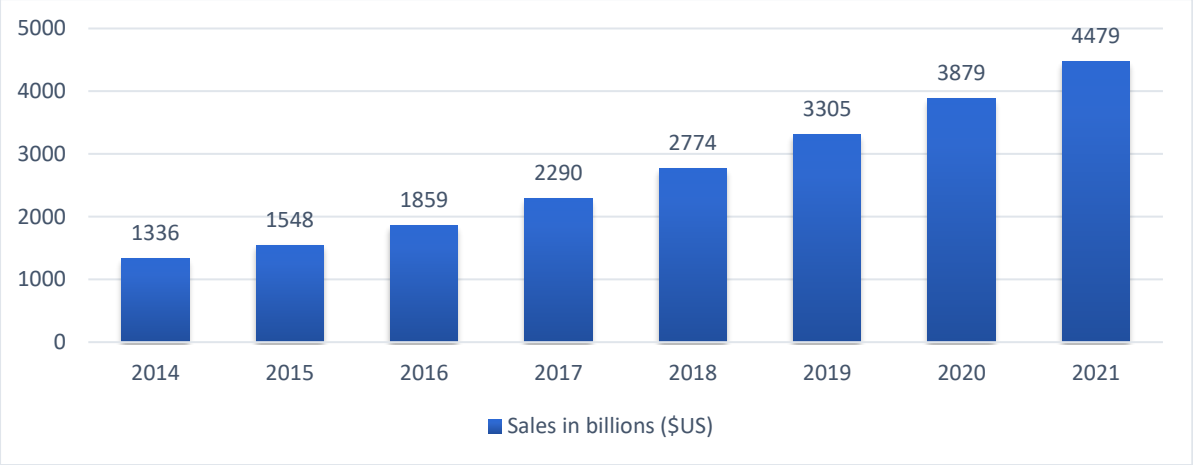
CHAPTER 3: DIGITAL SERVICES AND E-COMMERCE[55]

3.1. Sector overview

General economic contribution

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

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



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

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

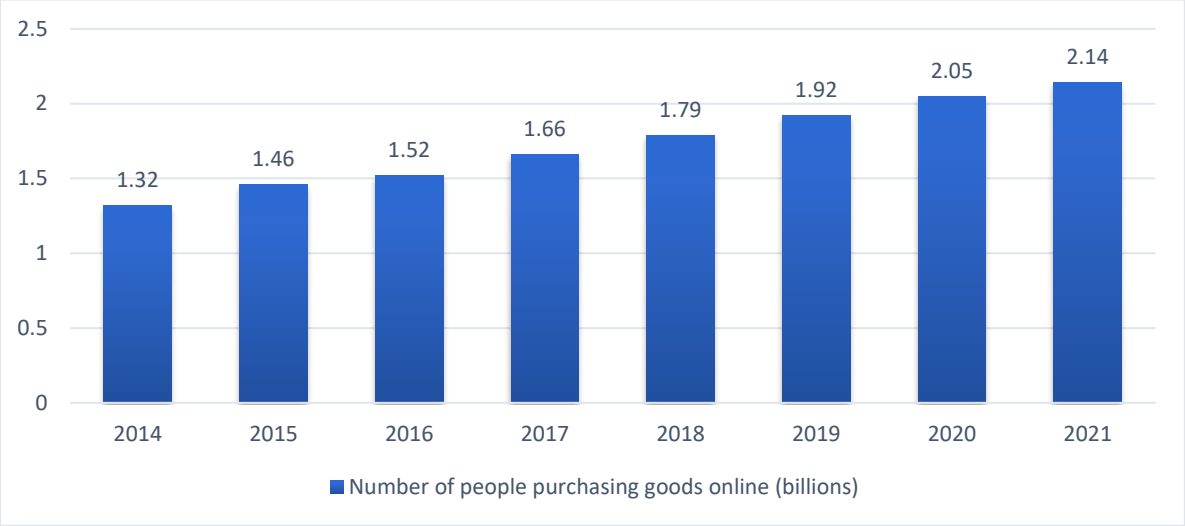
[55] This chapter discusses the collective views of fourteen firms consulted in the digital and internet services as well as e-commerce sectors. These are firms that themselves provide digital services and/or digital security services for other businesses and the wider public. The grouping of these industries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

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

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

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

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



Use of digital services in the APEC region

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

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

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

Productivity benefits of the digital economy

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

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

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

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

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

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

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

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

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

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

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

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

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

Variations in e-commerce retailing for regulation to consider

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

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

The variations in online retailing include:

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

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

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

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

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

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

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

APEC economies' approach to market regulation

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

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

3.2. Profile of firms interviewed

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

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

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

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

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

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

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

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

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

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

3.3. Role of data in firms' business models

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

Collection and use of consumer and business data

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

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

Collection and use of their own business data

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

Nature of data being managed

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

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

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

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

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

Source: Consultation with firms

How data flow enables the business

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

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

Table 11. Kinds of business practices relying on data flows

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

Source: Consultation with firms

Data storage options

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

Use of artificial intelligence (AI) and blockchain

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

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

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

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

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

Data security and privacy governance

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

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

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

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

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

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

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

Brand trust from good data management

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

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

3.4. How policies and regulations are impacting their business models

Applicable data regulation and compliance costs

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

Direct costs

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

Table 12. Kinds of compliance costs reported by firms

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

Source: Consultation with firms

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

Opportunity costs

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

Table 13. Opportunity costs reported by firms.

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

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

Source: Consultation with firms

The benefits of regulation

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

Concerns with current regulatory approaches

Regulatory scope

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

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

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

Regulatory alignment

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

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

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

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

Regulatory barriers

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

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

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

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

Preferred regulatory approaches

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

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

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

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

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