CHAPTER 2: TRANSPORT AND LOGISTICS[46]

2.1. Sector overview

Aviation

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

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

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

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

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

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

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

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

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

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

[48] APEC, Bogor declaration 1994

[49] APEC, Tourism Working Group

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

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

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

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

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

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

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

Logistics and transport (railways and shipping)

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

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

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

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

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

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

2.2. Profile of firms interviewed

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

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

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

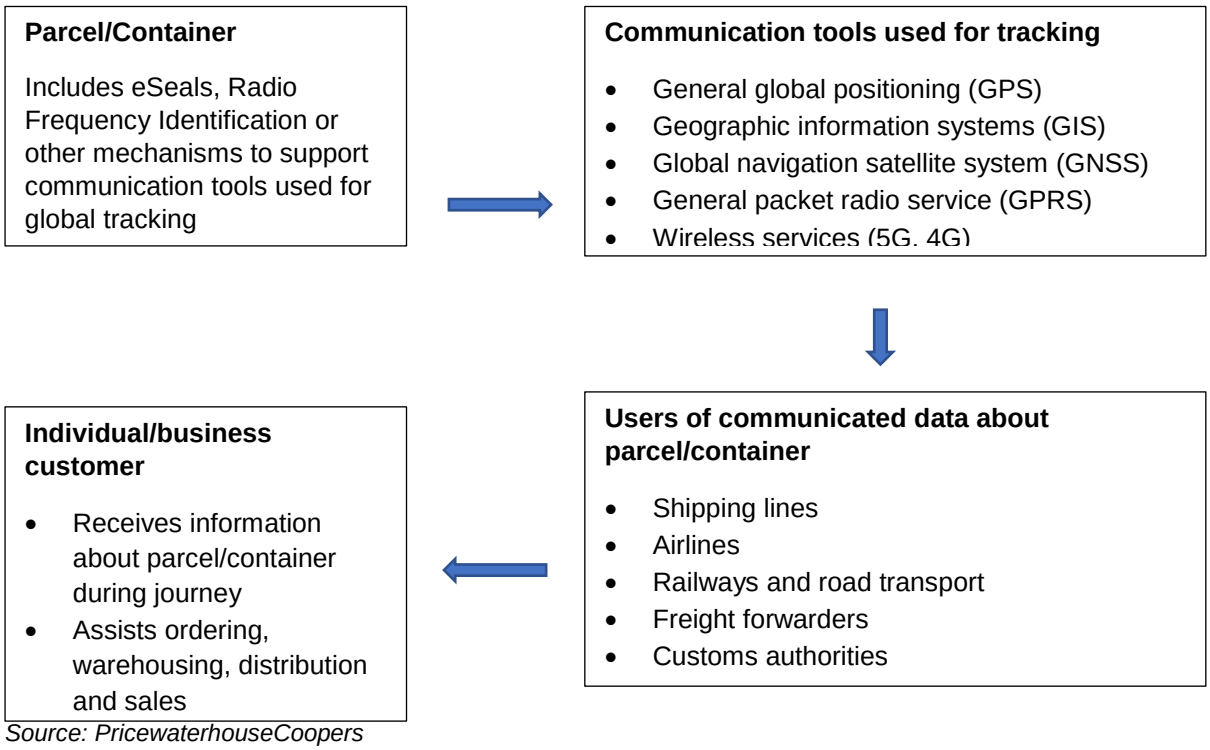
Of the logistics firms, four (Firms C, D E, F) are private firms and one (Firm G) is government owned. Key facts are:

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

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

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

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



Source: PricewaterhouseCoopers

2.3. Role of data in firms' business models

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

Collection and use of customer data

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

Collection and use of their own business data

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

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

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

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

Nature of data being managed

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

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

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

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

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

Source: Consultation with firms

How data flow enables the business

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

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

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

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

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

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

Table 5. Kinds of business practices relying on data flows

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

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

Source: Consultation with firms

Data storage options

The firms store data in various ways including the following.

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

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

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

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

Use of artificial intelligence (AI) and blockchain

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

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

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

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

Data security and privacy governance

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

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

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

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

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

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

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

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

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

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

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

Source: Consultation with firms

Brand trust from good data management

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

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

2.4. How policies and regulations are impacting their business models

Applicable data regulation and compliance costs

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

Direct costs

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

Table 7. Kinds of compliance costs reported by firms

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

Source: Consultation with firms

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

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

Opportunity costs

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

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

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

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

Table 8. Opportunity costs reported by firms

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

Source: Consultation with firms

The benefits of regulation

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

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

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

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

Concerns with current regulatory approaches

Regulatory scope

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

Regulatory alignment

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

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

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

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

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

Regulatory barriers

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

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

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

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

Preferred regulatory approaches

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

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

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