OCCASIONAL PAPERS

Competition Commission SINGAPORE

Data: Engine for Growth –

Implications for Competition Law, Personal Data Protection, and Intellectual Property Rights

In collaboration with:

Intellectual Property Office of Singapore
Personal Data Protection Commission, Singapore

16 August 2017

Director, Policy & Markets Division
The Competition Commission of Singapore
45 Maxwell Road
#09-01 The URA Centre
Singapore 069118
Email: ccs_feedback@ccs.gov.sg

This paper is downloadable for free at
https://www.ccs.gov.sg/media-and-publications/publications/occasional-papers

Contents

Data: Engine for Growth - *Implications for Competition Law, Personal Data Protection, and Intellectual Property Rights*

CCS: Chun Han WONG, Hui Chuan YEO, Rachel LEE, Rui Ping LEOW, Wei Lu LIM
IPOS: Adrian CHIEW, Gavin FOO, Trina HA
PDPC: Annabel LEE

I. EXECUTIVE SUMMARY

Data[1] is increasingly being recognised as an asset to businesses and an engine for economic growth with great potential to drive innovation and contribute to the transformation of industries in Singapore. With advancement in technology, the ease and speed of data collection has led to the emergence of "Big Data" which is characterised by the 4Vs – volume, variety, velocity and value.[2]

The accumulation, sharing and analysis of data can bring about a wide range of benefits. For businesses, the benefits include streamlining business operations, higher revenue from improved product offerings, and increased innovation through creation of new products. For consumers, the benefits include a reduction in information asymmetry and search costs, and improved customer experience with new and customised product offerings. Beyond that, there are social benefits from better-informed public policy-making supported by data analytics. In recognition of these benefits, the Government has identified the adoption of data analytics[3] and data sharing[4] as part of the strategy for Singapore's next stage of growth and development.

[1] Data is defined in this paper as any factual information which can be used for reasoning, discussion and/or calculation.
[2] Key features defining Big Data include: (i) volume, which refers to the quantity of data generated or collected. It determines the potential value and insight which may be derived from data because limited analysis can be conducted if there exist only a few data points; (ii) variety, which refers to the different types and sources. Firms which merge a variety of data may be able to gain insight previously not possible with traditional data sources; (iii) velocity, which refers to the speed at which data is generated and processed to meet the demands and challenges for growth and development. High-speed processing allows for swift and accurate actions and decisions to be taken; and (iv) value, which refers to the value of insights to be gained from data sets.
[3] Data analytics is the process of examining data sets to draw conclusions about the information contained in the data sets. With advancement in computing power, data analytics now include predictive analytics, machine learning and data mining.
[4] Data sharing refers to the act of making data available to other stakeholders, both internal and external.

In particular, the Committee on Future Economy has highlighted data as a recurring theme in its report.[5]

Aligned with the Whole-of-Government efforts to promote the adoption of data analytics and data sharing, the Competition Commission of Singapore ("CCS") undertook research to understand the data landscape in Singapore. In collaboration with the Personal Data Protection Commission, Singapore ("PDPC"), and the Intellectual Property Office of Singapore ("IPOS"), CCS also sought to explore the implications of the proliferation of data analytics and data sharing on competition policy and law, personal data protection regulation and intellectual property law in Singapore. The research conducted also sought to study the interface between competition law and each of these two other areas of law.

The research for this paper was conducted from January to July 2017. As part of its research, CCS commissioned KPMG Services Pte. Ltd. ("KPMG") to conduct a study to map out the data landscape in Singapore. Six sectors with varying levels of maturity in the adoption of data-related practices – **digital media,**[6] **finance,**[7] **healthcare,**[8] **consumer retail,**[9] **land transport,**[10] and **logistics**[11]**,** were selected based on their potential to reap significant benefits from the adoption of data analytics.[12]

Data landscape in Singapore

The KPMG study found that the main players in the data landscape in Singapore are government agencies, businesses, customers, data analytics solutions providers, data storage providers and data aggregators:

a. **Government agencies** have been actively rolling out initiatives to encourage the adoption of data analytics. As government agencies are in a

[5] Strategies set out in the Committee on Future Economy report include building capabilities in data analytics and cybersecurity, harnessing data as an asset, and building strong digital capabilities in the economy by helping Small and Medium Enterprises adopt digital technologies.

[6] The digital media sector refers to advertising platforms and other advertising technology companies.

[7] The finance sector refers to the banking sector and the insurance sector.

[8] The healthcare sector here refers to public and private healthcare providers and research institutions.

[9] The consumer retail sector refers to online retailers and brick-and-mortar retailers, with some businesses present in both segments.

[10] The land transport sector includes a variety of services ranging from ride booking companies (for example, Grab and Uber), to public transport operators and private bus hiring companies.

[11] The logistics sector includes both the logistics service providers, which operate the delivery networks and collect data on customers' transactions, and the e-commerce retailers, which generate delivery demand through end-customers' purchases.

[12] KPMG conducted interviews with twenty-seven stakeholders from these six sectors, to obtain feedback on data collection, the use of data analytics, data sharing, and data monetisation, including their views on the benefits of, as well as impediments to, greater adoption of data analytics and data sharing.

position to collect a large amount of data, they are able to shape the data landscape within their respective sectors through the sharing of data with the public. Increasingly, government agencies are adopting data analytics to improve policy decisions.

b. **Businesses** collect, generate and use data to varying degrees. Businesses are the main adopters of data analytics, with **customers** contributing to the data generation process (whether voluntarily or involuntarily) and benefitting from more targeted marketing or free services.

c. **Data analytics solutions providers** step in to customise data analytics solutions to the needs of businesses; while **data storage providers** supply physical or cloud storage services to meet businesses' needs.

d. **Data aggregators** compile industry data and act as a one-stop shop for businesses that want sector-level data.

Data analytics, sharing and monetisation are subject to legislation and regulations which directly govern the usage, collection and disclosure of data.

Data analytics, sharing and monetisation in Singapore

The KPMG study found that the maturity of adoption of data analytics not only varies across sectors, but also among businesses within the same sector. The maturity in each sector was evaluated based on a five-stage maturity map developed by KPMG.[13] A brief overview of the maturity of each sector, including their stage of maturity, is set out below:

a. **Digital Media Sector *(Level 5)***. This sector was found to have one of the highest levels of maturity. Insights derived from customers' online behaviour patterns allow online advertising platforms (consisting of search marketing

[13] The five stages of the maturity map are (starting from the most basic level): (i) **Level 1:** awareness – where the organisation is only starting to become aware of data analytics and has no structured approach to data collection and analysis; (ii) **Level 2:** experimental – where the organisation is starting to commission and experiment with data analytics projects and takes a needs-based approach towards data collection and analysis; (iii) **Level 3:** cohesive – where the organisation has a structured approach to collecting data and performing data analytics, together with data analytics programs and proper data governance procedures in place, but has not used insights generated to drive business decisions; (iv) **Level 4:** business driver – where the organisation actively incorporates insights from its data analytics into its decision-making processes, and has integrated data collection and analysis across different business units, but enriched data is only being used by select users, such as the IT or data analytics department; and (v) **Level 5:** embedded – where the organisation not only actively uses data analytics in its business decisions but opens up access to its data analytical functions to all business units and users.

platforms and social marketing platforms) to better target advertisements and connect customers to businesses.

b. **Finance Sector**. The finance sector is relatively advanced in the use of data analytics, with the Monetary Authority of Singapore championing its use. Financial institutions collect very detailed customer data, including personal data. This data is analysed to perform targeted marketing, improve business operations, automate fraud detection, and customise products. The banking sector ***(Level 3.5)*** is more advanced than the insurance sector ***(Level 2)*** in its usage of data analytics.

c. **Healthcare Sector *(Level 2.5)***. The public healthcare sector has implemented data analytics while the private sector has been slower to do so. The key player in the public healthcare sector is the Integrated Health Information System Pte. Ltd.[14] which has set up a coherent framework for the collection of healthcare data (i.e. the National Electronic Health Records) and has driven the use of data analytics among public healthcare providers to improve patient care and to maximise the allocation of limited healthcare resources.

d. **Consumer Retail Sector**. There are varying levels of maturity for the adoption of data analytics within the consumer retail sector, with e-commerce businesses ***(Level 3.5)*** being more advanced in the collection and use of data as compared to brick-and-mortar stores ***(Level 1)***.

e. **Land Transport Sector**. The level of maturity of data analytics adoption varies significantly across different segments of the land transport sector. Ride booking services ***(Level 5)*** have embedded data analytics in their operations to allow them to price according to current demand and supply and to match riders and drivers, while public and private transport services ***(Level 2)*** are beginning to experiment with data analytics. The Land Transport Authority drives the data analytics initiatives among public transport operators, and also facilitates data sharing in this sector.

f. **Logistics Sector *(Level 2)***. The logistics sector has been slower in the adoption of data analytics. Due to Singapore's small geographical size and dense road network, businesses using traditional business models have not felt compelled to evolve. However, the rise of e-commerce retailers has increased the demand for delivery services, and correspondingly stimulated the use of data analytics within the logistics sector. Some data analytics is used on a limited scale by a handful of market players. The Info-

[14] Integrated Health Information Systems Pte. Ltd. is a private entity wholly owned by Ministry of Health Holdings Pte. Ltd.

communications Media Development Authority has unveiled an Urban Logistics Technology Roadmap for 2020 on the usage of technology to improve operation processes and optimise resources in the logistics sector.

The efforts of government agencies in championing the adoption of data analytics and data sharing in certain sectors, and the presence of international companies with very strong data analytics capabilities, appear to account for why certain sectors are more advanced than others.

Despite the benefits, businesses face challenges in further adopting data analytics due to manpower constraints (particularly a lack of middle management with data analytics capabilities), high initial infrastructure costs (in terms of setting up data collection and analytics programs), and gaps in data sets (data which some businesses are not in a position to collect). Certain sectors have also highlighted a lack of clarity with regard to the types of data which may be shared (even internally between departments of the same company), further limiting the adoption of data analytics.

Apart from data sharing which occurs as a result of active facilitation by government agencies, the sharing of data within or across sectors generally occurs on a very limited basis. Businesses are generally not keen to share data externally because of the need to comply with the relevant data protection regulations. Data is also viewed as a source of competitive advantage which would be lost if data is shared. Businesses are also wary that their revenue may be affected due to the loss of customer trust, should customers find out that their information is shared without consent.

The KPMG research study found that direct monetisation of data (i.e. selling of data sets) does not take place in the sectors surveyed. Instead, data is monetised indirectly through more targeted advertising and greater customisation in product offerings.

Implications on competition policy and law

The benefits arising from the adoption of data analytics and data sharing may not be fully realised if businesses engage in anti-competitive conduct in the course of adopting data analytics and/or data sharing. It is thus crucial for competition policy and law to foster a level playing field for businesses.

In the assessment of competition issues, the first step is usually the identification of relevant markets. As many data-driven industries are characterised by multi-sided platforms, it is important to take into account the interactions between different customer groups on different sides of the market. Where such multi-sided platforms involve non-monetary transactions in exchange for data, it may then be

appropriate to consider the data flow in defining the relevant markets, and to also adopt a quantitative assessment of non-price factors.

A summary of how business practices may be assessed under the Competition Act (Cap. 50B) ("the Competition Act"), is shown in the table below.

Section 34 prohibition: Anti-competitive agreements and concerted practices	
The sharing of data within the framework of existing rules can be pro-competitive.	There are generally no competition concerns when the data shared is historical; sufficiently aggregated and not attributable to a particular business; and not commercially sensitive, strategic or confidential. In contrast, an appreciable adverse effect on competition is more likely where there exists only a few companies operating in the market; where data sharing is frequent; where the data shared is commercially sensitive; and where the sharing is limited to certain participating companies in the market to the exclusion of their competitors and buyers. Unless the sharing of data under such situations can result in net economic benefits, it is likely to raise competition concerns. Another dimension of data sharing relates to the stakeholders involved in the sharing. There are unlikely to be competition concerns when businesses share data with consumers or government agencies. The sharing of commercially sensitive data such as current or future pricing or production capacity with competitors is likely to raise competition concerns unless such sharing gives rise to net economic benefits. Sharing of data with businesses in other markets and industries is unlikely to be problematic.
The use of algorithms by businesses can bring about efficiency gains; but where algorithms are used to implement or facilitate collusive outcomes or anti-competitive agreements, this	The use of algorithms allows businesses to make predictions and decisions more efficiently and achieve greater customisation in their products. However, algorithms have the potential of providing new and enhanced means to foster collusion, particularly because algorithms can enhance market transparency and the frequency of interactions between firms.

would likely infringe the Competition Act.	Where the use of algorithms is in furtherance of, or to support or facilitate any pre-existing or intended anti-competitive agreement or concerted practice, such cases are likely to infringe the Competition Act as they fall squarely within the existing enforcement framework. Similarly, where algorithms are used in classic 'hub-and-spoke' scenarios which involve competitors colluding through a third party intermediary, this would be anti-competitive. There has been lively discussion about whether the existing competition enforcement framework is adequately equipped to deal with possible future developments involving algorithms. There are currently no settled positions on these issues and as the increasing use of algorithms in the Big Data environment is currently an evolving field, it is perhaps too early for anyone to have the last word on the matter.
Section 47 prohibition: Abuse of a dominant position	
The assessment of dominance needs to take into consideration the unique features of data-driven industries. **The accumulation of a large data set in and of itself does not equate to a firm being dominant.**	Two key questions when assessing market power in data-driven industries are (i) whether the data could be replicated under reasonable conditions by competitors; and (ii) whether the use of data is likely to result in a significant competitive advantage. To answer these two questions, features of data-driven industries need to be taken into consideration. In general, market power may be strengthened by network effects, but can be weakened due to the existence of multi-homing, ease of access and substitutability of data, and market dynamics.

Even if a firm is found to be dominant, competition concerns will only arise when the firm engages in exclusionary conduct that has, or is likely to have, an adverse effect on the competitive process.	Even if a firm is assessed to be dominant, competition concerns will only arise when the firm engages in exclusionary conduct that has, or is likely to have, an adverse effect on the process of competition. Examples of exclusionary conduct that could arise in the context of data-driven industries are: a. *Discriminatory access* – where a dominant firm discriminates access to critical data for competitors. Discriminatory access may also be achieved through vertical integration, for example, where a firm discriminates against downstream competitors; or by engaging in bundling/tying. b. *Exclusive dealing* – where a firm abuses its dominance by entering into exclusive contracts with customers. This forecloses the entry of new competitors. c. *Refusal to supply* – under limited circumstances where the data cannot be replicated and no alternative solution is available, a refusal to supply access to data to competitors by a dominant firm may constitute an abuse of dominance.
Section 54 prohibition: Mergers that substantially lessen competition	
The analytical framework for merger assessment remains relevant for mergers that lead to data concentration.	The focus of CCS's merger assessment is on evaluating how the competitive constraints on the merger parties and their competitors might change as a result of the merger. When reviewing a merger between firms which leads to the consolidation of two previously separate data sets, CCS will assess whether the concentration of data could substantially lessen competition in the affected markets. As shown in past merger cases assessed by CCS[15] and other overseas competition authorities,[16] the current

[15] For example, CCS 400/004/14, *Notification for Decision of the proposed acquisition of SEEK Asia Investments Pte. Ltd. of the JobStreet Business in Singapore pursuant to section 57 of the Competition Act* (13 November 2014); and CCS 400/007/07, *Notification for Decision: Merger between the Thomson Corporation and Reuters Group PLC*. (23 May 2008).

[16] For example, Case No. COMP/M.4731. *Google/DoubleClick*, Commission Decision (11 March 2008); and Case No. COMP/M.7217. *Facebook/Whatsapp*, Commission Decision (3 October 2014).

	analytical framework for merger assessment is sufficiently flexible and robust, and remains relevant.
Protection of privacy is not a competition issue. However, where data protection is a non-price factor of competition, the treatment of personal data may affect how CCS considers and assesses the competitive dynamics of market.	While there have been calls for competition law to be applied to promote data protection and privacy policy, this approach does not appear to be consistent with the role or function of CCS. The objective of competition law is to promote the efficient functioning of markets towards enhancing the competitiveness of the Singapore economy. However, where data protection is a non-price factor of competition, the treatment of personal data may affect how CCS considers and assesses the competitive dynamics of a market. CCS's current analytical framework already takes into account competition on the basis of non-price factors, thereby enabling CCS to consider data protection as a non-price factor of competition within its assessment.[17]

Implications on personal data protection

While most companies recognise the potential gains that may result from data sharing, there is very limited data sharing activity occurring amongst businesses, whether within or across industries. One of the reasons cited was the need to comply with the relevant data protection regulations. To enable the benefits of data analytics to be realised while safeguarding personal data from being misused, PDPC has released several guidelines to provide clarity to businesses on what is permitted under the PDPA:

a. The Guide to Data Sharing provides greater clarity to businesses on how data can be shared in compliance with the PDPA, including for the purposes of data analytics. This guide also includes a framework for data sharing arrangements that may be exempted under the PDPA in circumstances where obtaining consent is impractical or undesirable.

[17] *CCS Guidelines on the Substantive Assessment of Mergers 2016*, para 2.4 states that "CCS will assess the above factors when assessing the non-coordinated effects of the merger situation, which arise when there is a loss of competition between the merger parties and the merged entity finds it profitable to raise prices and/or reduce output or quality. In so doing, CCS will consider the extent to which the merger parties are close competitors. The above factors are also considered in assessing whether a merger situation raises or leads to increased scope for "coordinated effects", which arise if the merger situation raises the possibility of firms in the market coordinating their behaviour to raise prices, reduce quality or output."

b. While the use of anonymised data is a good way in which businesses can derive better insights and efficiencies, there is a residual risk of re-identification. PDPC has issued a set of guidelines on anonymisation, highlighting the methods and measures that organisations can put in place to mitigate the risks of re-identification.

PDPC also understands that it may not always be feasible or desirable for businesses to obtain consent for the collection, use and disclosure of personal data. PDPC has thus released a *Public Consultation for Approaches to Managing Personal Data in the Digital Economy* to seek opinions on parallel bases other than consent. These parallel bases cater to circumstances where consent is not feasible or desirable, and where the collection, use or disclosure would benefit the public.

The study also considered the potential interactions between personal data protection and competition policy and law:

a. The objectives of competition policy and law, and data protection, are not mutually exclusive. For example, data portability [18] seeks to enhance competition between businesses by reducing switching costs. At the same time, it could build customer trust, potentially leading to a virtuous cycle of users being more willing to provide personal data to companies.

b. Businesses may use compliance with data protection rules as a reason for not sharing data (and *vice versa*). CCS and PDPC will continue to work together to assess such claims by businesses.

c. While promoting data protection and privacy is not consistent with the role of CCS, where data protection is a non-price factor of competition, the treatment of personal data may affect how CCS considers and assesses the competitive dynamics of a market.

Implications on intellectual property rights

Intellectual property rights are far more than mere legal rights. They enable rights-holders to exploit their intellectual creations and recoup investment in effort, time and financial resources. Intellectual property rights are highly valuable, strategic business assets. As the cornerstone of the innovation ecosystem, intellectual property is a powerful driver of growth for businesses and the economy in Singapore.

[18] The right to data portability allows for data subjects to receive the personal data, which they have provided to a data controller, in a structured, commonly used and machine-readable format, and to transmit those data to another data controller without hindrance.

Extent to which intellectual property law protects data[19]

Copyright law does not protect data per se, although a compilation of data may be protected if the data has been selected or arranged with sufficient creativity. In such cases, the protection still does not extend to the underlying data, but only to the selection or arrangement thereof. This means that there may be no liability for copyright infringement if the same data is copied but selected or arranged differently. In drawing this distinction, copyright balances private rights (by rewarding the right-holders' efforts in compiling the data), with public needs and interests (by keeping the data per se free for others to work on so that the public can benefit from further additions to the pool of results).

The law of confidence, on the other hand, offers some measure of protection over data per se. Facts and data (and even databases) may be protected as confidential information in an action for breach of confidence. This involves enforcing an obligation of confidence that has arisen between parties in relation to some confidential information (the data) that has passed between them.

Emerging opportunities for commercialisation where intellectual property rights, data and analytics converge

In the course of performing data analytics, copyrighted works (including compilations of facts and data) may be copied or reproduced, which may give rise to liability for copyright infringement. As part of a broader review of Singapore's copyright regime, an exception to infringement has been proposed to permit both commercial and non-commercial "text and data mining" activities. If implemented, this exception will facilitate and encourage data analytics and interpretation. The exception will also clarify the use of legitimately accessed copyrighted works for data analytics, and thereby encourage data sharing and access for such purposes.

In the field of patent law, data analytics has already begun to unlock new commercialisation opportunities. Data analytics technology enables patent searches to be conducted far more economically, efficiently and accurately than manual searches. Data analytics is accelerating patent commercialisation and dissemination of the knowledge embodied in these patents in a growing number of ways.

Interface between intellectual property law and competition law

Both intellectual property law and competition law share the same basic objective of promoting economic efficiency and innovation. Intellectual property law

[19] For completeness, it should be noted that in addition to the protection afforded under intellectual property law, data may be protected by way of contract – dealings with data can potentially be enforced as contractual obligations independent of any intellectual property rights.

does this through the provision of incentives for innovation while competition law does this through the promotion of competitive markets.

In general, the legitimate exercise of an intellectual property right, even by a dominant undertaking, will not be regarded as an abuse of a dominant position. Typically, it is only in limited circumstances that the refusal to authorise a third party to use an intellectual property right may amount to a violation of competition law. Foreclosure through the refusal to supply may amount to an abuse of dominance insofar as it constitutes an attempt to maintain a monopoly in the market by edging out existing players, or preventing or discouraging the entry of new players.

Specifically in relation to data or data sets, the competition authority or courts in general are unlikely to require an intellectual property right-holder to grant access, unless such data or datasets are viewed as an essential facility, or objectively necessary, and denying access would clearly foreclose competition such as preventing the emergence of new products which the dominant player is not offering, thereby stifling innovation. Since data or data sets are accorded limited protection under Singapore's intellectual property laws and raw data sets are usually replicable, it would be unlikely that competition authorities or courts would have to compel the supply of or access to data sets. A key consideration for any assessment is the importance of innovation to foster competition.

Concluding remarks and next steps

The accumulation, sharing and analysis of data can bring about a wide range of benefits. However, these benefits may not be realised if businesses engage in anti-competitive conduct or misuse personal data. Competition law, personal data protection law and intellectual property law have their respective roles in ensuring businesses and consumers are protected from anti-competitive conduct; that an individual's personal data is safeguarded and businesses can leverage on personal data for legitimate use; and that incentives for innovation are provided through the protection of intellectual property rights.

Issues in competition policy and law, personal data protection and intellectual property rights are expected to overlap in the context of data-driven industries. One area with potential overlap would be data portability. In this regard, PDPC and CCS will be embarking on a joint study to explore the consumer protection and competition related issues of data portability.

Overall, while the ease of compilation of large data sets and proliferation of data analytics may be fresh developments, the existing analytical framework for competition assessment remains sufficiently flexible and robust to deal with competition issues that may arise in the context of data-driven industries. Nonetheless, CCS will stay vigilant, monitoring new developments to ensure it has the necessary tools to detect and deter

any possible harm to competition in markets in Singapore that emerges from the use of new technologies. Businesses should continue to operate on a level playing field even in a Big Data environment, to innovate, stay competitive and better serve their customers.

