

CHAPTER 8: CONSUMER SERVICES¹²⁷

8.1. Sector overview

Services dominate the general economic output of APEC economies representing about 70 percent of total APEC output. The different levels of economic development within APEC means that the share of services in economic output varies across economies¹²⁸. However, the share of services in APEC trade is small compared to manufacturing. In 2016 services represented about 17 percent of total APEC exports below the world average of 19.8 percent¹²⁹.

Energy

Energy services are often locally produced and consumed with minimal trade in the generation, distribution and retailing of energy between economies. This is because of the often natural geographic barriers to supplying energy from one economy to another. Nevertheless energy services that are tradeable between economies include those of a digital nature such as the provision or smart metering services in homes and businesses which enable consumers to control their energy use; platforms which facilitate trade in energy based securities such as hedge pricing; and software and systems providing transparent information on comparative retail pricing which consumers can rely on to choose energy suppliers in their local markets¹³⁰.

Healthcare

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

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

¹²⁷ This chapter discusses the collective views of four firms consulted in the consumer services sectors (energy, healthcare and education publishing). This grouping has been selected because: 1) There were not a sufficient number of firms in each sector to justify separate chapters on each; 2) The firms did not express different views to those reported in the other chapters in this report.

¹²⁸ APEC Committee on Trade and Investment, Report to Ministers: Collective Strategic Study on Issues Related to the Realization of the FTAAP 2016, p75

¹²⁹ Ibid

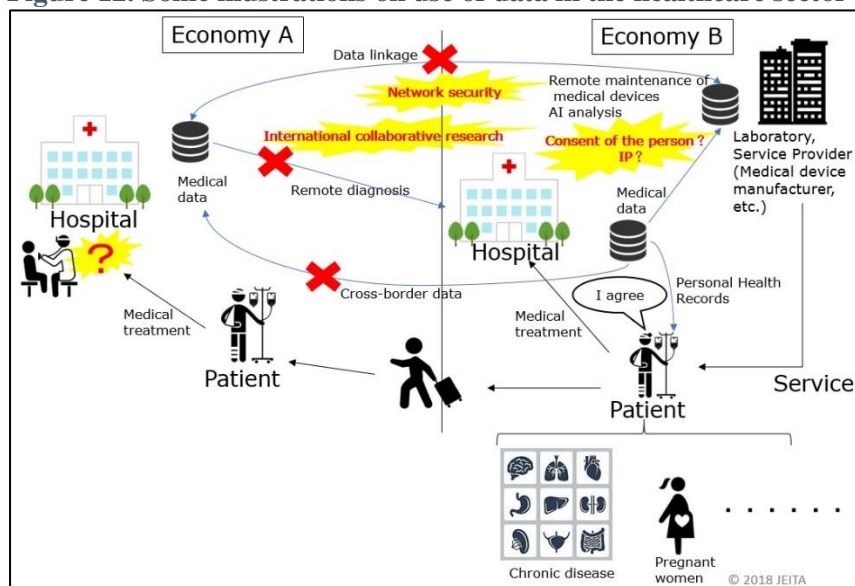
¹³⁰ Aegis Consulting Group

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

- Hospitals rely on effective data sharing within clinical settings to ensure the accurate and efficient management of patients. For example, patients admitted to the emergency department of a hospital with life threatening injuries or conditions may need to be managed through surgery, an intensive care unit, a recovery ward and when the patient returns home. Simple solutions can often improve data management and deliver benefits. For example, studies have estimated that the use of laptops at patient bedsides by medical staff to record and monitor patient information can deliver a 30 per cent improvement in clinical productivity including reduced staff time and increased accuracy in treatment¹³¹.
- Pharmaceutical companies collect patient data through clinical trials and via the clinical research conducted by medical practitioners prescribing their drugs. This data is critical to the research and development of new and improved pharmaceuticals. The costs of pharmaceuticals to individual patients in private medical systems and the taxpayer in government subsidised systems can increase when patients are prescribed drugs to which they have adverse reactions such as heightened side effects. Costs rise because patients may have to be prescribed numerous versions of medication before they find one that suits them. To avoid these risks, pharmaceutical companies are investing in DNA testing systems to assist medical practitioners target suitable medications to patients. This will require the sharing of highly sensitive and unique patient data and regulators will need to develop sophisticated regimes to govern this.
- Governments and private health insurers need to access and analyse high level data from clinical contexts to monitor and develop appropriate policy and insurance solutions to existing and emerging healthcare and health system priorities. The efficiency of healthcare funding in private insurance or government subsidised systems relies on insurers and governments understanding the capacity and limitations of funding to influence patient behaviour, prevent illness, manage chronic disease, and deliver improved clinical outcomes in hospital and non-hospital settings.

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

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



Source: JEITA

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

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

Education publishing

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

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

8.2. Profile of firms interviewed

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

Firms A and B provide energy-related services:

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

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

Firms C and D provide other consumer-related services:

- Firm C provides healthcare consulting such as policy planning to support the establishment of medical institutions.
- Firm D is a publisher of education material which provides digital content worldwide.

