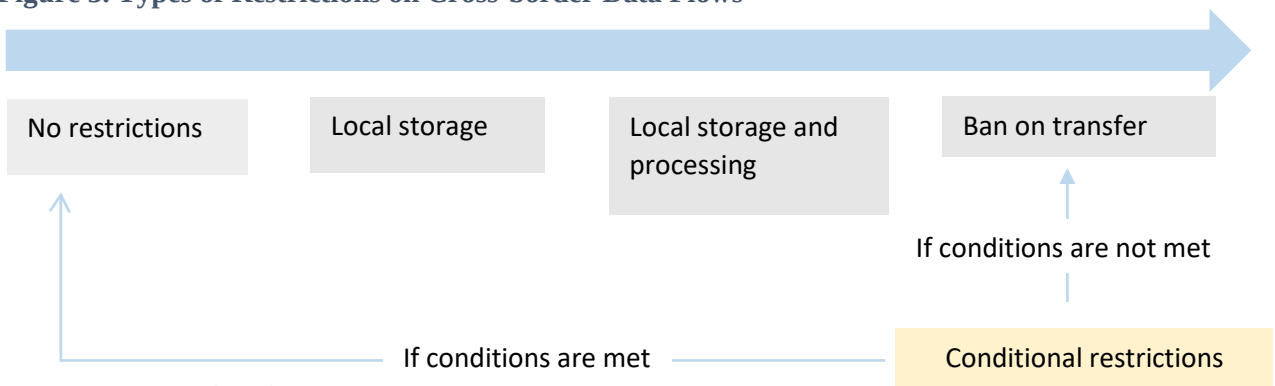


Source: Ferracane (2017)

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.

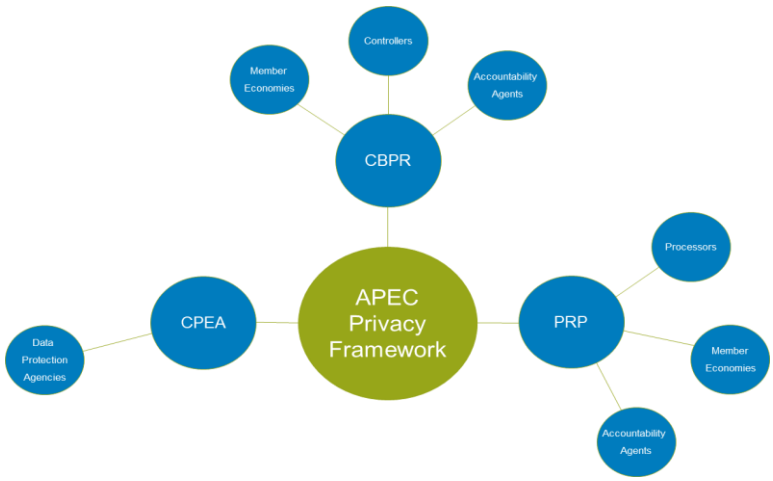
[39] 'Case C-498/16, Maximilian Schrems v Facebook Ireland Limited, (ongoing)'.
[40] See Chapter 2

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.

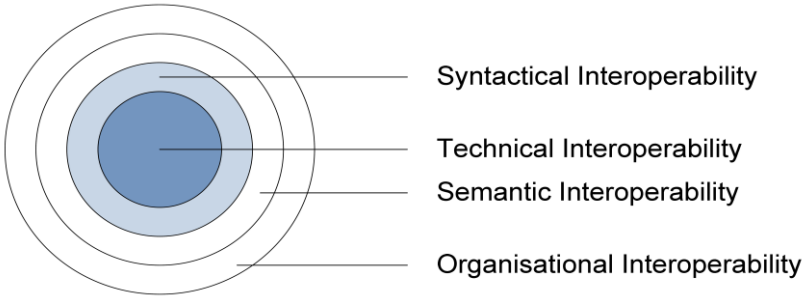
Anticompetitive behavior

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/