II. INTRODUCTION

1. The use of data is on the rise, with businesses and governments having identified the potential that data has to fundamentally accelerate the growth of economies, bring about opportunities, and create new challenges.[20] With the exponential growth of computing technology and power, advanced forms of data analytics are increasingly being adopted to derive more insights from data and ultimately unlock value from the vast amount of data that is accessible today.

2. For a city-state like Singapore with almost no natural resources (except human capital), the ability to capitalise on data analytics and data sharing provides a new avenue to promote economic growth through innovation and improvement in productivity. The potential and opportunities for Singapore are enormous. For businesses, data analytics has begun transforming business practices across different industries, enhancing efficiency, and enabling new business models that are driven by data. For consumers, benefits include reducing information asymmetry and search costs, and improving consumer experience. The sharing of data, within the confines of regulatory safeguards, has the potential to unlock further value from data and bring about greater innovation for both businesses and consumers.

3. Analysys Mason estimated in 2014 that data-driven innovation across six key sectors of the economy[21] will contribute more than S$4.30 billion to the Singapore economy in 2013, in the form of consumer surplus (i.e. lower cost of goods and services) and producer surplus (i.e. higher profits retained).[22] This amount is expected to grow almost three times to S$11.6 billion in 2018.[23] Beyond the economic benefits, there are also social benefits, including better-informed government policies through data analytics.

4. To capitalise on the opportunities from data analytics and data sharing for the Singapore economy and society, the Government has been actively promoting the adoption of data analytics and data sharing as part of the strategy for Singapore's next stage of growth and development. In February 2017, the Committee on Future Economy ("CFE") outlined Singapore's key strategies to stay ahead in a challenging

[20] The Economist (6 May 2017). *Data is giving rise to a new economy*.
[21] The traditional verticals considered in the study are manufacturing; trade (wholesale and retail); transport and logistics; financial services; information and communications; and health, education and social services. Analysys Mason estimates that these verticals make up 69% of GDP in Singapore in 2013, and about 65% of employment. See Analysys Mason (15 July 2014). *Data-driven Innovation in Singapore*, pp. 25.
[22] Analysys Mason (15 July 2014). *Data-driven Innovation in Singapore*, pp. 33.
[23] Analysys Mason (15 July 2014). *Data-driven Innovation in Singapore*, pp. 39.

climate.[24] Data is a recurring theme in the CFE report, and the strategies set out in the CFE report include building capabilities in data analytics and cybersecurity, harnessing data as an asset, and building strong digital capabilities in the economy by helping Small and Medium Enterprises ("SMEs") adopt digital technologies.

5. In line with the CFE strategy, the Data Innovation Programme Office ("DIPO") has been set up within the Info-communications Media Development Authority of Singapore ("IMDA") in 2017 to catalyse the adoption of data-driven innovation in Singapore.[25] DIPO will work closely with the industry to understand industry needs and to match these needs with appropriate data solutions. It will also assist businesses by facilitating the collection, protection, analysis and sharing of data.[26] At the same time, the Smart Nation and Digital Government Group was formed in the Prime Minister's Office to drive digital transformation for the public service, strengthen government information and communication technology infrastructure, and improve public service delivery through the application of digital and smart technologies.[27] In addition, a wide range of strategies and initiatives are being implemented in different sectors of the economy by other government agencies to encourage and facilitate data-driven innovation projects.[28]

6. Aligned with the Whole-of-Government's efforts to promote the adoption of data analytics and data sharing, the Competition Commission of Singapore ("CCS")

---

[24] Committee on the Future Economy (7 February 2017). *Report of the Committee on the Future Economy*.

[25] Ministry of Communications and Information. *Roles of the Data Innovation Programme Office*.

[26] To encourage data sharing amongst businesses, DIPO will be implementing the **Data Sandbox Programme**, which will provide a neutral, trusted and secure data exchange environment to help businesses and community experiment and discover the value of data and data exchange. DIPO will also be sharing frameworks, policy guidelines and best practices for data collection, exchange and transaction. Through the Data Sandbox Programme, the government aims to accelerate cross-companies and sector data exchanges for competitiveness and encourage new data services and innovative data technologies to be developed. See *Welcome & Opening Address* by IMDA Assistant Chief Executive (Development), Mr Khoong Hock Yun at Cloud Asia 2017, 11 April 2017.

[27] GovTech Singapore (20 March 2017). *Formation of the Smart Nation and Digital Government Group in the Prime Minister's Office*. Media Release.

[28] For instance, the **"SMEs Go Digital"** programme by IMDA is in response to CFE's call to help SMEs adopt digital technologies and adapt to a world where technology is increasingly disrupting businesses. The programme has three main initiatives, to provide pre-approved technology solutions; provide specialist technology advice; and support to innovative emerging technology solutions. In addition, the **Enhanced iSPRINT** programme has been put in place by IMDA to support SME's use of technology to enhance the productivity and growth of SMEs. This programme aims to boost supply of sector solutions from vendors by scaling up proven sector solutions and pilot sector-specific solutions, including the use of data analytics. Another example is the **Data Centre Park**, a multi-agency effort by IMDA, the Economic Development Board and JTC Corporation to strengthen Singapore's position as an economic and infocomm hub through attracting multinational corporations and enterprises to set up their headquarters and premium data centre operations in Singapore. This will attract internet and media companies to host their content and services in Singapore, thus attracting more Internet traffic and international network providers.

commissioned a research study to understand the landscape in Singapore in this regard, including the opportunities and challenges for businesses arising from the proliferation of data analytics, as well as the sharing and monetisation of data. In collaboration with the Personal Data Protection Commission, Singapore ("PDPC"), and the Intellectual Property Office of Singapore ("IPOS"), CCS also considered the implications of data analytics and data sharing on competition policy and law, personal data protection and intellectual property rights.

7. This paper is structured as follows:

a. Section III explains the objectives of the paper, including the methodology;

b. Section IV introduces the key concepts (e.g. "data", "Big Data") that are discussed in this paper;

c. Section V provides an overview of the data landscape in Singapore, including the key players and their roles, as well as the regulatory landscape;

d. Section VI elaborates on the findings in relation to the adoption of data analytics, sharing and monetisation practices in Singapore;

e. Section VII discusses the implications on competition policy and law;

f. Section VIII discusses the implications on personal data protection, including the interface between competition policy and law, and personal data protection law;

g. Section IX discusses the implications on intellectual property rights, including the interface between competition law and intellectual property law; and

h. Section X summarises the key findings in this paper and outlines next steps.

III. OBJECTIVES OF THIS PAPER

8. This paper seeks to explore:

a. The current industry landscape for the use of data analytics in Singapore, including the key players and their roles;

b. How industries are being transformed or will be transformed by harnessing data analytics;

c. The adoption of data analytics, the prevalence of data sharing and monetisation, the underlying motivations or reservations of businesses when dealing with data; and

d. The implications of the above on competition policy and law, personal data protection and intellectual property rights in Singapore.

Methodology

9. The research for this paper was conducted from January to July 2017. Relevant government agencies and businesses were engaged to provide feedback on the current industry landscape. In this regard, CCS commissioned KPMG Services Pte. Ltd. ("KPMG")[29] to map out the data landscape in Singapore by tapping into its domain knowledge and contacts in the industry. KPMG was involved in conducting interviews with businesses to understand their data analytics, sharing and monetisation practices. The businesses interviewed included firms across various industries and third party providers of data analytics solutions and infrastructure. The feedback received was complemented with desktop research.

10. Stakeholders who participated in this research study did so voluntarily. CCS thanks all stakeholders for providing their time and valuable inputs.

11. In collaboration with PDPC and IPOS, CCS also assessed the implications of the proliferation of data analytics and data sharing on competition policy and law, personal data protection law and intellectual property rights, particularly since some of these issues may potentially overlap.

[29] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore".*

IV. INTRODUCTION TO DATA ANALYTICS, DATA SHARING AND DATA MONETISATION

12. This section introduces and discusses the key terms and concepts explored in this paper.

What is data?

13. Data is generally any factual information that can be used for reasoning, discussion, and/or calculation.[30] Data can be characterised by several dimensions which may overlap. Data can be classified as personal or non-personal, and may relate to different subject matter, such as financial, economic or geographical data. Furthermore, data can differ in its nature (i.e. quantitative or qualitative), granularity (i.e. specific or aggregated) and quality (i.e. varying degrees of accuracy and reliability).

14. From an economic perspective, data is said to be non-rivalrous, excludable, and its value may vary according to usage and time: [31]

a. **Non-rivalrous**: Data is non-rivalrous, that is, the same data may be used concurrently by multiple users for different purposes. For example, public data sets made available by government agencies can be used by different parties with different objectives at the same time.

b. **Excludable:** Data may be excludable as it is possible to deny another party access to it.[32] Access to data could be denied due to regulations, such as intellectual property rights or personal data protection laws.

c. **Value of data may vary over time and usage**: The value of data is dependent on the type of analysis performed. Some types of data have enduring value and as such only need to be collected once (e.g. name or date of birth), whereas other types of data are more transient in nature, being relevant for a shorter period of time (e.g. transactions).

[30] Definition is obtained from Merrian-Webster Online Dictionary.
[31] Competition & Markets Authority (June 2015). *The commercial use of consumer data*, pp. 75-76; and Harry van Til, Nicolai van Gorp, Katelyn Price (13 June 2017). *Big Data and competition*, ECORYS, prepared for the Ministry of Economic Affairs, Netherlands.
[32] David Besanko and Ronald R. Braeutigam (2011*). "Microeconomics (4th Edition)",* John Wiley & Sons Inc., pp. 719.

15. Data can be collected (provided voluntary or involuntary), observed or inferred.[33] First-party data, such as consumer data, is obtained from a direct relationship that the company has with the source of data (e.g. consumers), while third party data is obtained through the exchange with or purchase from another company.[34]

16. While data collection is not new, advancements in technology have dramatically increased the rate that data is generated and collected. To put things into perspective, for every minute in 2014, nearly 220,000 new photos were posted on Instagram, 72 hours of new video content were uploaded on YouTube, and Amazon received over $80,000 in revenue for its online sales.[35] McKinsey's 2016 global report also estimated that 400 terabytes of data were exchanged globally per second – a rate 45 times greater than that of 2005.[36] Data generation and collection has never been easier, as we leave behind an almost inevitable digital footprint that can be tracked on our electronic devices. In view of increasing numbers of connected users, devices and sensors, the proliferation of data is set to continue.

17. The move into a digital age has ushered in "Big Data". Big Data is loosely defined as data sets that are so large or complex that traditional data processing application software programmes are inadequate to deal with them.[37] Undoubtedly, the *volume* of the data set is of paramount importance for analytical purposes. Minimal analysis can be performed with few data points. However, the large volumes of data processed is not what makes Big Data "big". *Variety* and *velocity*, as put forth by META Group (now Gartner) in their "3Vs" framework,[38] play important roles as well. The "3Vs" are as follow:

a. *Volume* refers to the quantity of data, generated or collected. It determines the potential value and insight that can be derived from the data as only a limited analysis can be performed when there exist only few data points.

b. *Variety* refers to the different types and sources of data that are now available for concurrent analysis. Firms which are able to merge varied data

[33] Autorité de la Concurrence and Bundeskartellamt (10 May 2016). *Competition Law and Data*, pp. 6-7.
[34] Autorité de la Concurrence and Bundeskartellamt (10 May 2016). *Competition Law and Data*, pp. 12.
[35] Susan Gunullus (12 July 2014). *The Data Explosion in 2014 Minute by Minute – Infographic*, ACI.
[36] Jacques Bughin & Susan Lund (9 January 2017). *The Ascendancy of International Data Flows*. Vox EU.
[37] Chris Snijders, Uwe Matzat, and Ulf-Dietrich Reips (2012). *'Big Data': Big Gaps of Knowledge in the Field of Internet Science*. International Journal of Internet Science 2012, 7(1), pp. 1-5.
[38] Doug Laney (6 February 2001). *3D Data Management: Controlling Data Volume, Velocity, and Variety*. META Group: Application Delivery Strategies.

for analysis may be able to gain valuable insights that were not previously possible with traditional data sources that tend to be more limited.[39]

c. *Velocity* refers to the speed at which the data is generated and processed to meet the demands and challenges that lie in the path of growth and development. High-speed processing allows for swift and accurate actions and decisions to be taken.

18. Big Data is often defined by a fourth V – *Value*[40] (i.e. the value of the insights derived from data sets). Value is both a cause and consequence of the aforementioned 3 "Vs". On the one hand, the value of the insights is derived from the volume, variety and velocity of data sets.[41] On the other hand, the volume and variety of data being collected and the velocity in processing data have increased because of the value derived from data.[42]

19. For the purposes of this study, references to the term "data' will include Big Data, unless otherwise specified, while specific references to Big Data will refer to data with the characteristics highlighted in paragraphs 17 and 18 above.

What is data analytics?

20. The value of data is derived from the analysis of data, which is generally the process of examining data sets in order to draw conclusions about the information they contain. Traditionally, the analysis of data refers to the use of business intelligence ("BI") tools in business operations and performance management. BI is mainly backward looking, focusing on trend analysis and historical patterns.[43]

21. In today's context, however, the advancement in computing power and capabilities to sieve through colossal data sets has paved the way for more advanced

[39] Maurice E. Stucke & Allen P. Grunes (9 June 2016). *"Big Data and Competition Policy".* Oxford Printing Press, pp. 21-22.

[40] Maurice E. Stucke & Allen P. Grunes (9 June 2016). *"Big Data and Competition Policy".* Oxford Printing Press, pp. 22-23; Veracity (i.e. quality) and variability (i.e. consistency) are sometimes included in a separate framework: see generally, Kelly Leboeuf (27 January 2016). *The 5Vs of Big Data: Predictions for 2016.* Exelacom.

[41] Big Data would have less value if companies could not process large volumes of data efficiently (time element) and effectively (value element).

[42] Maurice E. Stucke & Allen P. Grunes (9 June 2016). *"Big Data and Competition Policy".* Oxford Printing Press, pp. 22-23.

[43] With particular regard to how BI may be treated as a separate category from advanced analytics, see generally, Margaret Rouse (2016). *Data Analytics (DA).* Tech Target.

analytics, such as predictive analytics,[44] machine learning[45] and data mining.[46] Often, inductive statistics[47] and concepts from nonlinear system identification[48] are used to infer from large sets of data relationships and dependencies, or to perform predictions of outcomes and behaviours.[49] For the purposes of this study and to align with the definition adopted by KPMG in their study (see paragraph 66), "data analytics" as used within this paper will refer to the use of advanced analytics, which is predictive in nature.

22. There is much preparatory work before data can be used. This includes collecting, integrating and preparing data. Data is then used for developing, testing and revising analytical models to ensure that they produce accurate results. The various steps are categorised as follow:[50]

a. **Data Collection**: Data can be sourced from a variety of sources, such as being collected through business operations, purchases from third parties, or through publicly available sources.

b. **Data Integration**: For an accurate analysis, data sets should be consistent, error-free and unique (i.e. no duplicates). Standardisation is also important because data may be obtained from different source systems. Thus, data has to be treated and transformed into a common format before being uploaded into data warehouses or data lakes. Data warehouses only store

[44] Predictive analytics refer to the use of algorithms to find patterns in large volumes of data, thus enabling predictions to be made about the future. See generally, SAP (2017). *Your Predictive Journey.*
[45] Machine learning refers to the technique whereby algorithms are programmed to iteratively "learn" from data, allowing computers to independently adapt to produce reliable, repeatable decisions and results. See generally, SAP (2017). *Your Predictive Journey.*
[46] Data mining refers to sorting through large data sets to identify trends, patterns and relationships. See generally, Jiawei Han, Micheline Kamber (2000). *"Data Mining: Concepts and Techniques".* Morgan Kaufmann Publishers, pp. 3.
[47] Inductive statistics (or inferential statistics) refers to the method of making decisions or predictions about a population based on data obtained from a sample of that population. See generally, Agrestum Franklin and Klingenberg (2005). *"Statistics: The Art and Science of Learning from Data".* Pearson (4th Ed.).
[48] System identification is identifying relationships between inputs and outputs. A nonlinear system is defined as any system where output is not directly proportional to the input. In mathematical terms, a relationship is non-linear if the equation does not represent a straight line. Nonlinear models are frequently obtained from a theoretical modelling on the basis of *priori* knowledge on the nature and the intrinsic mechanisms of the systems. See generally, Rodolfo Orjuela, Benoit Marx, Jose Ragot, Didier Maquin (2013). *Nonlinear System Identification Using Heterogeneous Multiple Models*. International Journal of Applied Mathematics and Computer Science 23(1), pp. 103-115.
[49] Bhabani Shankar Prasad Mishra, Satchidananda Dehuri, Euiwhan Kim, Gi-Name Wang (2016). *"Techniques and Environments for Big Data Analysis."* Springer, pp. 115.
[50] Margaret Rouse (2016). *Data Analytics (DA)*. Tech Target.

structured data,[51] whereas a data lake (e.g. Hadoop) stores all kinds of data – structured, semi-structured, and unstructured.

c. **Data Analytics**: Once data is standardised, an analytical model is built using predictive modelling tools or other analytics software and programming languages such as Python, Scala, and R. The model will continue to be "trained" until it develops all the functions it was designed to acquire and may continue to "self-improve" with the further input of data.

d. **Data Interpretation**: Finally, the insights generated by analytical models are simplified for end-users or business executives to aid in their decision-making. This is achieved via data visualisation techniques such as charts and graphs.

23. Underlying the processes outlined above are the supporting infrastructures that have to be put in place, including data storage hardware and software, and data analytics software. Furthermore, technical expertise (either in-house or out-sourced) is required to manage the processes above, interpret the results of the data analytics, and translate them into business decisions or actions.

What is data sharing?

24. Data sharing refers to the act of making data available to other stakeholders, both internal and external. The objective behind data sharing is usually to derive new insights beyond one's own data set(s), or to solve business problems in a targeted way. Internally, businesses may share data between different business units. Externally, businesses may share their data with different stakeholders, including consumers, government, other players in the industry or other businesses in another industry.

What is data monetisation?

25. Often, the value of data can be translated into monetary value by increasing a company's revenues or decreasing costs.[52] There are four commonly applied business models for the monetisation of data:[53]

[51] Structured data is information that is highly organized. Structured data has a predetermined form or structure, and thereby can be processed directly (e.g. audit reports). In contrast, unstructured data has little or no organization. Unstructured data is usually associated with content (e.g. emails). See generally, Hennin Baars and Hans-George Kemper (7 April 2008). *"Management Support with Structured and Unstructured Data - An Integrated Business Intelligence Framework."* Information Systems Management 25(2), pp. 132-148.

[52] KPMG (2015). *Framing a winning data monetization strategy*, pp. 2.

[53] KPMG (2015). *Framing a winning data monetization strategy*, pp. 5.

a. *Return On Advantage Model* refers to the use of internal performance indicators and (sometimes) external demographics to segment customers for more effective business strategies. Such models adopt customer profiling, enabling targeted marketing, risk mitigation and fraud detection. In this model, data can be monetised both directly (e.g. advertising firms) and indirectly (e.g. traditional businesses).

b. *Premium Service Model* refers to how data is offered to customers as an additional service. For instance, statistics on sales are provided at an additional charge. Here, data is monetised directly.

c. *Differentiator Model* refers to data being offered as a value-added service to differentiate an enterprise from its competitors.[54] By doing so, the enterprise aims to build brand loyalty and deter customers from switching. In this case, data is monetised indirectly.

d. *Syndication Model* describes a business framework where data is transformed and delivered to third party entities. There is usually some intellectual input in consolidating, processing and/or analysing of data (e.g. ease of collection, complexity of algorithms). Such data is typically not easy to replicate, giving the data its value. Other times, data is aggregated and presented in reports to be sold.[55] In this model, data is monetised directly.

26. Against the backdrop of monetisation, data then assumes an enhanced status as a valuable asset that can deliver positive financial outcomes.

[54] For example, logistics companies may provide reports relating to the movement of goods to its customers to increase the ease of predicting demand, which would differentiate this logistics company from its competitors.

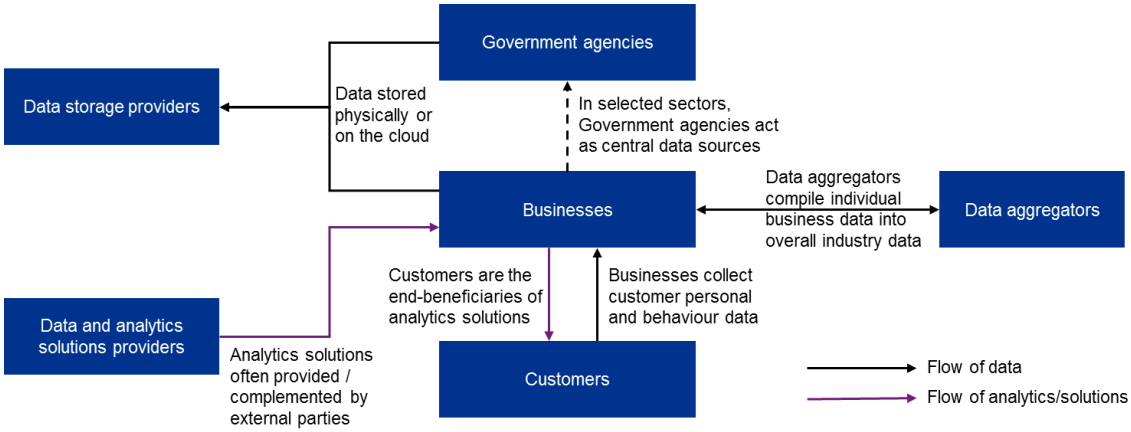
[55] For example, reports by research organisations such as IMS Research Ltd., Nielsen Holdings PLC, and Euromonitor International.

V. DATA LANDSCAPE IN SINGAPORE

Key players

27. The main players in the data landscape in Singapore are government agencies, businesses, customers, data analytics solutions providers, data storage providers, and data aggregators. The diagram below describes the role of and relationship between each player. [56]

Figure 1. Overview of the data landscape in Singapore



(1) Government

28. As outlined in paragraphs 4 and 5, the Singapore Government has been actively rolling out a wide range of strategies and initiatives in different sectors of the economy to encourage and facilitate data-driven innovation projects.

29. This is exemplified by government agencies who are shaping the landscape through the provision of data to industries or the public in various sectors. Government agencies are in a privileged position to collect data that cannot be easily obtained by the private sector as a result of their role in law enforcement, provision of public services and collection of official statistics. These roles make the public sector one of the biggest data owners in the economy.[57] The provision of data is not only meant for research purposes or businesses, but also for end-consumers. For example, the Urban Redevelopment Authority ("URA") and the Housing and Development Board ("HDB") release data on transacted prices and rental information for private and public

[56] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 3-6, section 2.