8.3. Role of data in firms' business models

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

Collection and use of customer data

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

Collection and use of their own business data

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

Nature of data being managed

All firms manage significant volumes of data. This includes:

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

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

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

Kinds of digitalisation	Examples
Principally online ordered and online supplied products/service	<ul style="list-style-type: none"> Provision of e-books.
Principally online ordered products or services that are then supplied offline (i.e. physical products or services provided offline)	<ul style="list-style-type: none"> Supply of energy smart meters where consumers order meters online but meters are physically installed.
Principally offline products or services	<ul style="list-style-type: none"> Provision of healthcare consulting services.
Online network, platform or matching service (i.e. enabling other entities that supply relevant products or services)	<ul style="list-style-type: none"> Provision of energy pricing and product information to consumer markets to support sales by retail energy firms. Remote monitoring of energy smart meters and provision of data to energy firms for customer billing and network control purposes.

Source: Consultation with firms

How data flow enables the business

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

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

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

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

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

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

Table 16. Kinds of business practices relying on data flows

Kinds of business activities enabled by data flows	Examples
Sourcing and procurement of inputs and suppliers.	<ul style="list-style-type: none"> Provision of client business data to inform healthcare consulting services. Provision of client business data to inform energy consumer market.
E-commerce or other sales and supply to customers directly or via third party platforms.	<ul style="list-style-type: none"> Sales or published material including e-books for education purposes.
Invoicing and payments.	<ul style="list-style-type: none"> Customer and supplier payments.

Kinds of business activities enabled by data flows	Examples
Customer relationship management (CRM).	<ul style="list-style-type: none"> • Corporate account management. • Consumer market management.
Enterprise resource planning (ERP).	<ul style="list-style-type: none"> • Supply of energy smart meters in line with planned roll out to customers by energy retailers.
Monitoring usage of services/products such as consumption of utilities and infrastructure.	<ul style="list-style-type: none"> • Remote monitoring of consumer energy use to inform energy retailers and distributors for customer billing and network management purposes.

Source: Consultation with firms

Data storage options

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

Use of artificial intelligence (AI) and blockchain

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

Data security and privacy governance

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

- Ensuring their policies, procedures and practices are consistent with international quality assurance instruments governing data security and privacy. This is primarily achieved by firms ensuring they are compliant with ISO27001 and BS10012.
- The systematic and regular review of local laws and regulations governing data security and management to ensure compliance. These local laws can include the personal data protection and privacy legislation in Australia, Japan and the Philippines. In the energy sector it can also include industry specific regulations including domestic energy network rules in Australia.
- Applying a sophisticated and comprehensive data governance framework which consists of firstly classifying all data according to its sensitivity and secondly restricting access within the firm to data according to levels of sensitivity.
- Regulatory compliance and cyber security awareness and best practice training for all staff involved in handling business and customer data depending on the level of data staff members are authorised to manage. Various staff within each organisation are responsible for handling and managing data including its reporting, security and privacy.
- Managing data flows within secure, transparent and auditable frameworks. This includes assessing the most secure and trusted hardware and location when choosing storage infrastructure; employing

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

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

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

Brand trust from good data management

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

8.4. How policies and regulations are impacting their business models

Applicable data regulation and compliance costs

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

Direct costs

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

- Development and operating costs associated with the need for separate data management systems in economies. This can lead to some information functions being disabled and services being unequally provided depending on the requirements in economies.
- Administrative costs of providing compliance documentation which can be a burden for MSMEs.
- Energy services need to comply with various regulatory measures such as customer frameworks, market conduct rules, and network regulation. The provision of smart meters must also comply with regulation in other markets which regulate hardware and software used by meters. For example energy smart meters contain 3G microchips and therefore must also comply with telecommunications regulations.

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

Table 17. Kinds of compliance costs reported by firms

Kinds of compliance costs	Examples
Recruiting specialised staff to improve compliance and/or reduce risk.	<ul style="list-style-type: none"> • Employment and/or contracting cyber security to oversee the design and management of hardware and processes to gather and store information.

Kinds of compliance costs	Examples
Investing in new infrastructure and information technology architecture to improve compliance and/or reduce risk.	<ul style="list-style-type: none"> • Investment in compliant information management hardware and software, data programming and cloud based or local information storage solutions.
Legal review of applicable regulation.	<ul style="list-style-type: none"> • Review local and international legal requirements and plan a compliance strategy with firm legal affairs, public relations, and IT departments and the use of external expertise. • Tighten in-house rules and monitoring of compliance. • Review agreements associated with data transfer. • Reform systems to obtain the consent of data providers and protect data (servers need to be locally installed or added if data transfer is not allowed).

Source: Consultation with firms

Opportunity costs

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

The benefits of regulation

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

Concerns with current regulatory approaches

Regulatory scope

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

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

Regulatory alignment

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

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

Regulatory barriers

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

Preferred regulatory approaches

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