[57] Organisation for Economic Co-operation and Development (27 October 2016). *Big Data: Bringing Competition Policy to the Digital Era*. DAP/COMP(2016)14, pp. 29-30.

housing units to assist home-buyers in making informed decisions.[58] Government agencies generally do not look to monetise (i.e. sell) data, but instead look to unlock the positive externalities generated from the wider access to data.[59] For example, the Land Transport Authority ("LTA") provides land transport data on DataMall for free, so that app developers can design useful tools to enhance commuters' experience on public transport; and the Monetary Authority of Singapore ("MAS") publishes data as Application Programming Interfaces to provide financial institutes and application service providers more opportunities to serve their customers better.[60]

30. Within Government, data analytics is also employed to streamline processes, resolve issues and for policy planning purposes. For example, the Government Technology Agency of Singapore ("GovTech") provides the foundation for this by building capabilities in new technologies, including focusing on application design, data science and cybersecurity. LTA employs data analytics for public transport planning purposes[61] and URA collaborates with relevant planning agencies to research into the use of Geographic Information System[62] modelling, analytics, and visualisation for scenario and options analysis in planning.[63]

(2) Businesses

31. Businesses are key in the data landscape in that they collect, generate and use data. Businesses have access to customer data through their daily operations and interactions with customers. Businesses usually collect data in relation to their own operations and market data more generally.

32. A business that is able to generate insights from data and tailor its products or services to suit customer preferences is more likely to gain a competitive advantage over other businesses that do not employ data analytics practices.

(3) Customers

33. Customers, paying or otherwise, contribute significantly to the data generation process, whether voluntarily or involuntarily. A customer's personal data, purchase

---

[58] Urban Redevelopment Authority (1 April 2015). *CEA, HDB and URA's reply, 1 Apr 2015*. Media Room.
[59] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 3, section 2.1.1.
[60] Monetary Authority of Singapore. *Application Programming Interfaces (APIs)*.
[61] Ministry of Communications and Information (28 March 2017). *Towards a Smarter, Greener, and More Inclusive Public Transport System*. Press Room.
[62] A Geographic Information System is a system designed to capture, store, manipulate, analyse, manage and present spatial or geographic data.
[63] Urban Redevelopment Authority. *Integrated City Planning and GIS-Enabled mapping, Modelling and Analysis (GEMMA)*.

habits, transaction histories or other behavioural patterns allow businesses to better cater their product offerings to meet their customers' needs. In the process of using certain free services, such as email and social media services, a customer may inadvertently provide personal and other information to the services providers, or may consent to the access of their data in return for certain free services.

(4) Data analytics solutions providers

34. At this point in time, most businesses do not usually perform data analytics as part of their core function. Rather businesses that require such services source these from external parties. These external parties provide a range of services,[64] and may or may not have access to actual data because they sometimes only provide software solutions or work with fabricated data. Businesses may also prefer their data to remain at their premises, requiring that solution providers work on their premises.

35. Third party mobile application developers also feature significantly in making data understandable and usable to end customers. These developers usually rely on free publicly-available data, which in turn makes it harder for them to directly monetise their applications through download fees, given that there are typically competing applications that are based on the same data set. Popular applications are, however, able to generate sizable advertising revenue, or generate revenue through in-app purchases.

36. Data analytics is often not just tied to software, but also hardware. For example, hardware used for data analytics needs to be sufficiently advanced to support the software running on the IT systems. Apart from online or mobile platforms, there may be other ways in which hardware is used to collect data, such as using sensors in the healthcare sector that allow the remote monitoring of patients.

(5) Storage providers

37. Data can be stored in two main ways – physically or in remote servers accessed from the cloud. Physical storage of data may be on-site or off-site. Many businesses store data on their premises, even though cloud storage is acknowledged by industry players as "the way of the future".

38. Cloud storage brings benefits such as the ability to perform real-time data analysis as data can be uploaded into the servers in real-time and businesses are able to access the data from anywhere in the world and conduct data analysis through cloud-based data analytics software. Globally, the largest cloud storage provider is Amazon Web Services ("AWS"), through its Simple Storage Service, or otherwise known as S3. Cloud providers are also moving to provide cloud-based data analytics

[64] Examples of data analytics services are trend prediction, route optimisation and data visualisation.

services that are often pay-per-use – this reduces the infrastructure investments businesses need to make. These solutions are nimble, in that they allow businesses to try new solutions very quickly, and move on to another one if the tested solution does not work.

39. However, businesses have raised concerns with cloud storage including the over-dependence on a single provider and the control the cloud storage provider has over the data that businesses own. That said, businesses have also raised concerns about the security of physical data storage.

(6) Data aggregators

40. Data aggregators (e.g. AC Nielson, Euromonitor) compile industry data and act as a one-stop shop for businesses that require sector-level data. The arrangements that data aggregators have with industry players vary – some data aggregators engage industry players on a quid pro quo basis, trading industry reports for insights, while others rely on individual relationships to gather insights.

41. Data aggregators add value to the data collection and compilation process by incorporating primary (e.g. shop surveys, interviews) and secondary research into standard data. Also, while individual businesses have data specific to themselves, data aggregators are able to extrapolate data and form insights at the industry and sector level.

42. A new form of data aggregator, data brokers, has emerged.[65] Data brokers collect data on individuals through many different channels, including personal and demographic data, social media feeds, browser histories and online transactions. This data is then sold to businesses for marketing purposes. Data brokers prefer to keep their business models confidential, as they rely on customers unknowingly making data available. However, the authenticity of such data has been questioned.[66]

Regulatory landscape pertaining to data protection and usage

43. Data analytics, sharing and monetisation are all subject to legislation and regulations directly governing the usage, collection, and disclosure of data. Legislation and regulations include those which apply generally to all market players in Singapore, alongside those that are sector-specific.

General legislation and regulations pertaining to data protection and usage

[65] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 5, section 2.1.6.
[66] Terence Lee (3 April 2014). *See how your private data is being sold without your permission at one cent apiece*. Singapore Business Review.

44. In Singapore, personal data is protected by the Personal Data Protection Act ("PDPA") enforced by PDPC. The PDPA ensures a baseline standard of protection for personal data across the economy by complementing sector-specific legislative and regulatory frameworks. This means that organisations will have to comply with the PDPA as well as the common law and other relevant laws that are applied to the specific industry to which they belong, when handling personal data in their possession. The PDPA protects individuals' personal data while at the same time, enabling organisations to leverage personal data for legitimate uses and business innovations that can deliver greater benefits for individuals and the society.

45. The PDPA takes into account the following concepts:

a. **Consent** – Organisations may collect, use or disclose personal data only with the individual's knowledge and consent (with some exceptions);

b. **Purpose** – Organisations may collect, use or disclose personal data in an appropriate manner for the circumstances, and only if they have informed the individual of the purposes for the collection, use or disclosure; and

c. **Reasonableness** – Organisations may collect, use or disclose personal data only for purposes that would be considered appropriate to a reasonable person in the given circumstances.[67]

46. The implications of the PDPA on data analytics and data sharing will be further elaborated upon in section VIII.

47. The PDPA operates alongside other rules and legislation which pertain to the disclosure of data generally. Notably, the PDPA does not apply to public agencies and organisations acting as agents of public agencies in relation to the collection, use and disclosure of personal data.[68] Public agencies are governed by internal rules that adhere to the same principles of the PDPA. Other relevant legislations include the Official Secrets Act (Cap. 213) which contains provisions preventing the disclosure of official documents and information, and the Statutory Bodies and Government Companies (Protection of Secrecy) Act (Cap. 319), which contains rules on the disclosure of secret or confidential information held by statutory boards or Government-linked companies.

48. Apart from the PDPA, the intellectual property rights regime of Singapore for which IPOS is responsible, gives rise to issues relating to the ownership and use of

[67] Personal Data Protection Commission. *Legislation and Guidelines – Overview*.
[68] Pursuant to section 4(1)(c) of the *Personal Data Protection Act 2012*.

data, derived data and the results of data analysis. Similar to the functioning of the PDPA, stakeholders need to take into account intellectual property law considerations when using data. The implications of intellectual property rights to data analytics and data sharing will be elaborated upon in section IX.

Sector-specific legislation and regulations pertaining to data protection and usage

49. There are other sector-specific rules governing the usage, collection, and disclosure of data in Singapore.[69]

50. For instance:

a. **The Banking Act (Cap. 19, 2008 Rev. Ed.)** sets out rules which provide for the licensing and regulation of the banking sector. Section 47(1) of the Banking Act provides that "customer information shall not, in any way, be disclosed by a bank in Singapore or any of its officers to any other person except as expressly provided in this Act." The Third Schedule to the Banking Act sets out circumstances under which customer information may be disclosed. In addition, merchant banks are subject to the banking secrecy provisions as set out in the Banking Regulations (Cap. 19, Rg. 5) ("the Regulations"). Regulation 10 states that section 47 and the Third Schedule to the Act, as modified by the Second Schedule and Third Schedule to the Regulations, shall apply to merchant banks and any person who contravenes these secrecy provisions will be subject to penal consequences.[70] Further, MAS may revoke the licence issued to a bank if it is satisfied that the said bank is "contravening the provisions of the Act".[71] These banking secrecy rules impact how financial institutions in Singapore may deal with their customers' data, and could limit the financial sectors' rate of data sharing.

b. **The Private Hospitals and Medical Clinics Act (Cap. 248)** ("PHMCA") sets out the rules for the control, licensing and inspection of private hospitals, medical clinics, clinical laboratories and healthcare

[69] Personal Data Protection Commission. *Overview of Legislation and Guidelines*.

[70] Section 47(6) of the Act states that "any person who contravenes sections 47(1) or 47(5) shall be guilty of an offence and shall be liable on conviction: (a) in the case of an individual, to a fine not exceeding $125,000 or to imprisonment for a term not exceeding 3 years or to both; or (b) in any other case, to a fine not exceeding $250,000." Paragraph 6 of the Second Schedule to the Regulations sets out the same consequences, which will apply to unauthorised disclosure of customer information by a merchant bank in Singapore, any of its officers, or any person who receives customer information pursuant to the provisions of the Banking Act or the Regulations.

[71] Section 20 of the *Banking Act* (Cap.19, 2008 Rev. Ed.).

establishments. Section 13 of the PHMCA sets out provisions to safeguard the confidentiality of information which is held by any private hospital, medical clinic, clinical laboratory and healthcare establishment licensed under the PHMCA.[72]

c. **The Human Biomedical Research Act 2015** ("HBRA") regulates the conduct of human biomedical research in relation to human research participants, tissue and health information. Sections 6 to 12 set out the requirements relating to obtaining appropriate consent for human biomedical research. Section 13 and the Fifth Schedule to the HBRA set out the circumstances under which appropriate consent for human biomedical research may be waived.

51. In addition, the PDPC has published Sector-Specific Advisory Guidelines which aim to address the unique circumstances faced by select sectors in complying with the PDPA and provide guidance on how market players within these select sectors may comply with the PDPA.[73] The PDPC has also provided comments and suggestions to sector-specific guidelines which are developed by industry associations.[74]

52. The implications of the sector-specific rules and regulations on the data landscape is examined in more detail at paragraphs 111 and 112.

Data Localisation Rules

53. Data localisation requirements in general impose a legal condition on businesses, both local and foreign, to host a copy of the data within the country and restrict the movement of personal data out of the country. Proponents for data

[72] Section 13(1) of the *PHMCA* states as follows: "Except in the case of a prosecution for an offence under this Act or any regulations made thereunder, the Director and an authorised officer shall not be compellable in any proceedings to give evidence in respect of, or to produce any document containing, any information which has been obtained from any private hospital, medical clinic, clinical laboratory or healthcare establishment in the course of carrying out any investigation or performing any duty or function under this Act.". Further, section 13(2) of the PHMCA states that the Director and an authorised officer shall not disclose any information which is contained in the medical record, or which relates to the condition, treatment or diagnosis, of any person, as may have come to his knowledge in the course of carrying out any investigation or performing any duty or function under this Act" unless the disclosure was made under certain specific circumstances.

[73] The Sector-Specific Advisory Guidelines are: (1) Advisory Guidelines for the Telecommunication Sector; (2) Advisory Guidelines for the Real Estate Agency Sector; (3) Advisory Guidelines for the Education Sector; (4) Advisory Guidelines for the Healthcare Sector; (5) Advisory Guidelines for the Social Service Sector.

[74] The industry-led guidelines which have been published to date are: (1) Life Insurance Association Code of Practice for Life Insurers on the Singapore Personal Data Protection Act; and (2) Life Insurance Association Code of Conduct for Tied Agents of Life Insurers on the Singapore Personal Data Protection Act.

localisation argue that data localisation improves the security of data and encourages job creation via the establishment of domestic data centres, while opponents argue that data localisation reduces business competitiveness and data centres are costly to build.[75]

54. Data localisation requirements or restrictions on the free flow of personal data have been implemented in a number of jurisdictions in recent years.[76] It should be noted that specific data localisation requirements differ depending on the jurisdiction in question. While some of these countries such as Indonesia, Russia, China, and Nigeria impose a blanket ban on the transfer of all categories of individuals' data abroad, others, such as Australia,[77] impose specific restrictions on the transfer of data in specific sectors such as healthcare and finance on grounds of safeguarding individuals' sensitive data.

55. The PDPA does not impose any requirement for data localisation. However, there is a transfer limitation obligation under the PDPA. The transfer of personal data out of Singapore, can only be effected through recognised data transfer instruments or where it meets certain requirements to ensure that the transferred data will be provided a standard of protection that is comparable to that of the PDPA.[78] Businesses with offices in countries that impose data localisation requirements may find it difficult to combine data sets from different countries to perform data analytics as they are restricted from moving customers' personal data out of the source countries.

[75] H. Akim Unver, Grace Kim (June 2016). *Cross-Border Data Transfers and Data Localization*. EDAM Cyber Policy Paper Series 2016/3.

[76] Nigel Cory (1 May 2017). *Cross-Border Data Flows: Where are the Barriers, and What do they cost?* Information Technology & Innovation Foundation (ITIF); and Neha Mishra (2016). *Data localization laws in a digital world*. The Public Sphere.

[77] Albright Stonebridge Group (September 2015). *Data Localization: A Challenge to Global Commerce and the Free Flow of Information*, pp. 5.

[78] These requirements include contractual arrangements or binding corporate rules when transferring personal data out of Singapore, to ensure compliance with the PDPA. See Section 9.3 of *Personal Data Protection Regulations 2014*.

VI. DATA ANALYTICS, SHARING AND MONETISATION IN SINGPAPORE

KPMG's methodology

57. KPMG was commissioned by CCS to study how industry players are responding to advancements in the data environment, specifically with regards to the adoption of data analytics, data sharing and data monetisation.

58. Based on their potential to reap significant benefits from the adoption of data analytics, six sectors were identified for the study. These sectors represent varying levels of maturity in their adoption of data-related practices in Singapore. The sectors studied were – **digital media, finance, healthcare, consumer retail, land transport** and **logistics**. To ensure a cross section of businesses were studied, a mix of companies of varying sizes and maturity in their use of data analytics within each identified sector were selected. Aside from these six sectors, companies that provide supporting data analytics services were also interviewed – these include infrastructure providers, data analytics solutions providers and data aggregators.

59. Twenty-seven interviews were conducted from May to July 2017. The sectors, and the number of interviewed companies are set out in the table below.

Table 1. Overview of Industry Players

Digital Media	Finance	Healthcare	Consumer Retail	Transport	Logistics	General
2	6	3	4	3	4	5

60. During each interview, questions were asked on the following key themes were asked:[79]

a. The types of data collected and how they are used and stored;

b. The benefits of using data analytics;

c. The extent of data sharing;

d. How data is monetised;

e. The impediments to greater adoption of data analytics and data sharing; and

[79] The survey questionnaire can be found at Appendix A to: KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*.

f. Relevant regulations governing data collection and usage.

61. The stakeholder engagements were complemented with KPMG's in-house expertise and domain knowledge on data analytics in Singapore to derive key findings on the data analytics, sharing and monetisation practices of businesses.

62. The subsequent sub-sections outline the key findings from KPMG's study.

Data analytics

Overview of KPMG's findings

63. KPMG's study found that the maturity of adoption of data analytics varies across the six sectors, as well as between businesses within the same sector.

64. KPMG developed a maturity map which sets out the progression of data analytics capabilities through five stages of maturity, and assessed the data analytics capabilities of the six sectors in Figure 2 below. It is important to note that an organisation's progress can "skip" stages, and need not progress sequentially through the map. The five stages are:[80]

a. **Awareness** – where the organisation is only starting to become aware of data analytics. In this stage, there is no structured approach to data collection and analysis. Data is usually stored in silos and may lack quality and integrity.

b. **Experimental** – where the organisation is starting to commission and experiment with data analytics projects. In this stage, the approach to data collection and analytics is ad hoc, and used as and when the need arises.

c. **Cohesive** – where the organisation has proper data governance procedures in place and data analytics programmes are set up. In this stage, the organisation follows a structured approach to collecting data and performing data analytics, but has yet to use insights from its analysis to drive business decisions.

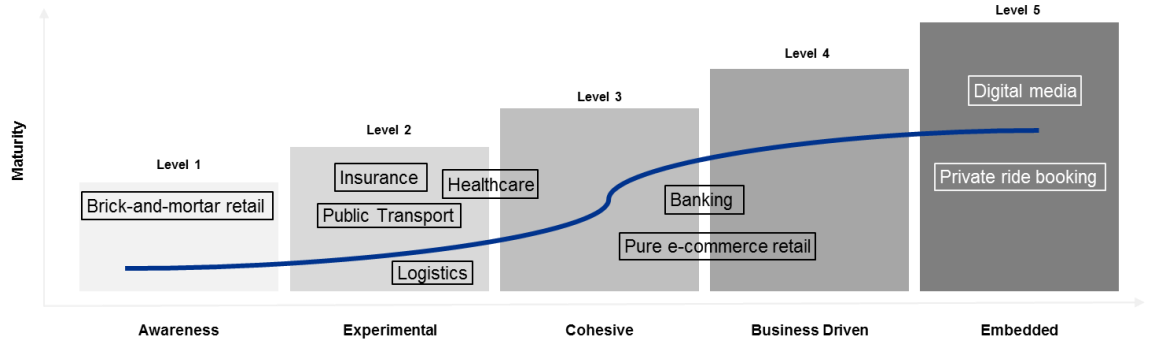
d. **Business driven** – where the organisation actively incorporates insights from its data analytics into its decision-making processes. At this stage, the organisation has integrated data collection and analysis across different business units, but enriched data is only being used by select users, such as the IT or data analytics departments.

[80] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 7, section 2.5.

e. **Embedded** – where the organisation not only actively uses data analytics in its business decisions, but opens up access to its data analytical functions to all business units and users.

65. Across sectors, the digital media sector and the ride booking companies are the most advanced, while many sectors are still within the awareness and experimental stages of the data analytics maturity map. At the conclusion of its study, KPMG assessed the maturity of each sector in the maturity map below:

Figure 2. Data Analytics Maturity Map in Singapore



66. It is important to note that the sector rankings are an overall representation of the businesses surveyed in that sector. Within any sector, there is a dispersion of data analytics capabilities between companies – in some cases, the disparity can be significant. It is also important to note that in designing the maturity map, KPMG drew a distinction between data analytics and BI.[81] As such, the maturity map set out in Figure 2 was premised on identifying the level of adoption of data analytics and the capabilities of businesses in that sector, as opposed to the usage of BI.

67. KPMG found that two key factors drive the use of data analytics and overall data capabilities in certain sectors:[82]

a. **Government initiatives** – the efforts of government agencies, such as LTA, MAS and IMDA, in supporting businesses' adoption of data analytics and facilitating data sharing in their respective sectors.

b. **Presence of international companies with very strong data analytic capabilities** – the presence of international companies such as the ride

[81] BI focuses on historical trend analysis and patterns. For example, BI is commonly used to generate insights on current business operations. In contrast, analytics is a forward-looking and predictive tool. See KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 7, section 2.4; See also, Justin Heinze (1 July 2016). *Business Intelligence vs. Business Analytics: What's the Difference?*

[82] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 59-60, section 9.1.

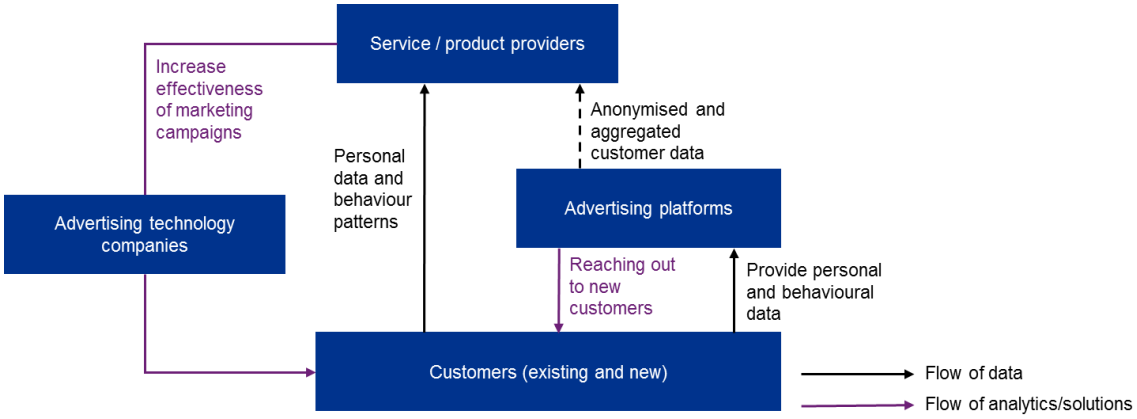
booking companies and pure e-commerce companies have disrupted business operations globally, and stimulated the development of data analytics capabilities in these sectors within Singapore.

68. Findings for each sector are discussed below.

(1) Digital Media Sector

69. The digital media sector is made up of online advertising platforms and other advertising technology companies. The digital media sector provides companies and organisations with a way to reach new customers, and facilitate the matching of demand (customers) and supply (businesses selling products and services) of advertisements.

Figure 3. Data Analytics Landscape in the Digital Media Sector



70. Online advertising platforms consist of search marketing platforms and social marketing platforms. These platforms actively collect customer data and use this data to build profiles and segments of customer bases. Data is generated from customer behaviour patterns on the internet (e.g. the websites they visit, the items they search for), and is usually provided voluntarily by customers.[83] The more data the online advertising platform collects on the individual consumer, the more complete the profile of that individual will be.

71. Examples of search marketing platforms include Google AdWords. Advertisements may appear on top of or below an organic search result after a user performs a search query, on the side of a search page, or on partner websites in the form of a banner. The objective of search marketing platforms is to make the most

[83] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 10, section 3.1.

relevant advertisements available to customers, so that the products advertised most closely match what the customers are searching for.[84]

72. Examples of social marketing platforms include Facebook and Twitter, which collect data on their users, that is then used to customise advertisements. A business can use the data from its existing customer base to complement the data available from the social marketing platforms, so that existing customers and other new customers who fit a similar profile (for example, based on location, age groups or gender) can receive targeted advertising messages.[85]

73. The digital media sector has also seen the emergence of advertising technology companies (otherwise known as "ad tech") which develop technologies that increase the effectiveness of marketing campaigns, and have contributed significantly to the use of data analytics in this sector. Examples of these innovative technologies include data management platforms,[86] customer retargeting technology,[87] cross-device advertising,[88] and demand-side platforms.[89]

(2) Finance Sector

74. The finance sector in this paper refers to the banking sector and the insurance sector. In Singapore, the finance sector is one of the leading users of data analytics,

---

[84] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 10, section 3.1.1.

[85] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 11-13, section 3.1.2.

[86] Data management platforms are centralised platforms that combines customer data from different sources to create more accurate customer profiles that increase the effectiveness of marketing efforts. Data management platforms are useful when advertisers have advertisements across multiple networks and media owners. They are also useful for media owners to understand where demand for advertisements is coming from, as well as the top sectors. See KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 13-14, section 3.2 and Box 2.

[87] Customer retargeting technology serves customers advertisements based on the products or services they recently browsed online. Facebook's Dynamic Ads is an example of such technology, although other companies are also able to provide such technology. See KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 13-14, section 3.2.

[88] Cross-device advertising is technology which allows a company to advertise its products to customers across devices. With this technology, companies can maintain consistency in their advertisements across all media such as tablets, phones, desktops. See KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 13-14, section 3.2.

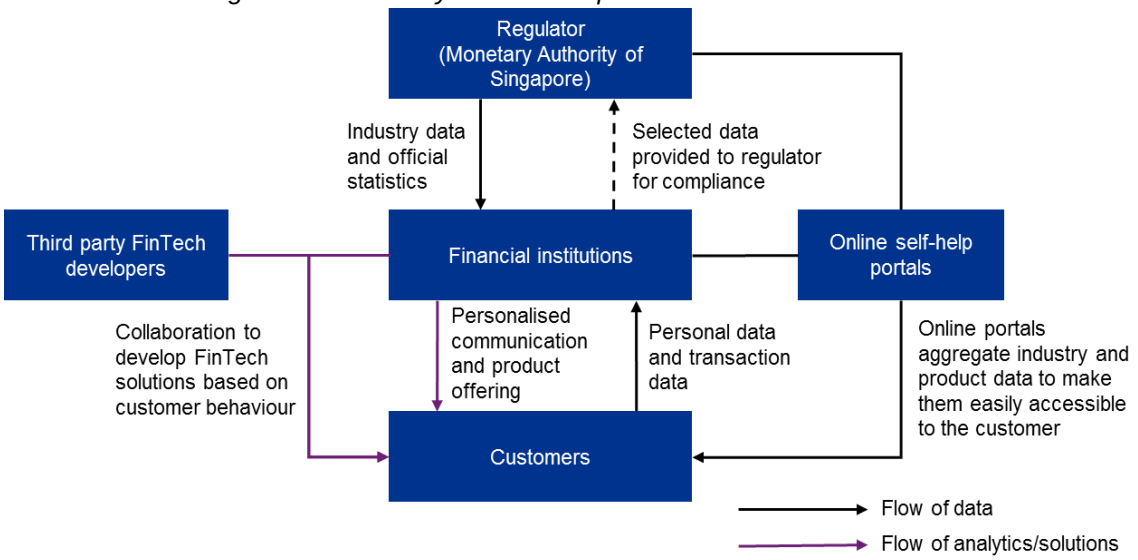
[89] Demand-side platforms help marketers manage and optimise their bids for advertisement space across platforms as advertisements and advertisement space are increasingly traded through ad exchanges daily. See KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 13-14, section 3.2.

with the banking sector generally more advanced than the insurance sector.[90] Financial institutions collect a myriad of customer information, including:

a. **Personal customer data** – This includes personal particulars, income levels, employment history, education background and even personal particulars of family members. This also refers to personal transactional data such as the setting up of a bank account, the purchase of a financial product, and all other monetary transactions.[91]

b. **Customer behaviour data** – With respect to the banking sector, this includes digital data, physical data and industry insights from external data providers.[92] With respect to the insurance sector, this includes customer lifestyle data, driving behaviour and digital data from online and self-help insurance providers. [93]

Figure 4. Data Analytics Landscape in the Finance Sector



75. In addition to the relatively more basic use of data analytics in improving customer experience and productivity, it is also being used in the finance sector to detect fraud, ensure system reliability and develop innovative products.

[90] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 17, section 4.
[91] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 18, section 4.1.1.
[92] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 18, section 4.1.2.
[93] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 19, section 4.1.3.

76. For instance, banks offer credit cards to customers with features that are catered to their preferences (e.g. dining features and promotions as banks pick up dining-out behaviour among customers). Banks also use data analytics to ensure that ATMs are sufficiently stocked with cash and that a list of "favourite transactions" is found on the home page of the ATM. This results in greater convenience for customers, and improves the customers' interaction with the bank.[94] Similarly, insurance companies use data analytics to create more value for the customers. For instance, insurance companies are starting to use sensors and wireless communication technologies in cars (i.e. telematics) to tailor insurance premiums based on individual driving patterns.[95]

77. In addition, banks have gone on to use data analytics to understand customer credit risks, and predict which customer might be more likely to default on his loan.[96] Data analytics is also used by banks to improve business operations, reduce staff turnover rates, and streamline customer authentication processes.[97] Further, banks use data analytics to detect fraud or money-laundering activities, to facilitate their compliance with the relevant rules and regulations.[98]

78. The use of data analytics in the finance sector is championed by MAS, which has set up its own Data Analytics Group ("DAG") to position itself and the sector for the digital economy of the future.[99] The DAG leads MAS' efforts to harness the power of data analytics to unlock insights, enhance the supervision of financial institutions, make regulatory compliance more efficient for financial institutions, and improve work efficiency across the organisation.

79. MAS also encourages innovation within the financial technology landscape ("FinTech") through the MAS FinTech Regulatory Sandbox, where promising innovations can be tested within a well-defined experimental space.[100] MAS provides regulatory support for businesses by relaxing some specific legal and regulatory requirements for the duration of the sandbox. The current active sandbox experiment is PolicyPal, a mobile app which allows users to track existing insurance policies and

---

[94] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 20, section 4.2.1.
[95] Kenneth Cheng (12 May 2016). *Car insurers turn to telematics to lower risks, deter fraud*. Today Online.
[96] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 21, section 4.2.2.
[97] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 21-22, section 4.2.3.
[98] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 22-23, section 4.2.4.
[99] Monetary Authority of Singapore (13 February 2017). *MAS Sets up Data Analytics Group*. Media Releases.
[100] Monetary Authority of Singapore. *MAS FinTech Regulatory Sandbox*.

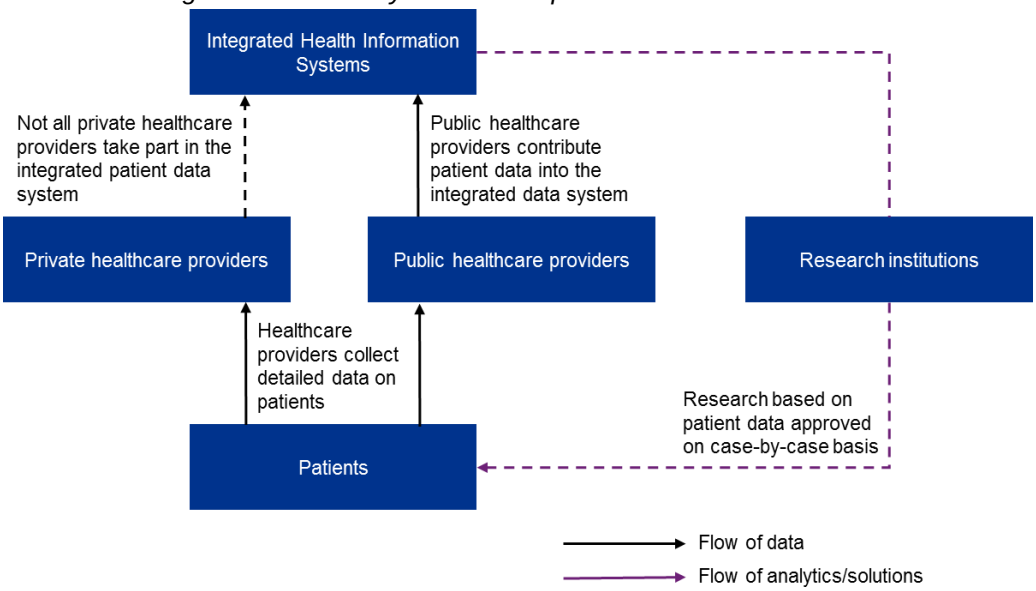
matches users to appropriate insurance policies offered by insurance companies. PolicyPal makes use of data analytics to match the insurance policies to the user, based on the user profile.[101]

80. The larger banks in Singapore have also set up similar sandboxes within their own organisations. An example of this is The FinLab, which is an accelerator programme focused on growing FinTech start-ups, set up by United Overseas Bank and Infocomm Investments Pte. Ltd.[102]

(3) Healthcare Sector

81. The key data analytics player in the healthcare industry is Integrated Health Information Systems ("IHiS") Pte. Ltd., which is a private entity wholly owned by Ministry of Health Holdings ("MOHH") Pte. Ltd.[103] Amongst other things, IHiS operates the National Electronic Health Records ("NEHR"), which is a patient data exchange system that enables healthcare professionals to view the medical records of patients across the national healthcare network. It collates patient information from all public healthcare institutions, as well as a growing number of private healthcare institutions.[104]

Figure 5. Data Analytics Landscape in the Healthcare Sector



[101] Roger Peverelli, Reggy de Feniks (24 April 2017). *PolicyPal: your digital insurance manager*. Digital Insurance Agenda.

[102] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 23-24, section 4.2.5 and Box 8; See also UOB (9 November 2015), *UOB and IIPL launch The FinLab to support the region's most innovative FinTech startups*. News Release.

[103] MOHH is the holding company of Singapore's public healthcare entities and acts as the strategic partner to the Ministry of Health, in ensuring the smooth implementation of healthcare policies across public healthcare institutions.

[104] Ministry of Health. *Institutions Participating in the National Electronic Health Records System (NEHR)*.

82. The NEHR is a rich source of patient information and includes information[105] such as:

a. Admission and visit history;

b. Hospital inpatient discharge summaries;

c. Laboratory and radiology results;

d. Medication history;

e. History of past operations;

f. Allergies and adverse drug reactions; and

g. Immunisations.

83. The NEHR operates on an implied consent model, in that a patient is deemed to have given his consent to share his data through the NEHR unless he opts out of the scheme.

84. IHiS has set up a coherent framework for collecting data, and has driven the use of data analytics among public healthcare providers.[106] Data analytics is used mainly to improve patient care as well as maximise the efficiency of how limited medical resources are allocated.

85. For instance, data analytics is used to optimise the limited supply of inpatient capacity. This can be done through remote monitoring of patients to identify a deterioration in health before a patient becomes critical or by deploying transitional care teams to provide non-emergency care to a patient at home.[107] Bed occupancy data is also used to identify trends in increased demand patterns so that beds can be more efficiently allocated across different wards or departments. Hospitals can also more accurately provide patients with an estimate of bed waiting times.[108]

---

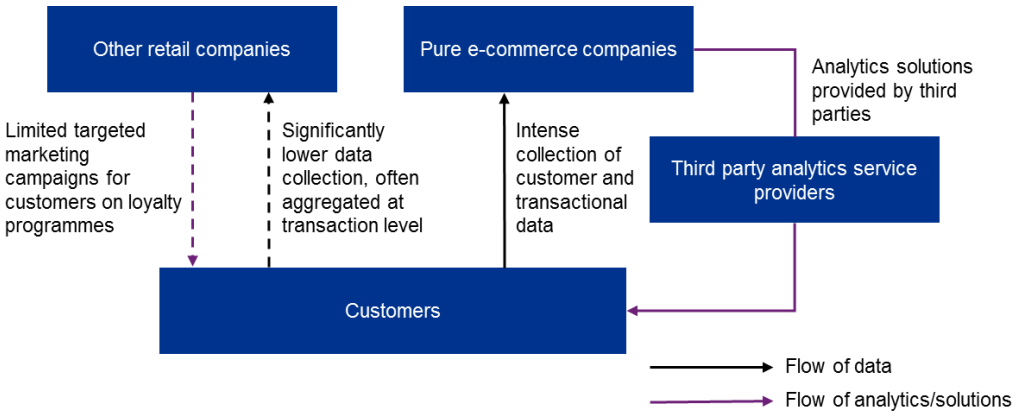
[105] Ministry of Health. *National Electronic Health Record (NEHR)*.
[106] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 30, section 5.2.
[107] KPMG (2016 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 30-31, section 5.2.1 and Box 9.
[108] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 30, section 5.2.1.

86. Additionally, patient care can be improved through the use of analytical models which predict a patient's likelihood of contracting a disease. Historical relationships between a patient's lifestyle and chance of disease, as well as indicators that tend to increase the chance of disease within the Singapore population are identified. People who possess these high-risk indicators are then actively engaged by the relevant healthcare providers to try and mitigate the risk of disease before it takes root.[109] There is also some usage of data analytics to predict the likelihood of disease from an individual's genetic makeup, although this research is at a very nascent stage.[110]

(4) Consumer Retail Sector

87. The consumer retail sector is broadly divided into two main segments – online retail and brick-and-mortar retail. Increasingly, the lines between the two are blurring, with online retail platforms expanding their business to physical stores, and brick-and-mortar shops hawking their goods on online retail platforms. Pure e-commerce platforms lead this sector in their usage of data analytics as compared to their brick-and-mortar counterparts.

Figure 6. Data Analytics Landscape in the Consumer Retail Sector



88. Pure e-commerce platforms collect a plethora of data from the daily operation of their desktop and mobile retail platforms. The two main types of data collected are:

a. **Customer data –** this pertains to data on customer activity, customer behaviour and transaction history.[111]

[109] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 32-33, section 5.2.2.
[110] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 33, section 5.2.3.
[111] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 37, section 6.1.1.

b. **Merchant data –** this pertains to data on a merchant's responsiveness, merchants' ability to fulfil orders and reviews of merchants by customers.[112]

89. The pure e-commerce retail platforms generally do not purchase customer or merchant data from external sources. The nature and specificity of the data to a company's operations necessitate internal data generation.[113] In turn, these retail platforms use data analytics to improve customer experience and their business operations.[114]

90. Data analytics is used to improve customer experience through some of the following means:[115]

a. With the data on the types of products a customer has recently viewed, the e-commerce retail platform can perform data analytics to predict the preferences and buying intent of a customer. The e-commerce retail platform can then start to recommend similar products to the customer.

b. With the data on the products that a customer has added to his cart but not checked out, the e-commerce retail platform can use dynamic advertising to prompt the customer to complete the transaction.

91. Data analytics is also used by e-commerce retail platforms which host third party sellers on their platforms to analyse customers' experience with third party sellers and improve business operations. Some examples include:[116]

a. Tracking of third party sellers sales revenue, and using data analytics to predict the top sellers to focus on; and

b. Tracking the ability of different third party sellers to meet demand and deliver goods, and using data analytics to predict when a seller might fail to meet orders.

---

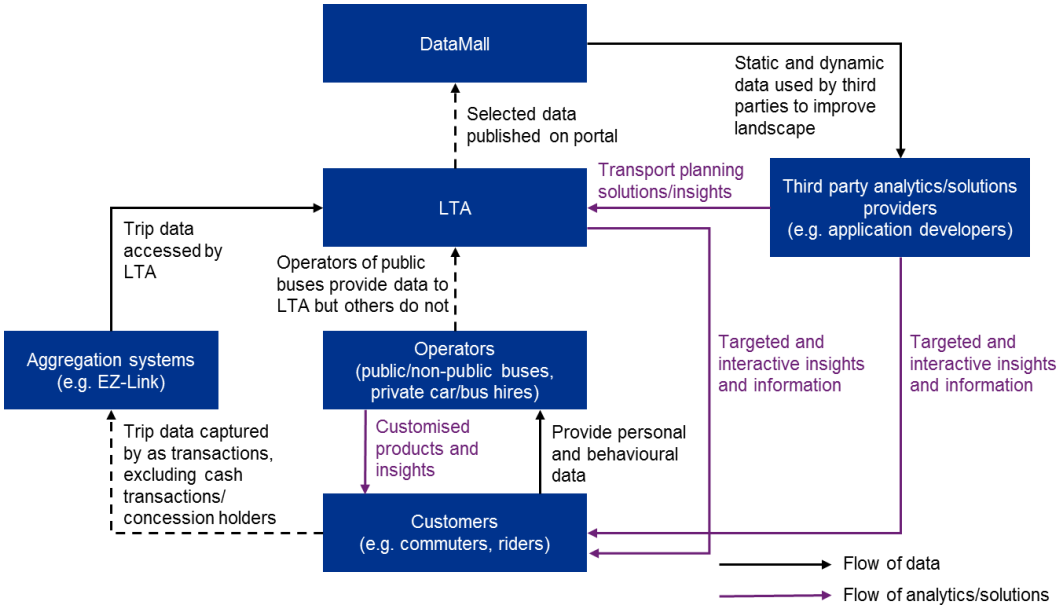
[112] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 37, section 6.1.1.
[113] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 37, section 6.1.1.
[114] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 38, section 6.2.
[115] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 38-39, section 6.2.1.
[116] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 40-41, section 6.2.2.

92. On the other hand, brick-and-mortar retailers collect a limited amount of data on customer behaviour and transactions. The data collected usually pertains to sales revenue data by product, transaction or store locations. However, this transaction data typically cannot identify individual customers, unless the customer is part of a loyalty programme.[117] Correspondingly, brick-and-mortar retailers currently make limited use of data analytics.[118] Indeed, targeted marketing campaigns can only be directed at customers who leave personal details with such retailers.[119]

(5) Land Transport Sector

93. The land transport sector is diverse; it ranges from ride booking companies (e.g. Uber, Grab) to public transport operators, and includes private bus hiring companies. Similarly, the data analytics capabilities of businesses range from very advanced to those that are just becoming aware. LTA drives the data analytics initiatives among public bus operators, and also facilitates data sharing in the sector. The sector is relatively self-contained, generating and using data internally.

Figure 7. Data Analytics Landscape in the Land Transport Sector



94. LTA obtains data from the aggregation systems and from the public transport operators it regulates. Data from its aggregation systems is able to map most commuter journeys reliably, as the systems track where each commuter gets on or off

[117] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 37, section 6.1.2.
[118] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 41-42, section 6.2.3.
[119] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 41-42, section 6.2.3.

a bus/MRT train. LTA has also put in place a Common Fleet Management System ("CFMS") to provide a unified solution for operations control, fleet management, passenger information, and business management between the various bus operators in Singapore.[120]

95. The CFMS enables bus operators to monitor the location and performance of their bus fleets in real-time. The CFMS also provides live updates on traffic accidents, expected arrival times, distances between buses, and passenger loads of the next bus. The bus operators have leveraged the data on the CFMS to perform data analytics to improve their business operations by optimising fleet resources and making adjustments to their bus operations in real-time.[121]

96. In addition, LTA is presently developing a Fusion Analytics for Public Transport Emergency Response ("FASTER") system which will combine data from various sources, including fare-card, video and telecommunication systems. The aim is to perform data analytics on this combined dataset to allow LTA and public transport operators to visualise commuting patterns to improve transport planning and trigger early alerts of crowd surges and transport incidents. The FASTER system will also be able to predict the impact of a transport incident in terms of extent of travel delay and number of commuters affected, so as to make recommendations on mitigating measures to alleviate the public transport crunch.[122] As part of LTA's Smart Mobility 2030 Master Plan, LTA is developing data visualisation techniques to easily observe travel patterns across bus routes and analyse the utilisation of bus services along different points of their routes. In this way, data analytics solutions are used to enhance the effectiveness of public transport planning policies.[123]

97. Third party application developers have also contributed to the adoption of data analytics within the public transport sector, by relying on data from DataMall to develop applications which predict the arrival times and passenger loads of buses. This way, passengers can get the information they require to better plan their journeys.[124]

---

[120] Land Transport Authority (9 April 2014). *Intelligent Bus Management System to Enhance Commuters' Journey Experience*. News Releases; and Land Transport Authority (8 December 2016). *Factsheet: Passenger Information Display System (PIDS) Trial to Offer Real-Time Travel Information to Commuters on Buses*. News Releases.

[121] Land Transport Authority (8 March 2017). *Factsheet: Leveraging Technology for a Smarter and Greener Transport System*. News Releases; and KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 47, section 7.4.1.

[122] Land Transport Authority (8 March 2017). *Factsheet: Leveraging Technology for a Smarter and Greener Transport System*. News Releases.

[123] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 48-49, section 7.4.2.

[124] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 49-50, section 7.4.3.

98. Data is also collected by ride booking and private bus hire companies. For example, ride booking companies such as Grab and Uber collect customer personal data when customers sign up for their services. Customer transactional data is also collected when customers make use of their applications to book trips. Transactional data includes travel patterns, travel times, pick-up locations and trip destinations.[125] The ride booking companies make use of advanced analytics to perform real-time demand and supply matching, as well as to predict driver behaviour and personalise the types of notifications received by a driver.[126]

99. With respect to private bus hire services, a limited data set is collected from business operations and customers. The data sets collected by private bus hire services include bus location data, trip timings and capacity data.[127] Currently, there is a low adoption of data analytics within the private bus hire sector. However, this may be set to change with the advent of initiatives such as Beeline's mobile application, through which commuters can indicate their preferred commuting routes and book seats on available bus routes.[128] Bus operators can then respond to these by providing shuttle bus services, with new routes being activated based on demand and existing routes evolving over time.[129]

(6) Logistics Sector

100. The logistics sector has been slower in the adoption of data analytics in its business operations.[130] The rise of e-commerce retailers has generated demand for delivery services, and has correspondingly stimulated the use of data analytics within the logistics sector to provide better services and shorten lead time.[131] Nevertheless, due to Singapore's small geographical size and dense road network, businesses using traditional business models have not felt compelled to evolve.[132]

---

[125] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 45, section 7.1.2.

[126] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 50, section 7.4.4.

[127] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 45-46, section 7.1.3.

[128] Beeline is an initiative by LTA and GovTech which is described as an "experimental demand-driven, shared micro-transit concept enabled by data analytics and mobile technology." For more information, see GovTech, *Initiatives – Beeline*.

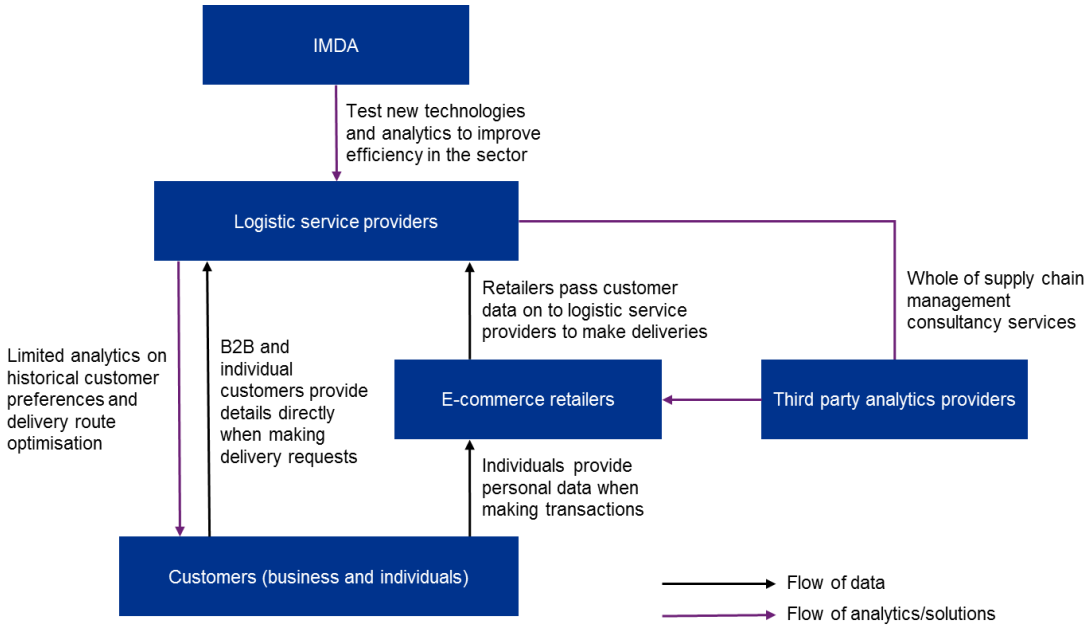
[129] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 46, section 7.1.4; and GovTech, *Initiatives – Beeline*.

[130] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 52, section 8.

[131] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 52, 54, sections 8 and 8.2.

[132] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 52, section 8; and World Economic Forum (January 2016). *Digital Transformation of Industries – Logistics Industry*.

Figure 8. Data Analytics Landscape in the Logistics Sector



101. Logistic service providers collect customer data[133] and shipment data[134] when they perform deliveries. Logistic service providers are increasingly adopting data and analytics to improve their business operations, albeit on a limited scale by a handful of market players.[135] Examples of some of the uses of data analytics include:[136]

a. Collaboration with pure e-commerce retailers to predict customer demand and deploy stock pre-emptively to a nearby location to reduce delivery lead times;

b. Usage of in-vehicle sensors for monitoring delivery vehicles in real-time and the analysis of driving patterns for safety purposes, as well as for the reduction of insurance premiums on vehicles; and

[133] Customer data includes parcel origin, sender personal details, recipient address, delivery method and option (e.g. express, standard) and special delivery instructions. See KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 53, section 8.1.1.

[134] Shipment data includes data on shipment routes, particularly the costs and delivery times of each permutation of shipment route. See KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 53, section 8.1.2.

[135] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 55-56, section 8.2.2.

[136] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 55-56, section 8.2.2.

c. Mini-routes are identified within longer delivery routes, and data analytics is used to provide better estimates of delivery times to customers and to reduce the chances of failed deliveries arising from customers not being at home.

102. There is potential for an innovative firm to fill the gap in the market by using advanced predictive analytics to optimise delivery schedules and supply chains, and to better manage delivery fleets.[137] There is also the potential for logistic companies to use data analytics to forecast demand for delivery services, particularly for B2B logistic service providers. Predictive insights can be derived from transactional patterns to forecast demand, such that resources can be allocated more efficiently. Predictive analytics can also result in benefits for consumers, as they may be able to reduce delivery costs by allowing consumers to avoid paying for last-minute delivery rates and also avoid errors arising from rushed delivery orders.[138]

103. To boost productivity and streamline supply chains through the use of technology and data analytics within this sector, IMDA has unveiled an Urban Logistics Technology Roadmap for 2020 on the usage of technology to improve operation processes and optimise resources in the logistics sector. In October 2015, the Government announced the allocation of S$20 million to the transformation of domestic logistics, and the roadmap was drafted to test how different stages of the logistics process can benefit from technology. The solutions, systems, and processes developed under the roadmap are required to be interoperable and open to industry players to adopt or adapt. This is to ensure that a level playing field is set for small and medium enterprises in the logistics sector.[139]

104. One example of inefficiency in the logistics supply chain is multiple trucks making deliveries, all with less than full loads. Multiple logistics service providers make deliveries to the same destinations, with no knowledge of each other's deliveries, or ways to share resources and combine deliveries. In such instances, assets are inefficiently used. IMDA has launched the Offsite Consolidation Centre, which is an initiative that seeks to improve truck load utilisation. Technologies such as cloud-based dock scheduling solutions, queue management systems, and change of custody systems, can be similarly deployed to enable efficient goods delivery.

[137] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 55-56, section 8.2.2.
[138] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 57, section 8.2.3.
[139] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 54-55, section 8.2.1.

Advanced robotics can also be deployed to help with sorting cargo, while fleet optimisation solutions can enable smooth, tracked, and optimised deliveries.[140]

Summary of benefits of data analytics

105. Based on the review of the six sectors, it is apparent that the adoption of data analytics and sharing of data by businesses can bring about a wide range of benefits across all sectors. These benefits can be summarised as follows:

a. **Internal benefits** which broadly refer to benefits to the company arising from the streamlining and improvement of business operations, the increased ability to comply with rules and regulations, and higher revenue from improved product offerings.

b. **External benefits** which broadly refer to benefits to the industry and consumers at large through the creation of new or improved products, the generation of predictive trend analysis to benefit the entire industry, and the implementation of effective public policies.

106. Consumers also benefit when businesses adopt data analytics. For example, products offered to them can be more customised to their preferences thus reducing their search costs. Businesses may also offer more innovative offerings to meet unfulfilled needs.

Impediments to the greater adoption of data analytics

107. Given the benefits that data analytics brings about, it is surprising that certain industries and companies are slow to adopt data analytics practices in their business operations. During the interviews, companies were asked about the impediments or challenges they faced. Several impediments highlighted by the interviewees are common across all sectors, while a number of challenges raised are sector-specific.

Common impediments across all sectors

108. One key impediment faced by companies across all sectors is manpower constraints. In particular, companies find that there is a lack of skilled talent within the middle management level with ten to twelve years of data analytics experience. Whilst companies have noted that local universities and educational institutions have rolled out programmes specialising in data analytics, the available skilled manpower in

[140] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 54-55, section 8.2.1; See generally, Annex A and Annex B of Infocomm Media Development Authority Singapore (1 December 2016) *Launch of Urban Logistics Technology Roadmap, 12 Additional Malls to Benefit from Tech-Enabled Process Re-Engineering*. Media Releases.

Singapore is at the relatively junior level. Industry players that are lagging behind in their adoption of data analytics find it particularly difficult to attract the relevant talent or find it too expensive to hire consultants to interpret and analyse their data.

109. Companies have also cited the high infrastructure costs to build up the relevant data storage and data analytics capabilities to be a hurdle. With respect to data storage, many interviewees have identified cloud storage as the way forward.[141] However, as noted above in paragraph 39, companies are reluctant to host all of their data with cloud storage providers for fear of over-reliance on a single cloud storage provider and loss of control over confidential data in the event of a security breach. Companies which eschew cloud storage providers would have to invest in private cloud storage or other data storage facilities. Companies could find it challenging to afford these infrastructure investments or to see the immediate value in such investments.[142]

110. Companies have also indicated that there are gaps in the datasets available to them. This could be due to late adoption of data analytics, such that companies have yet to collate a critical mass of data to draw any meaningful insights. This could be exacerbated by the fact that data is not presently collected in a form which can be recorded, processed and used easily. For instance, customer data collected by insurance companies is often not recorded in a central database. Data which is required for the ongoing management of policies is recorded, but other personal data on customer application forms is scanned and stored.[143] Further, without data sharing within the industry, insights that can be drawn out will be limited to a company's own data.

Sector-specific impediments

111. The finance sector is subject to additional regulatory safeguards with respect to data protection under the Banking Act. The KPMG study found that financial institutions have taken a conservative approach towards the interpretation of these requirements as they are unclear on the extent of data protection requirements they are subject to. This, in turn, affects the sharing and utilisation of data both within and outside of the company, which limits the adoption of data analytics by their employees.

112. As for the healthcare sector, there is still a sizeable segment of private healthcare providers which do not participate in the NEHR scheme. The advancement of data analytics within the healthcare sector will benefit from the broader participation

[141] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 5 and 60, sections 2.1.5 and 9.3.
[142] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 57 and 60, sections 8.6 and 9.4.
[143] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 18, section 4.1.1.

of the private healthcare sector and the consolidation of a more complete set of medical records. However, patient confidentiality concerns may form strong countervailing concerns against such participation. For instance, private clinics which treat sexually transmitted diseases may be reluctant to participate in the NEHR scheme as their patients prefer anonymity.

Data sharing

113. The KPMG study found that apart from data sharing which occurs as a result of the active facilitation by government agencies, the sharing of data within or across industries generally occurs to a very limited extent.

114. KPMG found that in sectors where data sharing takes place, the data that is shared usually involves industry or product data (as opposed to customer data), and such activities are usually spearheaded by government agencies. In the finance sector for example, MAS provides real-time industry data sets (on interest rates, exchange rates etc.) to industry players through making Application Programming Interfaces ("APIs") available. Some banks have also, in the same spirit, developed their own APIs (e.g. OCBC's Connect2OCBC) to make information on their products and services more accessible to external parties, enabling such information to be more easily integrated into third party applications.[144] Another example would be the land transport sector, where LTA makes static and dynamic industry transport data sets available to the general public through DataMall.[145] The sharing of dynamic data, such as real-time bus location data, has since spawned many third party applications and solutions (e.g. Bus Uncle, SG Buses), which has helped make public transport more accessible to the general public.[146]

115. KPMG found that there is very limited data sharing activity occurring amongst businesses, whether within or across industries. This is despite the fact that some companies do recognise the potential gains that may result from data sharing. Several reasons have been cited by industry players.

116. First, businesses informed KPMG that they do not share data externally due to the need to comply with the relevant data protection regulations. For example, due to the banking secrecy provisions under the Banking Act, banks do not share customer

[144] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 24-25, section 4.3.1.
[145] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 46, section 7.2.
[146] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 49-50, section 7.4.3.

data with others;[147] indeed, there even appears to be some wariness in sharing such data within the organisation. In the insurance sector, KPMG found that customer risk profiles and histories are also not shared between insurance companies for life insurance products. Insurance companies shared that the net benefit to customers from sharing of such data is ambiguous, and there is a concern of making some customers "un-insurable".[148] In the healthcare sector, while sensitive patient data is collected through the NEHR system, access to this information is guarded strictly and only doctors and healthcare providers who are directly involved in the patient's care have access to it.[149]

117. Second, companies also shared that they do not share data, as they view it as a source of competitive advantage. In the digital media and online retail sectors in particular, customer data relating to purchasing behaviour and customer preferences has provided useful insights for more targeted advertising, in turn leading to increased revenue streams.[150] As such, companies view the sharing of such data as a potential loss of revenue to competitors, and are consequently, reluctant to share it. The KPMG study also suggests that businesses may also be concerned that their revenue would be adversely affected by a loss in trust, if customers find out that their information is shared without consent.

118. Notwithstanding the foregoing reasons, it is surmised that a more vibrant data sharing environment (within or across industries) would enable companies to unlock greater value from their respective data sets and derive additional insights, so long as it is done within the confines of the relevant regulatory safeguards. For example, the consolidation of consumer behaviour data from a supermarket chain, with credit card data from a bank, can assist both businesses to better understand consumers' purchasing habits and demand patterns. With the benefit of data analytics, more accurate predictive insights may then be derived to assist the supermarket chain in planning the location of its next outlet, or aid the bank in achieving greater customisation in its promotions and advertising messages for its credit cards.

Data monetisation

[147] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 25, section 4.3.2.
[148] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 25, section 4.3.3.
[149] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 34, section 5.3.
[150] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 15 and 42, sections 3.3 and 6.3.

119. Apart from data aggregators and data brokers which directly monetise data by selling the data they compile (and insights derived from it) to third parties,[151] the KPMG study found that the direct monetisation of independently collected data (i.e. selling of these data sets) does not take place in the six sectors surveyed. Government agencies also do not monetise data directly; rather, data is typically shared free-of-charge to benefit society at large.[152]

120. What emerges from the KPMG study, however, is that businesses indirectly monetise the data they collect. Such indirect means include the use of data to achieve more targeted advertising through data insights, which ultimately leads to more advertising revenue for businesses. This is seen most clearly in the digital media,[153] finance[154] and consumer retail sectors,[155] where insights from data collected not only allow businesses to achieve more personalised products and solutions for customers, but also increase the effectiveness of marketing campaigns and conversion rates through more targeted marketing, thereby increasing customer demand and advertising revenue streams. Companies in the consumer retail sector even indicated that the value derived from such indirect monetisation probably far exceeds the value that any direct monetisation can bring.

[151] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 5-6, section 2.1.6.
[152] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 51 and 60, sections 7.5.1 and 9.2.
[153] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 15-16, section 3.4.
[154] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 26, section 4.4.
[155] KPMG (16 August 2017). *"Understanding the Data and Analytics Landscape in Singapore"*, pp. 42, section 6.5.

VII. IMPLICATIONS ON COMPETITION POLICY AND LAW

121. As discussed above in Section VI, the benefits arising from the adoption of data analytics and data sharing are manifold. However, these benefits may not be fully realised if businesses engage in anti-competitive conduct in the course of adopting data analytics and/or data sharing. It is thus crucial for competition policy and law to foster a level playing field for businesses in the data economy.

122. Enacted in 2004, the Competition Act (Cap. 50B) ("the Competition Act") aims to promote the efficient functioning of our markets and enhance the competitiveness of the Singapore economy, by providing a generic law to protect businesses and consumers from anti-competitive conduct. The Competition Act is administered and enforced by CCS.

123. The Competition Act prohibits specified activities which adversely affect competition within a market in Singapore, including:

a. agreements and/or concerted practices that prevent, restrict or distort competition ("section 34 prohibition");

b. abuse of a dominant position ("section 47 prohibition"); and

c. mergers that substantially lessen competition ("section 54 prohibition").

124. This section will first discuss the factors which CCS will generally consider when defining the relevant market. It will then discuss how business practices, in the context of data-driven industries, may be assessed to ascertain their compliance with the Competition Act.

Defining the relevant market

125. Market definition, normally the first step in any competition assessment, is relevant for all three prohibitions under the Competition Act, but it is especially pertinent for the prohibition on an abuse of a dominant position.

126. The purpose of defining the relevant market is to identify all the products that buyers regard as reasonable substitutes for the product in question (i.e. focal product) and all the sellers of those products. These are the competitors that actually constrain the exercise of market power.[156] The hypothetical monopolist test, or the small but significant, non-transitory increase in price test ("SSNIP test") is usually used in defining markets. The test starts with a narrow definition of the product and geographic market, which would be the focal product or the area in which the focal product is sold.

[156] *CCS Guidelines on Market Definition*, para 2.2.

It follows with the question of whether a significant number of buyers will switch to other products (or areas) that are the next best substitutes if the price of the focal product is raised by a small but significant, non-transitory amount above competitive levels. If the answer is yes, these other products (or areas) should be included in the definition of the market because these other products potentially constrain the exercise of market power. The group of products (or areas) is widened to include those products (or areas) and their sellers and the question is asked again until the point is reached where a significant number of buyers do not respond to the price increase. This then forms the relevant market that contains the principal constraints on the exercise of market power.[157]

127. Many data-driven industries are characterised by multi-sided platforms, where players may be vertically integrated. Defining the relevant market in such markets therefore may have additional complexities due to the multiple roles played by the players in the market.[158] For example, an e-commerce company may provide platform services, sell directly on its own platform (and thereby compete with third party sellers), and may also provide logistics services. Players serving different roles may also collaborate with each other.[159] For example, an e-commerce retailer may partner with a logistics service provider instead of acquiring it.

128. When defining the relevant market for multi-sided platforms, it is important not to ignore or neglect the interactions between different customer groups and the resulting network effects. Where there are interactions between the various customer groups from different sides of the platforms, it may be appropriate to define a single relevant market.[160] In such a case, the relevant price is the sum of charges to the various customer groups. The analysis should be undertaken under the assumption that the hypothetical monopolist would optimally adjust the balance of prices, and it should consider feedback effects from each side of the platform.[161]

129. There often are cases where such multi-sided platforms engage in multiple non-monetary transactions in exchange for data.[162] Accordingly, it may be difficult to use

---

[157] *CCS Guidelines on Market Definition*, para 2.6-2.7.

[158] Organisation for Economic Co-operation and Development (27 October 2016). *Big Data: Bringing Competition Policy to the Digital Era*. DAP/COMP(2016)14, pp. 15, para 45.

[159] Organisation for Economic Co-operation and Development (27 October 2016). *Big Data: Bringing Competition Policy to the Digital Era*. DAP/COMP(2016)14, pp. 15, para 45.

[160] By contrast, in the case where customer groups on each side do not interact with each other, it may be appropriate to identify two separate, but inter-related markets.

[161] Filistrucchi L, Gerardin D, van Damme E and Affeldt P (16 March 2013). *Market Definition in Two-Sided Markets: Theory and Practice*. TILEC Discussion Paper No. 2013-009; Tilburg Law School Research Paper No. 09/2013.

[162] Organisation for Economic Co-operation and Development (27 October 2016). *Big Data: Bringing Competition Policy to the Digital Era*. DAP/COMP(2016)14, pp. 15, para 46.

the traditional SSNIP test, which is dependent on the price mechanism[163] to define the relevant market(s). In such cases, the SSNIP test may have to be adapted to consider not only the monetary transactions, but also the non-monetary ones by identifying the data flow through the different markets (such as users of online search services and advertisers) to determine the relevant markets.[164]

130. In addition, where firms are offering "free services",[165] they may nonetheless be competing on aspects other than price.[166] In such instances, a quantitative assessment of quality may have to be adopted instead.[167] Quality which consumers value while using such "free services" may include level of privacy or ease of use and a quantitative assessment of such qualities may be taken into consideration for easier identification of the relevant market. The methodology adopted will depend on the quality being assessed at that point in time.

Anti-competitive conduct in relation to data

131. In recent years, the impact of the proliferation of data and use of data analytics on competition has gained the attention of governments and competition authorities in many countries, including those in Europe (e.g. Germany and France (joint study),[168] United Kingdom[169] and Netherlands[170]) and Japan.[171] The Organisation for Economic Co-operation and Development ("OECD") has also led several discussions and conducted research in this area.[172]

132. Having regard to the three prohibitions under the Competition Act, the following paragraphs summarise the current views on anti-competitive conduct that can arise in the context of data and the challenges for competition authorities:

a. Anti-competitive agreements and concerted practices facilitated by (i) data sharing, or (ii) algorithms;

---

[163] Organisation for Economic Co-operation and Development (27 October 2016). *Big Data: Bringing Competition Policy to the Digital Era*. DAP/COMP(2016)14, pp. 15, para 47.
[164] Organisation for Economic Co-operation and Development (27 October 2016). *Big Data: Bringing Competition Policy to the Digital Era*. DAP/COMP(2016)14, pp. 15, para 46.
[165] Examples of such "free services" include social media services, email services and even matchmaking services.
[166] Autorité de la Concurrence and Bundeskartellamt (10 May 2016). *Competition Law and Data*, pp. 27
[167] A "small but significant non-transitory decrease in quality" test may be used in industries where quality measures are well-accepted and quantifiable.
[168] Autorité de la Concurrence & Bundeskartellamt (10 May 2016). *Competition Law and Data*.
[169] Competition & Markets Authority (June 2015). *The commercial use of consumer data*.
[170] Harry van Til, Nicolai van Gorp, Katelyn Price (13 June 2017). *Big Data and competition*, ECORYS, prepared for the Ministry of Economic Affairs, Netherlands.
[171] Japan fair Trade Commission (6 June 2017). *Report of Study Group on Data and Competition Policy*.
[172] See generally, Organisation for Economic Co-operation and Development (27 October 2016). *Big Data: Bringing Competition Policy to the Digital Era*. DAP/COMP(2016)14.

b. Abuse of dominance – exclusionary conduct, including refusal to supply; and

c. Mergers between and acquisitions of firms engaged in data collection and data analytics which substantially lessen competition.

(a) (i) Anti-competitive agreements and concerted practices facilitated by data sharing

133. This paper has already examined how data sharing may enhance the value of an existing data set in paragraph 118 above.

134. In the normal course of business, businesses exchange information on a variety of matters legitimately with no risk to the competitive process. Indeed, competition may be enhanced by the sharing of information (e.g. on new technologies or market opportunities), particularly where consumers are also informed.

135. In general, it is unlikely that the competitive process will be harmed when the data that is shared is:

a. historical;

b. sufficiently aggregated and cannot be attributed to a particular business;

c. not sensitive, strategic or confidential; and

d. shared with consumers or government agencies.[173]

136. However, in certain circumstances, the sharing of data may have as its object or effect the appreciable prevention, restriction or distortion of competition within Singapore and be caught under the section 34 prohibition.[174]

137. In Singapore, section 34 of the Competition Act prohibits any agreements between undertakings,[175] decisions by associations of undertakings or concerted practices which have as their object or effect the prevention, restriction or distortion of

[173] *CCS Guidelines on the Section 34 Prohibition 2016*, paras 3.17 - 3.24.
[174] *CCS Guidelines on the Section 34 Prohibition 2016*, para 1.1.
[175] Undertaking means any person, being an individual, a body corporate, and an unincorporated body of persons or any other entity, capable of carrying on commercial or economic activities relating to goods or services. The key consideration in assessing whether an entity is an undertaking for the application of the section 34 prohibition is whether it is capable of engaging, or is engaged, in commercial or economic activity. *CCS Guidelines on the Section 34 Prohibition 2016*, para 2.5 - 2.6.

competition within Singapore. “Agreement” has a wide meaning and includes both legally enforceable and non-enforceable agreements, whether written or oral (including so-called “gentlemen’s agreements”) – what is required is that parties arrive at a consensus on the actions each party will, or will not, take (the so-called “meeting of the minds”).[176] In a related vein, “concerted practices” refers to any informal co-operation without any formal agreement or decision. It may be found to exist if parties, even if they did not enter into an agreement, knowingly substituted the risks of competition with practical co-operation between them.[177]

138. In relation to data sharing, the section 34 prohibition therefore strictly precludes any direct or indirect contact between parties where the object or effect is either to influence the conduct on the market of an actual or potential competitor, or to disclose to such a competitor the course of conduct which they themselves have decided to adopt or contemplate adopting on the market.[178] What is clear, is that each party must determine independently the policy which it intends to adopt in the market, and has the right to adapt intelligently to the existing and anticipated conduct of its competitors.[179]

139. Care should be taken when the sharing of data would allow a business to have access to or draw inferences from a competitor’s commercially sensitive information, such as pricing or production figures. This is because the knowledge of such data is deemed to reduce uncertainty over future behaviour of the competitor, raising the presumption that the business’s commercial policies on the market will no longer be independently determined but instead, determined with knowledge of the data shared. The fact that the data could have been obtained from other sources is not necessarily relevant.

140. In general, an appreciable adverse effect on competition is more likely where there exists:

a. only a few companies operating in the market;

b. data sharing is frequent;

c. data shared is commercially sensitive, strategic and confidential; and

---

[176] *CCS Guidelines on the Section 34 Prohibition 2016*, para 2.10.

[177] *CCS Guidelines on the Section 34 Prohibition 2016*, para 2.18.; See also Case C-8/08 *T-Mobile Netherlands BV v Raad van bestuur van de Nederlandse Mededingingsautoriteit* [2009] ECR I-4592, para 26 and the cases cited therein.

[178] Cases 40/73 etc., *Suiker Unie v Commission* [1975] ECR 1663, para 174.

[179] Cases 40/73 etc., *Suiker Unie v Commission* [1975] ECR 1663, para 173-174.

d. data shared is limited to certain participating companies in the market to the exclusion of their competitors and buyers,[180]

unless the sharing of data can result in net economic benefits.[181]

141. In general, data sharing can be categorised as the sharing of price-related data and non-price related data.

Sharing of price related data

142. **The sharing of price related data can lead to price co-ordination and therefore diminish competition, which would otherwise be present between businesses.** This will be the case whether the data shared relates directly to current prices or future prices to be charged or to the elements of a pricing policy, for example, discounts, costs, terms of trade and rates, and dates of change. Price announcements made in advance to competitors may be anti-competitive where they facilitate collusion. In the *Ferry Operators* case, CCS found that the communication between two ferry operators in providing commercially sensitive and confidential price information regarding ferry tickets sold to corporate clients and travel agents for routes from Singapore,[182] had the object of restricting competition. Over the period of the infringing conduct, the routes were served by only these two ferry operators. In such a concentrated market, the sharing and provision of sensitive and confidential price information is particularly restrictive of competition because where one ferry operator makes a disclosure of a quoted price, the other would be the only other competitor which can provide an alternative price to the potential customer. [183] The circulation of historical price data however, is unlikely to have an adverse effect on competition.

---

[180] *CCS Guidelines on the Section 34 Prohibition 2016*, para 3.20 and para 2.22.

[181] *CCS Guidelines on the Section 34 Prohibition 2016*, para 4.1. The Net Economic Benefit exclusion may be applicable to agreements including the sharing of data. An agreement that brings about nets economic benefits can be excluded from Section 34 of the Act where such agreements contributes to:

a. improving production or distribution; or
b. promoting technical or economic progress,

but which does not:

a. impose on the undertakings concerned restrictions which are not indispensable to the attainment of those objectives; or
b. afford the undertakings concerned the possibility of eliminating competition in respect of a substantial part of the goods and services in question.

[182] The two routes are Singapore (Harbourfront) – Sekupang, and Singapore (Harbourfront) – Batam Centre.

[183] CCS 500/006/09 ID. *Infringement of the Section 34 Prohibition in relation to the price of ferry tickets between Singapore and Batam*. 18 July 2012, para 163.

Sharing of non-price related data

143. **The sharing of non-price related data may prevent, restrict or distort competition within Singapore depending on the type of data shared and the structure of the market to which it relates**. For example, the sharing of excess capacity figures of a firm's factories may allow competitors to infer if they are likely to face strong competition when submitting a bid for new projects, thus affect the bids submitted. The sharing of non-price related data among businesses operating in different markets on the other hand, is unlikely to have an appreciable adverse effect on competition in a market, since they do not compete in the same market.

144. In general, the sharing of data on output and sales should not affect competition so long as it is sufficiently historical and aggregated. In such circumstances, it is unlikely that an agreement to share such data would reduce or remove the uncertainties inherent in the process of competition.

Data sharing with different stakeholders

145. In addition to the type of data shared, another dimension of data sharing relates to the stakeholders involved in the sharing. As set out in paragraph 26, businesses may choose to share their data with consumers, government, businesses from other industries and competitors etc. Often, in these circumstances whether competition issues arise from data sharing is dependent on the stakeholders involved:

a. Data Sharing By Businesses with Consumers. As a general principle, the more informed consumers are, the more effective competition is likely to be. As such, **businesses making their data publicly available to consumers is generally unlikely to harm competition**. In fact, such behaviour is likely to be pro-competitive as it allows consumers to make informed decisions. For example, the release of details of mobile plan packages and prices by telecommunication companies allows consumers to compare and select the optimal mobile plan, thus promoting effective competition.

b. Data Sharing By Businesses with Government. Government agencies rely on data analytics in the formulation of new policies (refer to paragraph 29). When businesses make their data available to government agencies either voluntarily or to comply with applicable regulations and licencing conditions, **Government agencies are able to conduct data analytics on a wider and richer dataset and thus able to make more informed policy decisions, to the benefit of society.** For example, the reporting of unusual increase in gastroenteritis cases by general practitioners helped MOH and

other relevant government agencies to analyse, pinpoint the possible virus sources, and contain the spreading of the virus.[184]

c. Data Sharing By Businesses with Businesses from another market or industry**. Competition concerns are generally unlikely to arise when businesses share data with other businesses in a different market or industry**, including data analytics solutions providers and data aggregator firms. For example, the sharing of aggregated consumer profiles and spending patterns by credit card companies may help other businesses to generate better insights, conduct targeted marketing and offer more customised product to consumers. **However, data sharing by businesses with other businesses from another market or industry, which has the object or effect to prevent, restrict or distort the competitive process in a specific market or industry would still be caught under section 34 of the Competition Act.** For example, "hub-and-spoke" cartels where competitors come together to share sensitive data via a third party (in another market or industry) that facilitates collusion amongst competitors would be caught under the Competition Act. Another example which would be caught under the Competition Act would be businesses in different markets coming together to share data for the purpose of jointly boycotting a particular common customer or supplier.

d. Data Sharing By Businesses with Competitors. As highlighted above, **the sharing of commercially sensitive data such as pricing or production capacity with competitors, is likely to infringe section 34 of the Competition Act.** This is because such data sharing is likely to prevent, restrict or distort competition which would otherwise be present between businesses. **However, there are scenarios where such sharing may have net economic benefits and be excluded under the Competition Act**.[185] In the EU, the European Commission's ("EC") Insurance Block Exemption Regulation ("IBER"), which was in place for 25 years till 31 March 2017,[186] exempted (i) the exchange and/or aggregation of data in statistics and studies by insurers, and (ii) the common coverage of certain types of risk by means of co-(re)insurance pools.[187] The EC is of the view that insurance is a product that covers future risks – the cost of which is unknown when the insurance contract is concluded. Consequently, the availability of

[184] Liyana Othman, Xabryna Kek (25 May 2016). *Never seen such a massive number of cases': Doctor who alerted MOH about gastroenteritis outbreak*. Channel News Asia.
[185] *CCS Guidelines on the Section 34 Prohibition 2016*, para 4.1.
[186] European Commission (13 December 2016). *Antitrust: The Insurance Block Exemption Regulation expires on 31 March 2017*. Daily News.
[187] European Commission (17 March 2016). *Report from the Commission to the European Parliament and the Council*. COM(2016) 153 final.

adequate and accurate past statistical information on the actual cost of risk classes is crucial to operations in various segments of the insurance business.[188] The exchange and/or aggregation of data (for example, the exchange of historical statistical data in the form of joint compilations, tables and studies [189]) was exempted because the EC recognises certain information exchanges to be justifiable to allow (re)insurers to accurately assess risk, and that they would be conducive to the efficient functioning of the insurance sector.[190] The EC announced that the expiry of the IBER does not mean that these forms of co-operation have become unlawful, but that companies need to assess their co-operation in the market context to see whether it is in line with competition rules.[191]

The position taken by the EC in the context of the insurance sector is persuasive in Singapore. For example, the sharing of data such as accident and claim histories by the insurers via an independent third party for the purpose of enabling each insurer to more accurately assess customer risk profiles and likelihood of future claims, is unlikely to pose competition concerns as long as the data shared is historical, factual, non-price related, and all insurers have fair access to these aggregated data. The presence of an independent third party helps to mitigate the risk of exchange of other commercially sensitive information in the process. There may also be net economic benefits generated by the sharing of such data as motor insurers can better detect and prevent insurance fraud, while at the same time, process each insurance application more quickly.

Concluding remarks on data sharing

146. In short, sharing of data is unlikely to cause competition concerns as long as it does not appreciably prevent, restrict or distort competition in Singapore. There are unlikely to be competition concerns when businesses share data with consumers or government agencies. In fact, such sharing is likely to be pro-competitive and overall beneficial to society. With regard to the sharing of data with competitors, the sharing of aggregated and historical information is unlikely to be problematic while the sharing of commercially sensitive data such as pricing or production capacity is likely to raise competition concerns, unless such sharing gives rise to net economic benefits. In relation to the sharing of data with businesses in other markets and industries, it is unlikely to be problematic as long as the sharing of data does not appreciably prevent,

[188] European Commission (17 March 2016). *Report from the Commission to the European Parliament and the Council*. COM(2016) 153 final.
[189] European Commission (17 March 2016). *Report from the Commission to the European Parliament and the Council*. COM(2016) 153 final.
[190] European Commission (17 March 2016). *Report from the Commission to the European Parliament and the Council*. COM(2016) 153 final.
[191] European Commission (13 December 2016). *Antitrust: The Insurance Block Exemption Regulation expires on 31 March 2017*. Daily News.

restrict or distort competition. The analytical framework set out in the CCS Guidelines on the Section 34 Prohibition 2016 for assessing anti-competitive conduct remains applicable for data sharing activities in data-driven industries.

(a) (ii) Anti-competitive agreements and concerted practices facilitated by algorithms

147. The advent of Big Data and data analytics has prompted the increasing widespread use of algorithms to capture, process and extract value from the vast volumes of data available today. Algorithms may be thought of as sequences of rules to be performed in order to carry out a certain task – they are instances of logic that generate an output from a given input.[192] With advances in computer science and artificial intelligence, algorithms have been developed to automatically perform repetitive tasks and solve problems involving complex calculations and data processing; and even make predictions or take decisions more efficiently than humans.[193]

148. Indeed, given that algorithms become better at their tasks when they are able to learn from a large volume of data, Big Data has in turn led to great improvements in algorithm technology.[194] While there are important efficiencies associated with this phenomenon, the risks associated with the use of data and pricing algorithms in facilitating or enabling collusive anti-competitive conduct has attracted much scrutiny in recent times.[195] This is unsurprising, given the latest indication in the EC's E-Commerce Sector Inquiry that approximately half of the respondent retailers track the online prices of competitors – of which 67% use automatic software programmes for such price-tracking.[196] The emerging issues with respect to algorithms and anti-competitive agreements are outlined below.

Algorithms and increased risks of collusive anti-competitive conduct

149. For any collusive equilibrium to be reached and sustained over time, it is necessary that colluding parties are in a position to (i) agree on a "common policy"; (ii)

---

[192] See generally, Organisation for Economic Co-operation and Development (9 June 2017). *Algorithms and Collusion*. DAF/COMP(2017)4, Section 2.1.

[193] Organisation for Economic Co-operation and Development (9 June 2017). *Algorithms and Collusion*. DAF/COMP(2017)4, para 9.

[194] See generally, Note by Avigdor Gal for OECD Roundtable on Algorithms and Collusion. (7 June 2017). *It's a Feature, not a Bug: On Learning Algorithms and what they teach us*, pp. 3, para 5-7.

[195] See generally, Organisation for Economic Co-operation and Development (27 October 2016), *Big Data: Bringing Competition Policy to the Digital Era*. DAF/COMP(2016)14; Autorité de la Concurrence and Bundeskartellamt (10 May 2016). *Competition Law and Data*; and Organisation for Economic Co-operation and Development (9 June 2017). *Algorithms and Collusion*. DAF/COMP(2017)4.

[196] Commission Staff Working Document accompanying the Final Report on the E-commerce Sector Inquiry, document SWD(2017) 154 final of 10 May 2017, para 149.

monitor the adherence to this common policy; and (iii) enforce the common policy by punishing any deviations.[197] Concerns have therefore been raised on how algorithms, Big Data and data analytics have the potential to provide new and enhanced means of fostering collusion, particularly because algorithms can enhance market transparency and the frequency of interactions between firms.[198] Two concerns are elaborated below.

150. First, market transparency may be enhanced through the use of monitoring algorithms, which allow companies to automatically collect and analyse real-time information concerning competitors' prices, business decisions and other market data.[199] The same technology that promotes market transparency and therefore consumer benefits, can also facilitate the monitoring of competitors' actions, as well as the detection of deviations from a collusive agreement – be it through the use of internet bots[200] which extract data automatically from websites (a process known as *web scraping* or *crawling*) or through other means, such as receiving data from data aggregators like price comparison websites. Furthermore, algorithms (enabled by powerful data mining capacity) may also prevent unnecessary retaliations through their ability to predict and distinguish between intentional deviations from collusion, and natural reactions to changes in market conditions, or even mistakes.[201] With the advent of even more sophisticated monitoring algorithm technologies such as those involving "wireless sensor networks" and "computer vision algorithms",[202] or Uber's "God View",[203] the ease and speed at which competitors' actions can be monitored

[197] See generally, economic literature cited in Organisation for Economic Co-operation and Development (11 October 2012). *Roundtable on Unilateral Disclosure of Information with Anticompetitive Effects (e.g. through press announcements).* DAF/COMP/WP3 (2012)1, at Section 2.2.

[198] See generally, Organisation for Economic Co-operation and Development (9 June 2017), *Algorithms and Collusion.* DAF/COMP(2017)4, at sections 4.2 and 4.3; European Commission (2017), *Final Report on E-Commerce Sector Inquiry,* COM(2017) 229 final, para 13; and Ezrachi, A. and M. E. Stucke (November 2016), *"Virtual Competition: The Promise and Perils of the Algorithm- Driven Economy",* Harvard University Press, United States, pp. 36.

[199] In relation to monitoring algorithms, see generally, Section 4.3.1 of Organisation for Economic Co-operation and Development (9 June 2017). *Algorithms and Collusion.* DAF/COMP(2017)4.

[200] Often referred to as "spiders": see, *Commission Staff Working Document* accompanying the Final Report on the E-commerce Sector Inquiry, document SWD(2017) 154 final of 10 May 2017, para 603.

[201] Organisation for Economic Co-operation and Development (9 June 2017). *Algorithms and Collusion.* DAF/COMP(2017)4, pp. 20, para 46.

[202] For more details on the application of such algorithm technologies to the monitoring of fuel prices in the petrol industry, see Organisation for Economic Co-operation and Development (9 June 2017), *Algorithms and Collusion,* DAF/COMP(2017)4, pp. 25 (Box 8).

[203] Ezrachi, A. and M. E. Stucke (November 2016), "*Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy*", Harvard University Press, United States, pp. 72-74.

may facilitate collusive outcomes by reducing incentives for deviations, making collusion more efficient.[204]

151. Second, the use of algorithms increases the frequency of interaction between firms and the ease of price adjustments, potentially increasing the speed at which firms can make business decisions.[205] With automated pricing algorithms, firms can more easily adjust prices to offer competitive pricing to consumers or align prices with competitors' real-time pricing, since algorithms allow online market price adjustments to be implemented more frequently and at a much lesser (or even no) cost, as compared to traditional brick-and-mortar businesses. Where previously, companies would have had to frequently renegotiate any collusive agreement through meetings, phone calls or emails in response to changes in trading conditions of highly dynamic markets, algorithms can instead automate the decision process of colluding companies so that prices react immediately and simultaneously to any changes in market conditions. Further, they could also be used to retaliate upon any deviations from collusion without the need to engage in further communication.[206]

152. Algorithms are by nature neutral and may be applied towards promoting competition or towards anti-competitive ends. While the use of algorithms does undoubtedly lead to efficiency gains, the preceding paragraphs highlight the need to balance these gains with the increased risk of collusion. As more firms become incentivised to invest in algorithm technology to benefit from "algorithmic competitive advantage",[207] competitors may find it easier to profitably sustain prices above competitive levels.[208]

Algorithms and competition enforcement

153. As elaborated upon earlier at paragraphs 137 to 138, section 34 of the Competition Act prohibits any agreements between undertakings, decisions by associations of undertakings or concerted practices which have as their object or effect the prevention, restriction or distortion of competition within Singapore. Where the use of algorithms is in furtherance of, or to support or facilitate any pre-existing or intended

---

[204] See also similar observations by the European Commission in the Commission Staff Working Document accompanying the Final Report on the E-commerce Sector Inquiry, document SWD(2017) 154 final of 10 May 2017, para 608.

[205] Organisation for Economic Co-operation and Development (9 June 2017), *Algorithms and Collusion*, DAF/COMP(2017)4, pp. 20, para 47.

[206] See generally, Organisation for Economic Co-operation and Development (9 June 2017). *Algorithms and Collusion*. DAF/COMP(2017)4, at Section 4.3.2 on parallel algorithms and Section 4.3.3 on signalling algorithms.

[207] Organisation for Economic Co-operation and Development (9 June 2017). *Algorithms and Collusion*. DAF/COMP(2017)4, pp. 19-20, para 45.

[208] Autorité de la Concurrence and Bundeskartellamt (10 May 2016). *Competition Law and Data*, pp. 14-15.

anti-competitive agreement or concerted practice, such cases fall squarely within the existing enforcement framework, even while competition agencies unravel how the algorithm technology works in the context of each particular anti-competitive infringement.[209]

154. For instance, in the 2015 *Topkins*[210] case in the United States, Topkins and his co-conspirators adopted a pricing algorithm that collected competitors' pricing information and wrote a computer code to instruct their software to set the posters' prices in conformity with their price-fixing agreement. Similarly, in the UK Competition and Markets Authority's 2016 infringement decision against price-fixing between two competing online sellers of posters and frames,[211] Trod Limited and GB eye Limited, the price-fixing agreement was also implemented using automated re-pricing software (a pricing algorithm) which monitored and adjusted prices to ensure that neither party was undercutting the other in certain specified circumstances.[212] Both these cases illustrate that as long as algorithms are used to assist in the implementation of an anti-competitive agreement and are ancillary to the main infringement, liability for breaching the section 34 prohibition can still be established based on evidence of the underlying anti-competitive agreement or concerted practice.

155. Similarly, where algorithms are used in classic 'hub-and-spoke' scenarios[213] which involve competitors colluding through a third party intermediary, this would equally be caught by the section 34 prohibition. Such a scenario could arise, for example, where there is an industry-wide use of a single algorithm to determine prices, and competitors use and rely on that same third party owned "hub" (a pricing algorithm) to coordinate their pricing strategies. In the EU case of *Eturas*,[214] which concerned travel agencies coordinating discount rates through the system administrator of a common computerised booking system, the European Court of Justice ("ECJ") stated in no uncertain terms that such a scenario would constitute a concerted practice under Article 101 of the Treaty on the Functioning of the EU (i.e. the EU equivalent of the section 34 prohibition), if competitors were aware of the system administrator's message to impose a cap on discount rates, and if they did not publicly distance themselves from that practice. Thus, by extension, if a common third party pricing

[209] Organisation for Economic Co-operation and Development, (9 June 2017). *Algorithms and Collusion*, DAF/COMP(2017)4, pp. 32, para 83.
[210] No. CR 15-00201 WHO. *United States of America v David Topkins*. United States District Court of the Northern District of California in San Francisco (30 April 2015).
[211] Case 50223, *Online sales of posters and frames*, Decision of the CMA (12 August 2016).
[212] Case 50223, *Online sales of posters and frames*, Decision of the CMA (12 August 2016), para 3.45-3.46, 3.62-3.93.
[213] See for example, *Replica Football Kits*, OFT decision (1 August 2003) and other similar cases; see also Case No 1188/1/1/11 *Tesco v OFT*, [2012] CAT 31, para 57, 74, citing the English Court of Appeal's judgement in *Argos Ltd v OFT*, [2006] EWCA Civ 1318, para 141.
[214] Case C-74/14, *Eturas and Others*, Judgment of the European Court of Justice (21 January 2016).

algorithm were to be used by competitors to coordinate prices, that would likely infringe the section 34 prohibition.

156. There has been lively discussion among competition practitioners, experts, and academics alike, about whether the existing competition enforcement framework is adequately equipped to deal with future developments involving algorithms.[215] For the most part, the main concern lies in how algorithms may lead to greater instances of tacitly collusive equilibriums which may well fall outside the current scope of competition enforcement.[216] Such a market outcome is expected to occur more frequently, given how algorithms are likely to change the structural characteristics of digital markets and how they enable collusive agreements to be reached more easily without any explicit communication between competitors.[217] Other key concerns raised include how a firm's independent and rational business justifications for using a third party pricing algorithm (such as it being too costly or time-consuming to independently develop the pricing algorithm and collect the needed market data) may be weighed against any anti-competitive effect that may result from such use;[218] and also, how liability may be established for any autonomous decision-making that results in collusive outcomes, in situations where self-learning algorithms (and in particular, deep learning algorithms) are involved.[219]

157. Equally, much can be said about how the use of algorithms may, in some material ways, render collusion difficult to sustain. For instance, increased customisation and differentiation of products and prices associated with the use of algorithms and Big Data may make tacit or explicit collusion more difficult because of

---

[215] See for example, Organisation for Economic Co-operation and Development (9 June 2017), *Algorithms and Collusion*, DAF/COMP(2017)4 at Section 5; and Ezrachi, A. and M. E. Stucke (November 2016), *"Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy"*, Harvard University Press, United States, on the possible collusion scenarios involving algorithms at Part II.

[216] See Organisation for Economic Co-operation and Development (9 June 2017), *Algorithms and Collusion*, DAF/COMP(2017)4, para 36; and see generally, discussion on the "oligopoly problem" at pp. 34 (Box 12).

[217] See generally, Note by A. Ezrachi & M. E. Stucke for OECD Roundtable on Algorithms and Collusion, (31 May 2017), *Algorithmic Collusion: Problems and Counter-Measures*, at Section 1.1; Organisation for Economic Co-operation and Development (9 June 2017), *Algorithms and Collusion*, DAF/COMP(2017)4, at Section 5.1; and see also earlier discussion above at para 149-152.

[218] Ezrachi, A. and M. E. Stucke (November 2016), "*Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy"*, Harvard University Press, United States, at pp. 48-49, 53-55 and 65; Note by A. Ezrachi & M. E. Stucke for OECD Roundtable on Algorithms and Collusion, (31 May 2017), *Algorithmic Collusion: Problems and Counter-Measures*, para 31.

[219] See generally, Organisation for Economic Co-operation and Development (9 June 2017*), Algorithms and Collusion*, DAF/COMP(2017)4, at Section 5.3; Ezrachi, A. and M. E. Stucke (November 2016), *"Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy"*, Harvard University Press, United States, at pp. 77-79.

cost asymmetry that may result as between competitors.[220] In addition, the innovative nature of digital markets involving algorithms as a source of competitive advantage also reduces the present value of collusive agreements and the ability of less innovative firms to retaliate, counterbalancing the enhanced risk of collusive outcomes that algorithms are thought to bring.[221] Furthermore, algorithms may even be designed and used to impede market transparency – by blocking rivals' web scraping/crawling bots, for example.[222]

Concluding remarks on algorithms and anti-competitive agreements

158. This section has sought to surface several key ideas in the ongoing debate on how algorithms might undesirably facilitate anti-competitive infringements – no matter how theoretical they may seem at this point in time. While it is clear that the current analytical framework is equipped to assess anti-competitive conduct involving algorithms, there are currently no settled positions on the various other concerns raised at paragraph 156 above.[223] Indeed, as the increasing use of algorithms in the Big Data environment is currently an evolving field, it is perhaps too early for anyone to have the last word on the matter.

159. Ultimately though, it must be recognised that algorithms are merely tools. In this regard, CCS remains committed to staying vigilant and ensuring that the use of new algorithms or artificial intelligence technologies do not result in harm to competition.

(b) Abuse of Dominance – Exclusionary conduct, including refusal to supply

160. A firm with a substantial degree of market power may be considered dominant. Section 47 of the Act prohibits any conduct amounting to an abuse of a dominant position, on the part of one or more undertakings, in any market in Singapore. According to the CCS Guidelines on the Section 47 Prohibition 2016 ("the Section 47 Guidelines"), conduct that constitutes an abuse of a dominant position in a market

[220] *Note from the Business and Industry Advisory Committee for OECD Roundtable on Algorithms and Collusion,* (9 June 2017), para 9; and Organisation for Economic Co-operation and Development (9 June 2017), *Algorithms and Collusion,* DAF/COMP(2017)4, pp. 21, para 52.

[221] Organisation for Economic Co-operation and Development (9 June 2017), *Algorithms and Collusion,* DAF/COMP(2017)4, pp. 20-21, para 51.

[222] See Jeffrey Dastin. (10 May 2017). *Amazon trounces rivals in battle of the shopping 'bots'*. Reuters.

[223] See generally, Organisation for Economic Co-operation and Developmen (9 June 2017). *Algorithms and Collusion,* DAF/COMP(2017)4 at Section 5; see also, for example, Note from the European Union for OECD Roundtable on Algorithms and Collusion (14 June 2017). *Algorithms and Collusion,* (14 June 2017); and Note by A. Ezrachi & M. E. Stucke for OECD Roundtable on Algorithms and Collusion, (31 May 2017). *Algorithmic Collusion: Problems and Counter-Measures*.

includes conduct that protects, enhances or perpetuates the dominant position of an undertaking in ways unrelated to competitive merit.[224]

161. CCS undertakes a two-step test to ascertain whether the section 47 prohibition has been infringed:[225]

a. First, it assesses whether an undertaking is dominant in a relevant market, either in Singapore or elsewhere. An undertaking will not be deemed to be dominant, unless it has substantial market power.[226]

b. If the undertaking is dominant, whether the conduct constitutes an abuse of the dominant position. CCS will undertake an economic effects-based assessment in order to determine whether the conduct has, or is likely to have, an adverse effect on the process of competition.[227]

162. The considerations in assessing each step are discussed below.

Assessing market power

163. Market power is usually understood as the ability to price profitably above the competitive price level, or to restrict output or quality below competitive levels. An

[224] Section 47(2) of the Act provides an illustrative list of conduct which may constitute an abuse of dominance as follows: (a) predatory behaviour towards competitors; (b) limiting production, markets or technical development to the prejudice to consumers; (c) applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage; and (d) making the conclusion of contracts subject to acceptance by other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of the contracts.

[225] *CCS Guidelines on Section 47 Prohibition 2016*, para 3.1.

[226] *CCS Guidelines on Section 47 Prohibition 2016*, para 3.3.

[227] In Appeal No. 1 of 2010. *In a matter of: notice of Infringement Decision issued by the Competition Commission of Singapore, Abuse of Dominant Position by SISTIC.com Pte Ltd, CCS 600/008/07, 4 June 2010*. Competition Commission of Singapore (28 May 2012), para 290-291, the Competition Appeal Board ("CAB") agreed with CCS that the "correct and proper test" in determining an abuse of dominance is as follows: "...an abuse will be established where a competition authority demonstrates that a practice has, or likely to have, an adverse effect on the process of competition. In particular: (a) It is sufficient for the competition authority to show a likely effect, and is not necessary to demonstrate an actual effect on the process of competition; (b) If an effect, or likely effect, on restricting competition by the dominant undertaking is establish[sic], the dominant undertaking can advance an objective justification. If it can adduce evidence to demonstrate that its behaviour produces countervailing benefits so that it has the net positive impact on welfare. However, the burden is on the undertaking to demonstrate an objective justification."

undertaking[228] will be considered to be dominant if it has substantial market power.[229] In assessing whether an undertaking is dominant, the extent to which there are constraints on an undertaking's ability to profitably sustain prices above competitive levels will be considered. Such constraints include the extent of competition from existing competitors, the possibility of new competitors entering the market (which is affected by the barriers to entry), the ability of buyers to counter the exercise of market power by the dominant player, government regulation, etc.[230]

164. Two key questions when assessing market power in data-driven industries are (i) whether the data could be replicated under reasonable conditions by competitors; and (ii) whether the use of data is likely to result in a significant competitive advantage.[231]

165. In addressing the two questions above, the unique aspects of data-driven markets would need to be taken into consideration. Set out below are features of data-driven markets that should be considered when assessing the market power of firms engaged in using data and applying data analytics. These features include network effects, multi-homing, access to substitute data, and market dynamics.

Network effects

166. Network effects refer to how the use of a good or service by a user impacts the value of the product to other users. In industries where data plays a prominent role, several forms of network effects may arise:

a. *Traditional network effects.*[232] This can be direct, where the value of a platform's product (e.g. email) to a user depends on the number of other users on the same side of the platform; or indirect, where the value of a platform's product to a user depends on the number of users on another side of the platform (e.g. Microsoft's operating system, where developers are attracted to the platform with the most users).

[228] Undertaking means any person, being an individual, a body corporate, an unincorporated body of persons or any other entity, capable of carrying on commercial or economic activities relating to goods or services. It includes individuals operating as sole proprietorships, companies, firms, businesses, partnerships, co-operatives, societies, business chambers, trade associations and non-profit-making organisations, whatever its legal and ownership status (foreign or local, government or non-government), and the way in which is it financed. See *CCS Guidelines on Section 47 Prohibition 2016*, para 2.4.

[229] *CCS Guidelines on Section 47 Prohibition 2016*, para 3.3.

[230] *CCS Guidelines on Section 47 Prohibition 2016*, para 3.4.

[231] Autorité de la Concurrence & Bundeskartellamt (10 May 2016). *Competition Law and Data*, pp. 11-13, 25-30.

[232] Maurice E. Stucke & Allen P. Grunes (9 June 2016). *"Big Data and Competition Policy"*. Oxford Printing Press, pp. 162–169.

b. *Scale of data – "Learning-by-doing".*[233] This refers to the phenomenon where the more users there are, the more data can be collected to make the product better for other users. This in turns encourages more potential users (e.g. Google search engine).

c. *Scope of data.*[234] This occurs when a firm extracts value from numerous data sources across its platform to make its product and services better, thereby encouraging more users to join (e.g. Google could gain insights about a user by combining information from Gmail, Chrome and YouTube, etc, to make more accurate predictions in search results).

d. *Spill-over effects.*[235] Traditional spill-over effects typically occur in a two-sided platform, where the increase in users on one side increases the value to the other side (e.g. more consumers shopping on an e-commerce platform attracts more sellers). Personal data magnifies these spill-over effects, as customised advertising leads to higher probability of purchase and encourages more advertisers.

167. Network effects may be asymmetric, such as in the context of a social network, where advertisers may derive benefits from a greater number of users but users may not derive benefits from a greater number of advertisers. Data collection and exploitation could potentially reinforce network effects, and substantial (sunk) expenditure will be required to counter or overcome existing network effects.[236]

168. While there are benefits to consumers from these network effects, the existence of strong and numerous forms of network effects in data-driven industries increase barriers to entry and expansion for new or smaller firms. Once the number of users reaches a critical mass, the market could "tip" in favour of one supplier (or sometimes, few suppliers).[237] When the market has "tipped", smaller firms will find it very challenging to compete effectively with the leading supplier, as they may not have

[233] Maurice E. Stucke & Allen P. Grunes (9 June 2016). *"Big Data and Competition Policy"*. Oxford Printing Press, pp. 170-185.
[234] Maurice E. Stucke & Allen P. Grunes (9 June 2016). *"Big Data and Competition Policy"*. Oxford Printing Press, pp. 186–189.
[235] Maurice E. Stucke & Allen P. Grunes (9 June 2016). *"Big Data and Competition Policy"*. Oxford Printing Press, pp. 189–199.
[236] Daniel L. Rubinfeld & Michal S. Gal (2 September 2016). *Access Barriers to Big Data*. Arizona Law Review 59(339), pp. 17.
[237] Maurice E. Stucke & Allen P. Grunes (9 June 2016). *"Big Data and Competition Policy"*. Oxford Printing Press, pp. 203.

access to the same quantity and quality of data to continuously make their product better.[238]

169. With network effects, the empirical question would be the level of the minimum scale that makes entry viable in order to overcome such network effects, and whether the minimum efficient scale is achievable.[239] Apart from looking at the cost of obtaining the data, the quality of the data analytics should also be taken into consideration. This may depend on the unique characteristics of each market, and may change from one market to another. One way of assessing the quality would be through consumers' revealed preferences, where the quality of the service which creates the platform for data collection forms an essential part of the analysis.[240]

170. Therefore, the impact of network effects must be carefully considered when assessing market power, especially when data and information (whether in a monetary form or not) forms a key part of the services provided.

Multi-homing

171. The potential for customers to "multi-home" in membership (i.e. to gain access to more than one platform for the same type of service) is a factor to consider in the assessment of market power. Where customers multi-home in membership, customers may be in a better position to resist attempts by a platform to exert its market power (e.g. increase prices) by switching to competing platforms. As part of CCS's conditional approval of the proposed acquisition by SEEK Asia Investments Pte. Ltd. of the JobStreet Business in Singapore,[241] CCS accepted the commitments offered by SEEK Ltd. and SEEK Asia Investments Pte. Ltd. not to enter into exclusive agreements with employer and recruiter customers (see paragraphs 203 to 205 below). These commitments sought to retain the existing practice of multi-homing (i.e. using more than one online recruitment advertising platform) by these customers, thereby ensuring that competing platforms can continue to enter and expand so that competition is preserved in the online recruitment advertising services market.

172. In cases where there exists high switching costs, multi-homing in usage (i.e. to use more than one platform for the same type of service) may be limited. Customers

[238] Maurice E. Stucke & Allen P. Grunes (9 June 2016). *"Big Data and Competition Policy"*. Oxford Printing Press, pp. 204.
[239] Daniel L. Rubinfeld & Michal S. Gal (2 September 2016). *Access Barriers to Big Data*. Arizona Law Review 59(339), pp. 18.
[240] Daniel L. Rubinfeld & Michal S. Gal (2 September 2016). *Access Barriers to Big Data*. Arizona Law Review 59(339), pp. 18.
[241] CCS 400/004/14 *In relation to the Notification for Decision of the proposed acquisition of SEEK Asia Investments Pte. Ltd. of the JobStreet Business in Singapore pursuant to section 57 of the Competition Act*, (13 November 2014).

may be discouraged from using competing services sufficiently to enable them to switch from one provider to another easily. For example, e-commerce platforms or ride booking companies may have loyalty programmes that require customers to spend a minimum amount within a given period of time to maintain their membership status and/or to enjoy additional benefits.[242] This may increase switching costs and limit the extent of multi-homing between platforms. New entrants or smaller firms may therefore find it difficult to attract customers, which then limits the extent of information that they are able to collect. Switching costs, both monetary and non-monetary in nature, have an impact on the ease of replicating data and should be taken into account when assessing market power.

Access to substitute data

173. Data may also be obtained from third parties, which would allow businesses to overcome the problem of large investments into the collection of data.[243] With advancements in technology and the increasing awareness of the usefulness of data, various types of data may have been collected, with only some being substitutable for others in relation to their use. For example, data from internet service providers relating to websites which a customer has surfed may possibly be substituted by data relating to the customer's social media account, with both indicating the preferences of the customer.[244] The scope and scale of data available to non-incumbents from third parties may not however rival the scope and scale of data possessed by an incumbent; the incumbent may still retain a significant competitive advantage as a result of the data it has. This is especially so if substitutable data, both in terms of quality and mass, is not available from third parties.

174. There may also be legal barriers to the collection of data. A case in point would be the French case of *GDF Suze*,[245] where GDF, as the sole regulated provider of gas, was in a unique position to collect contact details, technical information and consumption data. From 2007, French consumers could purchase gas at the regulated tariff (which only GDF could offer) or at the contestable market rates which GDF and other competitors could offer. GDF refused competitors access to data that could identify customers and their consumption pattern, which it had collected as the sole provider of gas at the regulated tariff. The French Competition Authority*, Autorité de la Concurrence,* was of the view that the data set was not replicable under reasonable financial conditions and in a sufficiently short time. Although the dataset was not considered an essential asset, the *Autorité de la Concurrence* concluded that it gave

[242] These benefits may include discounts (i.e. monetary), or priority booking of rides (non-monetary).
[243] Autorité de la Concurrence & Bundeskartellamt (10 May 2016). *Competition Law and Data*, pp. 44-45.
[244] Case No. COMP/M.4731. *Google/DoubleClick*, Commission Decision (11 March 2008).
[245] Maurice E. Stucke & Allen P. Grunes (9 June 2016). *"Big Data and Competition Policy"*. Oxford Printing Press, pp. 290.

GDF an unjustified competitive advantage relative to its competitors and that GDF was likely to have abused its dominant position on the gas market using this data. The *Autorité de la Concurrence* imposed interim measures on GDF ordering that it grant its competitors access to some of the data it collected as a provider of gas at the regulated rate, in particular consumer data.[246]

Market dynamics

175. E-commerce and other data-driven markets are characterised by rapid innovation, with new entrants being able to gain a foothold quickly under certain circumstances. For example, Facebook was able to displace the incumbent MySpace relatively quickly, despite the existence of network effects.[247]

176. Market contestability can be crucial in the assessment of market power.[248] The EC cited rapid innovation in consumer communications as the main reason for its clearance of the Facebook/Whatsapp merger, despite the presence of network effects (refer to paragraph 210 below).

177. An interesting view when considering market dynamics in the context of businesses dealing with data is that data is transient in nature, and the usefulness of data, regardless of volume, may be limited once the data gets outdated.[249] Further, while the intent is to use data for predictive purposes, feedback provided by businesses during the course of this research study indicated that the irrationality of human behaviour is such that the accuracy of such predictions is limited. The competitive advantage of collecting and holding a large amount of data may therefore not be as significant as expected, and the assessment of the market power of companies holding large amount of data should also be considered in this context.

Exclusionary conduct that could constitute an abuse of dominance

178. Even if a firm is assessed to be dominant, competition concerns will only arise when the firm engages in exclusionary conduct that has, or is likely to have, an adverse effect on the process of competition. The Section 47 Guidelines states that

[246] French Competition Authority, Decision 14-MC-02 of 09.09.2014. Due to privacy laws, the release of GDF data to competitors was conditional upon approval of consumers, and a significant proportion of the consumers refused to consent to the release of the data to the competitors; See also Autorité de la Concurrence and Bundeskartellamt (10 May 2016). *Competition Law and Data*, pp. 20, 31.
[247] Autorité de la Concurrence and Bundeskartellamt (10 May 2016). *Competition Law and Data*, pp. 29-30.
[248] Organisation for Economic Co-operation and Development (27 October 2016). *Big Data: Bringing Competition Policy to the Digital Era*. DAF/COMP (2016)14, pp. 17; and Autorité de la Concurrence and Bundeskartellamt (10 May 2016). *Competition Law and Data*, pp. 29-30.
[249] Competition & Markets Authority (June 2015). *The commercial use of consumer data*, pp 76.

exclusionary behaviour may include, amongst others, refusal to supply, or vertical restraints (e.g. tying) which foreclose (or are likely to foreclose) markets or weaken competition.[250] Such conduct may be abusive to the extent that it harms competition, for example, by removing an efficient competitor, limiting competition from existing competitors, or excluding new competitors from entering the market.[251]

179. Some examples of likely anti-competitive exclusionary conduct[252] that may arise in the context of data-driven industries are described in the following paragraphs.

Discriminatory access

180. A dominant firm could engage in exclusionary conduct by discriminating access to critical data for competitors.[253] This could occur when a dominant firm seeks to exclude a competitor from competing effectively in the market by refusing customers access to its data when customers use the competitor's services. A recent case involved the *Autorité de la Concurrence*, which examined whether market leader Cegedim's refusal to sell access to its widely-used customer relation management ("CRM") medical database to pharmaceutical laboratories using its competitor's, Euris, software constituted an abuse of dominance.[254] Cegedim was still selling access to laboratories using Cegedim's own and other competing CRM management software. Euris, who was the complainant, claimed that it lost 70% of its customers between 2008 and 2012, and lost all opportunities to develop its market share.

181. It was found that Cegedim was in a position of dominance and its CRM database was an essential and objectively indispensable facility. The *Autorité de la Concurrence* noted that Cegedim's database would be extremely costly and difficult to reproduce.[255] This decision was affirmed by the Court of Cassation in France.[256]

182. Discriminatory access to data for competitors may also be achieved through vertical integration.[257] For example, there is a possibility that e-commerce platforms which operate both the platform and their own online retail arm, could restrict data

[250] *CCS Guidelines on the Section 47 Prohibition 2016*, para 4.3.
[251] *CCS Guidelines on the Section 47 Prohibition 2016*, para 4.3.
[252] Maurice E. Stucke & Allen P. Grunes (9 June 2016) *"Big Data and Competition Policy"*. Oxford Printing Press, pp. 288 – 299.
[253] Autorité de la Concurrence & Bundeskartellamt (10 May 2016). *Competition Law and Data*, pp. 18 – 19.
[254] Autorité de la Concurrence. Decision n14-D06, as quoted in Autorité de la Concurrence & Bundeskartellamt (10 May 2016). *Competition Law and Data*, pp. 18-19.
[255] The Autorité de la Concurrence has imposed Cegedim a 5.7 million euros fine for having abusively refused to sell its medical information database to certain pharmaceutical laboratories, Autorité de la Concurrence, Press Release, 8 July 2014.
[256] *Cour De Cassation/Supreme Court of Appeal*, 21 June 2017.
[257] Autorité de la Concurrence & Bundeskartellamt (10 May 2016). *Competition Law and Data*, pp. 19.

available to other online retailers operating on the same platform. This gives the vertically-integrated e-commerce platform a competitive advantage over other online retailers, as it would have access to richer datasets on consumer preferences and buying patterns.

183. A dominant firm could also engage in exclusionary conduct by engaging in bundling/tying, which allows a firm to leverage on its market power in one market onto another.[258] Tying occurs when a firm dictates that the purchase of one product (the tying product) is conditional on the purchase of a second product (the tied product).[259] For example, a dominant firm which has market power through the possession of large datasets could tie the access of the data with its analytics services.[260] While this could bring about efficiency benefits for consumers in certain cases, it could also have an adverse effect on competition by foreclosing competitors or increasing barriers to entry for new firms.

Exclusive dealing

184. A business could potentially abuse its dominance by entering into exclusivity contracts with customers thus excluding entry of new competitors. In the case of *SISTIC,*[261] CCS issued an infringement decision against SISTIC.com Pte. Ltd. for abusing its dominance via a series of exclusive agreements with event venues and event promoters which restricted the choices of venue operators, event promoters and ticket buyers. CCS's decision was subsequently upheld by the Competition Appeal Board. Similarly, in the context of a data-driven industry, exclusive agreements can also harm competition in the market. For example, a dominant data aggregator offering access to a large body of data could enter into long term exclusive contracts with its customers such that other data aggregators would not be able to enter the market even if they are able to replicate the data.

Refusal to supply

185. Generally, many types of data are easily available and/or replicable. It is only in limited circumstances that certain types of data or data bases would be objectively indispensable such that the data/database cannot be replicated and no alternative

[258] Competition & Markets Authority (June 2015). *The commercial use of consumer data*, para 3.60 - 3.61.
[259] *CCS Guidelines on the Section 47 Prohibition 2016*, footnote 10.
[260] Competition & Markets Authority (June 2015). *The commercial use of consumer data*, para 3.60 – 3.61
[261] Appeal No. 1 of 2010. *In a matter of: notice of Infringement Decision issued by the Competition Commission of Singapore, Abuse of Dominant Position by SISTIC.com Pte Ltd, CCS 600/008/07, 4 June 2010*. Competition Commission of Singapore (28 May 2012), para 290-291.

solution is available. In these limited circumstances, refusal to supply[262] access to such data may constitute an abuse of dominance.

186. CCS has previously looked into a matter where an industry association required all its members (which made up a significant portion of the industry) to use the services of a service provider affiliated with the association and in the process, to provide relevant customer data to this service provider. As a result of this requirement, the affiliated service provider also accumulated an extensive amount of customer data which significantly enhanced the quality of its product offering. When a competing service provider entered the market, it found great difficulty persuading the association members to take up its services given that they were already required to use the service of the affiliated service provider. The association members also refused to provide customer data to the competing service provider since they were not using its service. This became a self-perpetuating cycle as the competing service provider was unable to develop a credible product to persuade the association members to take up its service. Subsequently, the association removed this requirement over concerns of an abuse of a dominant position and its members were free to use and supply customer data to competing service providers subject to compliance with existing regulations.

187. In Magill,[263] three broadcasters in Ireland, which owned the copyright in their programme listings, obtained injunctions against Magill TV Guide Ltd. ("Magill"), which was attempting to publish comprehensive weekly television guide. Magill lodged a complaint with the EC, alleging abuse of dominance by the broadcasters' refusals to grant licences for the publications of their listings.

188. The ECJ found that the broadcasters' refusal to provide basic information by relying on national copyright provisions prevented the appearance of a new product, which the broadcasters did not supply and for which there was potential consumer

[262] *CCS Guidelines on the Section 47 Prohibition 2016,* para 10.13-10.14 states that a facility will only be viewed as essential only when it can be demonstrated that (i) access to it is indispensable in order to compete in a related market, and (ii) where duplication (of the data) is impossible or extremely difficult owing to physical, geographical, economic or legal constraints (or is highly undesirable for reasons of public policy). As with refusal to supply cases in general, a refusal to allow access will constitute an abuse only if there is evidence of (likely) substantial harm to competition and there is no objective justification for the dominant undertaking's behaviour. In determining whether a refusal to allow access to an essential facility constitutes and abuses, and if so, on what terms access should be granted, care must be taken not to undermine the incentives for undertakings to make future investments and innovations, especially where the product is a result of previous innovation. It is rare that any datasets would be deemed as critical given that companies who require such datasets can either replicate the dataset or collect similar dataset with certain cost. It is only in limited circumstances that certain types of data are only available to certain parties.

[263] Joined Cases C-241/91P and C-242/91P, *Radio Telefis Eireann v. Commission*, 1995 O.J. (C137) 3 (6 April 1995).

demand. Such refusal constitutes an abuse of dominance, and the ECJ also clarified that the exercise of an exclusive right by a proprietor may, in exceptional circumstances, involve abusive conduct, but did not elaborate on what constitutes exceptional circumstances.

189. In *IMS Health*,[264] IMS Health was a supplier to pharmaceutical companies of German regional sales data in the form of a brick structure which corresponded to a designated geographical area. IMS obtained preliminary injunctions against its competitors on the basis that its competitor had infringed its copyright in the brick structure. One of its competitors, NDC, counterclaimed by alleging an abuse of dominance through IMS's refusal to supply, and also argued that it had not been able to develop alternate brick structures.

190. The ECJ found that it must be established that the creation of the alternatives is not economically viable for the production on a scale comparable to that of the incumbent. The ECJ highlighted the fact that a high degree of participation by the pharmaceutical laboratories in the improvement of the brick structure may have created a technical dependency by users on that structure, consequently, very significant technical and financial efforts would have had to be put in by these laboratories to use data presented in a different structure. Accordingly, it would not be economically viable for other suppliers to offer an alternative structure for the data on a scale comparable to IMS. The ECJ confirmed the position that switching costs should be taken into consideration when determining whether access is indispensable.

191. The ECJ also set out the conditions under which a refusal to license by a dominant firm that owns an indispensable product would constitute an abuse:

a. the undertaking requesting for the licence must intend to offer new products or services, on the market for the supply of data in question, for which there is potential consumer demand which the dominant player is not offering;

b. there are no objective justifications for the refusal; and

c. the refusal was such that it will reserve the market for the dominant player by eliminating all competition on that market.

Concluding remarks on abuse of dominance

192. Even in data-driven industries, the two-step test for assessing complaints relating to an abuse of dominance at paragraph 161 still applies. It is important to note that the mere accumulation of a large amount of data by a company in and of itself

[264] Case C-481/01, *IMS Health GmbH & Co. OHG v NDC Health GmbH & Co. KG*, 2004 O.J. (C3) 16 (29 April 2004).

does not equate to a firm being dominant. Even if the firm is assessed to be dominant, competition concerns will only arise when the firm engages in exclusionary conduct that has, or is likely to have, an adverse effect on the process of competition, for example, by foreclosing competitors in the market.

(c) Mergers between & acquisitions of firms engaged in data collection and data analytics which substantially lessen competition

193. As data collection and advanced analytics becomes more prevalent amongst companies in Singapore, issues could arise from the mergers and acquisitions of firms which engage in data analytics.

194. Under section 54 of the Competition Act, mergers that have resulted, or may be expected to result, in a substantial lessening of competition within any market in Singapore for goods and services are prohibited. Section 54(4) of the Competition Act also provides that the creation of a joint venture to perform, on a lasting basis, all the functions of an autonomous economic entity shall constitute a merger.

195. One issue which might arise involves how CCS will assess the merging between firms which hold large data sets, and correspondingly the consolidation of two previously separate data sets. A second issue which might arise involves whether CCS might treat data protection concerns arising from the merging of these data sets as a relevant competition-related consideration.

Competition assessment of mergers involving large data sets

196. According to the CCS Guidelines on the Substantive Assessment of Mergers 2016 ("the Section 54 Guidelines"), the determination of whether there is a substantial lessening of competition involves an assessment of the degree to which competition is harmed and this assessment depends on the facts and circumstances of each merger.[265] Where a merger has a significant impact on rivalry between firms within a market over time, and reduces the competitive pressure on firms to improve their offerings to customers or become more efficient or innovate, a substantial lessening of competition is likely to arise. In applying the substantial lessening of competition test, the competitive effects on immediate, subsequent, intermediate and final customers of the merged entity will be examined.[266] The assessment of whether a merger situation is likely to substantially lessen competition will compare the likely state of competition if the merger situation proceeds, with the likely state of competition if the merger situation does not proceed.[267]

---

[265] *CCS Guidelines on the Substantive Assessment of Mergers 2016*, para 4.5.
[266] *CCS Guidelines on the Substantive Assessment of Mergers 2016*, para 4.10.
[267] *CCS Guidelines on the Substantive Assessment of Mergers 2016*, para 4.14.

197. The focus of CCS's assessment of a merger is on evaluating how the competitive constraints on the merger parties and their competitors might change as a result of the merger. CCS's merger assessment typically starts with defining the relevant market(s), which provides a framework within which to identify and assess the competitive constraints a merged firm would likely face.[268] An elaboration of the complexities arising from market definition for firms which engage in data analytics is found above at paragraphs 126 to 130.

198. As set out within CCS's Section 54 Guidelines, horizontal and non-horizontal mergers will affect competition in different ways.[269] A horizontal merger is a merger between two entities active (or potentially active) in the same market at the same level of business and could give rise to non-coordinated effects or coordinated effects.[270] Non-coordinated effects may arise when a company merges with an existing competitor, which might otherwise provide a significant competitive constraint.[271] Coordinated effects may arise when the merger increases the incentive for some or all firms in the same market to coordinate their behaviour by raising prices, reducing quality or reducing output, and such collusion is sustainable due to no or little competition from other sources.[272]

199. A non-horizontal merger is one where the relevant markets in which the merging parties operate are distinct, with no overlap of directly competing products.[273] Non-horizontal mergers include vertical mergers and conglomerate mergers. Vertical mergers are mergers between firms that operate at different but complementary levels in the chain of production and/or distribution,[274] while conglomerate mergers involve the consolidation of firms that operate in different product markets without a horizontal or vertical relationship.[275] Non-horizontal mergers may result in efficiencies, and are less likely to result in competition concerns.[276]

200. Regardless of whether the merger is a horizontal or non-horizontal one, CCS will assess the following factors when considering whether there is a substantial lessening of competition in the relevant market, both with and without the merger:

---

[268] *CCS Guidelines on the Substantive Assessment of Mergers 2016*, para 5.2.
[269] *CCS Guidelines on the Substantive Assessment of Mergers 2016*, para 4.11.
[270] *CCS Guidelines on the Substantive Assessment of Mergers 2016*, para 5.17 – 5.19.
[271] For a more comprehensive discussion on the assessment of non-ordinated effects, see *CCS Guidelines on the Substantive Assessment of Mergers 2016*, para 5.20 – 5.30.
[272] For a more comprehensive discussion on the assessment of the coordinated effects, see *CCS Guidelines on the Substantive Assessment of Mergers 2016*, para 5.33 – 5.45.
[273] *CCS Guidelines on the Substantive Assessment of Mergers 2016*, para 6.1.
[274] *CCS Guidelines on the Substantive Assessment of Mergers 2016*, para 6.3 – 6.20.
[275] *CCS Guidelines on the Substantive Assessment of Mergers 2016*, para 6.21 – 6.29.
[276] *CCS Guidelines on the Substantive Assessment of Mergers 2016*, para 6.5 – 6.6 and 6.21 – 6.23.

a. Market shares and concentration – the number and size of firms in a market can be an indicator of competitive pressure pre- and post-merger.

b. Barriers to entry and expansion – the extent to which existing competitors would expand their sales or new competitors would enter and compete effectively if prices were increased, and also competition from potential competitors which involves assessing barriers to entry and whether entry is likely, timely and sufficient in extent.

c. Countervailing buyer power – the potential for a business to be sufficiently constrained by a purchaser's ability to exert substantial influence on negotiations.

201. It should be highlighted that the discussion found at paragraphs 163 to 177 pertaining to the features of data-driven markets should be taken into account when assessing the above-mentioned factors.

202. This analytical framework was used in CCS's assessment of past mergers involving combination of data sets that were held by competitors.

203. In its assessment of the proposed acquisition by SEEK Asia Investments Pte. Ltd. of the JobStreet Business in Singapore,[277] CCS considered that the proposed transaction involved the merging of the recruitment platforms operated by JobsDB Singapore and JobStreet Singapore, and correspondingly their jobseeker databases. CCS noted that quality jobseeker databases would take time to build up, and jobseeker information was not something that a new entrant – even with resources – could collect overnight. At the point of CCS's assessment, none of the alternative job portals had the reach and depth of candidate pool as the merged entity would have. Any new entrant would have to invest heavily in advertising and marketing to garner a critical mass of jobseekers and recruiters to its platform, to overcome the significant network effects enjoyed by the merging parties. This represented a significant barrier to entry for a new entrant.

204. At the end of its assessment, CCS concluded that the proposed transaction would be likely to result in a substantial lessening of competition in the market for the supply of online recruitment advertising services. CCS noted that the proposed transaction would result in a loss of rivalry between close competitors, and that there was a lack of effective competitive constraints by existing and new competitors. CCS was concerned that the proposed transaction would result in the following non-coordinated effects:

[277] CCS 400/004/14, *Notification for Decision of the proposed acquisition of SEEK Asia Investments Pte. Ltd. of the JobStreet Business in Singapore pursuant to section 57 of the Competition Act* (13 November 2014).

a. Ability/incentive to change the structure of the market by demanding exclusive "lock-in" contracts, which prevent customers from switching away from the merged firm;

b. Ability/incentive to bundle and tie products across its two brands which would have the effect or likely effect of preventing customers from switching away from the merged firm; and

c. Ability/incentive to impose price increases post-merger.

205. Behavioural commitments were offered by the merging parties to address the abovementioned competition concerns. Divestiture commitments were also offered to address CCS's other concerns over SEEK Asia Investments Pte. Ltd.'s ownership of a job aggregator site. The transaction received conditional clearance, subject to the implementation and compliance with these commitments.

206. In CCS's assessment of the merger between Thomson Corporation and Reuters Group PLC,[278] the concentration of data sets of the merging parties was also a relevant factor in considering the barriers to entry. With regard to the earnings estimates market, CCS noted that a new entrant would have to secure contracts with a large number of brokers in order to form a critical mass of earnings estimates data so that it might be able to effectively compete. Additionally, the new entrant would require skilled staff to normalise the detailed estimates data from many brokers to produce consensus estimates. With regard to the fundamentals market, CCS noted that an effective fundamentals database would take a long time to compile before it could achieve the requisite geographical reach and historical depth. Skilled staff would similarly be needed to standardise the "as reported" fundamentals. These factors tended to indicate high entry costs, which in turn, suggested that the merger might substantially lessen competition in Singapore.

207. Nonetheless, CCS noted that the merging parties had offered commitments to the Department of Justice ("DOJ") and the EC. These commitments were subsequently amended and accepted by the DOJ and EC. Under these commitments, the parties undertook, amongst other things, to do the following:

a. To sell copies of certain databases to allow the purchaser to rapidly enter the market and compete with the merged entity's offerings;

b. To allow the purchaser of the databases to hire the necessary personnel from the parties;

[278] CCS 400/007/07, *Notification for Decision: Merger between the Thomson Corporation and Reuters Group PLC*. (23 May 2008).

c. To license to the purchaser of the databases all intellectual property rights, trade secrets, know-how and technical information for collection, aggregation, normalisation and transmission that will allow the acquirer to operate the database; and

d. To provide the purchaser with transitional technical support services such that the purchaser is able to integrate the purchased databases into its own offerings.

208. Having assessed these commitments, CCS concluded that they would have worldwide effect and would be able to address any competition concerns which may arise. As such, CCS concluded that the merger would not infringe the section 54 Prohibition.

209. Similarly in its assessment of Google's acquisition of DoubleClick,[279] the EC assessed the merger using its existing analytical framework. The EC considered whether the mere combination of Google and DoubleClick's customer data sets would result in a foreclosure of Google's competitors. The EC concluded that data collection on customer search and web-browsing behaviour would not significantly impede effective competition even if the merged data set could potentially be used to better target ads to users. This is because the merged data set was already available to a number of competitors, or could be purchased from third parties. In fact, the EC noted that the data collected from third party companies which offer "deep packet inspection" of network traffic routed through internet service providers might be more broad and insightful than the data collected by DoubleClick, the merged entity, or its competitors. The EC thus concluded that "the possible combination of data of Google and DoubleClick post-merger is very unlikely to bring more traffic to AdSense so as to squeeze out competitors and ultimately enable the merged entity to charge higher prices for its intermediation services."

210. In 2014, the EC again considered the issue of data concentration in Facebook's acquisition of Whatsapp.[280] The EC considered whether competition in the provision of online advertising services would be significantly hampered by Facebook leveraging on Whatsapp as a potential source of user data to improve its ability to target advertisements or by introducing advertisements on Whatsapp. The EC concluded that regardless of whether Facebook did so, there existed a sufficient number of alternative providers of online advertisement services which collected user data alongside Facebook. The EC noted that Facebook only accounted for a 6.39% share of data collected across the internet. Additionally, a large amount of internet user data which is valuable for advertising purposes is not within Facebook's exclusive control.

[279] Case No. COMP/M.4731. *Google/DoubleClick*, Commission Decision (11 March 2008).
[280] Case No. COMP/M.7217. *Facebook/Whatsapp*, Commission Decision (3 October 2014).

211. In both EC merger cases, the assessment took into account the availability of the data to and the existing data collection practices of the merging parties' competitors. These factors assisted the EC to consider whether the concentration of data conferred any competitive advantage upon the merging parties, to an extent that its rivals would not be able to effectively compete. Having regard to the fact that the close competitors of the merging parties were or could amass data sets of a similar or larger scale, the concentration of data post-merger would not result in a significant competitive advantage over said competitors, such that it would significantly impede effective competition.

212. While the advancement of technology and advent of data analytics may be fresh developments, the consolidation of data sets of merging parties is not. As evinced from the abovementioned cases, the current analytical framework is sufficiently flexible and robust to assess whether the concentration of data will result in non-coordinated or coordinated effects that could substantially lessen competition.

Data protection as a competition consideration

213. Facebook's acquisition of Whatsapp also raised an important question about the role that privacy-related considerations ought to play in a merger assessment. The EC stated that for the purposes of this merger assessment, it "analysed potential data concentration only to the extent that it is likely to strengthen Facebook's position in the online advertising market or in any sub-segments thereof. Any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the transaction do not fall with the scope of EU competition rules but within the scope of EU data protection rules."[281] In other words, any loss of privacy arising from the consolidation of Facebook and Whatsapp's data sets was, in and of itself, irrelevant for the purposes of the competition assessment.

214. This statement was subsequently clarified in the EC's decision on Microsoft's acquisition of LinkedIn.[282] In its analysis of the potential data concentration as a result of the merger, the EC made clear that privacy concerns per se is not a competition issue. Nonetheless, privacy-related concerns can be taken into account in the competition assessment to the extent that consumers see it as a significant factor of quality and the merging parties compete on this basis. In this case, privacy was found to be an important parameter of competition and driver of customer choice and thus ought to be taken into account in the competition assessment.

215. On this issue, Federal Trade Commission's Commissioner Terrell McSweeny stated that: "The decisions firms make about consumer privacy can give rise to non-

[281] Case No. COMP/M.7217. *Facebook/Whatsapp*, Commission Decision (3 October 2014), para 164.
[282] Case M.8124. *Microsoft/LinkedIn*, Commission Decision (6 December 2016).

price competition. In this context, we can consider consumer privacy in a merger investigation. Absent a clear nexus to competition, privacy and data protection concerns are considered under applicable consumer protection statutes rather than under our antitrust laws."[283]

216. While there have been calls for competition law to be applied to promote data protection and privacy policy,[284] this does not appear to be a consideration that is consistent with the scope of CCS's role and functions. The objective of competition law in Singapore is to promote the efficient functioning of our markets towards enhancing the competitiveness of the Singapore economy. However, where data protection is a non-price factor of competition (e.g. privacy is something which affects the quality of a service delivered), the treatment of personal data may affect how CCS considers and assesses the competitive dynamics of a specific market. It should be highlighted that CCS's current analytical framework already takes into account competition on the basis of non-price factors, thereby enabling CCS to consider data protection as a non-price factor of competition within its assessment.[285]

[283] Commissioner Terrell McSweeny's remarks at the EDPS-BEUC Joint Conference on 29 September 2016; See also Commissioner Terrell McSweeny's keynote remarks at the 16th Annual Loyola Antitrust Colloquium on 15 April 2016.

[284] For example, the European Data Protection Supervisor ("EDPS") suggests that competition law should be applied to promote data protection and privacy policy, and that data protection should be seen as a standalone factor in consumer welfare. This position is elaborated upon in the Preliminary Opinion of the EDPS (March 2014). *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*.

[285] *CCS Guidelines on the Substantive Assessment of Mergers 2016*, para 2.4 states that "CCS will assess the above factors when assessing the non-coordinated effects of the merger situation, which arise when there is a loss of competition between the merger parties and the merged entity finds it profitable to raise prices and/or reduce output or quality. In so doing, CCS will consider the extent to which the merger parties are close competitors. The above factors are also considered in assessing whether a merger situation raises or leads to increased scope for "coordinated effects", which arise if the merger situation raises the possibility of firms in the market coordinating their behaviour to raise prices, reduce quality or output."

VIII. IMPLICATIONS ON PERSONAL DATA PROTECTION

217. Notwithstanding the immerse benefits from data analytics, data activities carry inherent risks, especially the potential for misuse of personal data derived from connected devices and sensors. Data protection plays a crucial role in the growth of Singapore's digital economy by strengthening consumers' trust in our companies' capabilities to protect their data with new ways of doing business, and enhancing their competitive advantage in the evolving data landscape. Against this backdrop, Singapore's PDPA[286] was enacted in 2012 with the purposes of protecting individuals' personal data and at the same time, enabling organisations to leverage personal data for legitimate uses and business innovations that can deliver greater benefits for individuals and the society.

Personal data protection legislation in Singapore

What is Personal Data?

218. Personal data is defined in the PDPA as "data, whether true or not, about an individual who can be identified —

a. from that data; or

b. from that data and other information to which the organisation has or is likely to have access."

219. The term "personal data" is not intended to be narrowly construed and covers all types of data from which an individual can be identified, regardless of whether such data is true or false.[287]

---

[286] *Personal Data Protection Act 2012* (No. 26 of 2012) (Singapore).

[287] An individual can be identified by an organisation if that individual can be singled out from other individuals based on one or more characteristics of the data itself and/or combined with other pieces of information. Such characteristics or data form part of the individual's personal data.

Similarly, an individual can be identified based on certain data and other information to which the organisation has or is likely to have access. Even if such data does not directly identify the individual in question, it may still be considered personal data if the organisation has access to other information that, when taken together with the data, would allow the individual to be identified.

In the context of Big Data, data is collected or generated in a regular and continuous manner in high volume, and may even be collected passively and/or discreetly (without the individual's knowledge or action). Though the data collected may or may not contain directly identifying data, the risk of the data identifying an individual is significant considering the volume of data generated in the process.

Summary of Legislative Requirements for Processing Personal Data in Singapore

220. The PDPA provides for consent as a key basis for collecting, using and disclosing personal data. The consent obligation allows individuals to exert choice and authority over activities involving the collection, use or disclosure of his personal data. Unless an organisation's activities fall within an exception under the PDPA, the organisation must seek the individual's consent for any collection, use or disclosure of his personal data. In addition to the consent obligation, individuals have the right to withdraw their consent at any time.

221. The purpose limitation obligation establishes the boundaries for what the personal data may be collected, use and disclosed for, while offering organisations some measure of flexibility in using the data. It is predicated on two notions - first, the purposes must be considered appropriate in the circumstances by a reasonable person, and second, the individual must be informed of the purposes.[288]

222. The PDPA also contains provisions for the care of personal data, such as the obligation to ensure the accuracy of personal data if the organisation is likely to use the data to make a decision about the individual or if the data is likely to be disclosed to another organisation. In addition, organisations are required to make reasonable security arrangements to protect the personal data in their possession or under their control; and to cease to retain the personal data when there is no legal or business purpose to do so.

223. In addition, the PDPA requires, upon the individual's request, for the organisation to provide access or to correct his personal data, as well as make available information about its data protection policies, practices and complaint process. Annex 1 provides a more complete summary of all the data protection obligations under the PDPA. The PDPA confers various powers on the PDPC to enforce its data protection provisions. [289]

Furthermore, given that Big Data analytics involve the meshing of datasets and data streams, insights generated from the analytics could also create additional personal data. For example, data generated automatically and meshed with a dataset containing identifying information could result in new attributes associated with an individual, adding a "fuller picture" to an individual's characteristics and resulting in the generation of "new" personal data.

[288] Pursuant to the Notification obligation, an organisation would have to notify the individual of the purpose(s) for which it intends to collect, use or disclose the individual's personal data on or before it does so. Personal Data Protection Commission (Revised 15 July 2016). *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*, para 7.

[289] a) Powers relating to alternative dispute resolution – these powers generally relate to the manner by which a complainant and organisation may resolve the complaint, for example through mediation or other modes of dispute settlement;

Commercial Transactions of Databases

224. While the PDPA does not prevent the buying or selling of data, the purpose limitation obligation does require that data is only collected, used and disclosed for a reasonable purpose. This means that any commercial activities conducted in relation to the sale of personal data must be tempered with an objective test of "reasonableness". Hence, whether the commercial sale (i.e. disclosure from one organisation to another) of personal data and its subsequent collection, use or disclosure by the purchasing organisation can be considered reasonable would depend on the specificity of the consent obtained.

225. In general, the PDPC has stated that any determination of whether a reasonable person would consider the collection, use or disclosure of data appropriate would need to take into account the relevant circumstances. For example, where the purpose is harmful to the individual concerned, such purposes would unlikely be considered appropriate by a reasonable person. Similarly, if consent was obtained for a very broad purpose (e.g. "for analytics purposes"), but the personal data was subsequently sold and used by the purchasing organisation to market directly to a specific individual, or to make specific decisions about an individual that have an impact to the individual concerned, then it is unlikely the consent obtained for the purpose of data analytics would reasonably extend to the activities of the purchasing organisation.

Ensuring relevance of personal data protection in a Big Data environment

226. In a digital economy, personal data is expected to generate significant economic and societal value. It is often argued that for data assets to be fully utilised, it is essential to treat data as something to be meshed, analysed and used, and for fewer restrictions on data use to spur innovation. However, this has to be balanced against the need for the individuals to have control over their own personal data. Otherwise, a vicious cycle of suspicion towards data and analytics activities could emerge, leading to individuals becoming more reluctant to consent and organisations, in turn, becoming more opaque in their data activities. In this context, data protection

b) Powers relating to reviews – these powers enable the PDPC to review an organisation's reply to an individual's request for access or correction to his data, and to confirm the organisation's reply or direct the organisation to take certain action in relation to the individual's request; and
c) Powers relating to investigations – these powers enable the PDPC to determine whether an organisation is complying with the PDPA and to direct a non-compliant organisation to take appropriate action. In addition to other sanctions, the PDPC is empowered to direct organisations to pay a financial penalty not exceeding $1 million.

legislation is all the more relevant as it acts as an arbiter, establishing the balance and proportionality[290] between commercial needs and individual rights.

Addressing the challenges of consent-based approach to personal data protection

227. Data mining and data use appear contrary to the aims of protecting personal data. Arguments have been made that conventional approaches to data protection legislation may be ill-equipped to address how data is handled and managed today.[291] A key aim of the consent-based approach was to address specific concerns pertaining to computerised databases.[292] Advances in technology are changing the way data is collected and processed. This poses new challenges for a consent-based approach to the protection of personal data. Regulations will need to evolve to keep pace with the developments. For example, enforcement actions taken in Europe and the United States have often focused on providing privacy notices, which may not involve allegations of substantial harms to individuals.[293]

228. Some advocates opine that the data minimisation[294] approach present in many of the data protection laws, limits innovation and the discovery of unexpected but potentially important insights. [295] Proliferation of data analytics presents a key challenge in particular for purpose limitation, because consent obtained at the point of data collection, cannot be extended to the subsequent re-purposing for data meshing or analytics. Organisations are unable to define their purposes at the outset as these may change with context or in light of new discoveries.

---

[290] Andrew Serwin (18 August 2009). *Privacy 3.0 – The Principle of Proportionality*, University of Michigan Journal of Law Reform 42(4), pp. 875.

[291] Data collection practices are extremely complex and the way organisations collect information on one occasion, for one purpose, and then subsequently retain, analyse and distribute for a variety of purposes in unpredictable, renders "notice and choice" model, inadequate. See, R. Sloan and R. Warner (2014). *Beyond Notice and Choice*. Journal of High Technology Law XIV(2), pp. 391

[292] Specific concerns related to the developments in automated data banks, and the growing use of computers in the private and public sectors, meant that individuals no longer had control over their own data and by extension, their privacy. See, Eloïse Gratton (11 July 2016). *Beyond Consent-based Privacy Protection*.

[293] Fred Cate (2006). *The Failure of Fair Information Practice Principles*, J. Winn (Eds.), Consumer Protection in the Age of the Information Economy, pp. 367.

[294] Under the European General Data Protection Regulations, data minimisation refers to the concept that personal data collected must be adequate, relevant and limited to those which are necessary in relation to the purposes for which they are processed. See Bird & Bird (May 2017) *Guide to the General Data Protection Regulation*.

[295] See generally, Jules Polonetsky, and Omer Tene (April 2013). *Big Data for All: Privacy and User Control in the Age of Analytics*. Northwestern Journal of Technology and Intellectual Policy 11, pp. 242.

229. The consent-based approach to personal data protection continues to be relevant in providing individuals control over their personal data as a safeguard against potential misuse of personal data, particularly as commercially-driven third parties would not typically prioritise the individual's or society's interests beyond those of their own commercial activities.[296] This is particularly evident in many of existing Internet business models, where there are often commercial incentives to re-purpose, mesh and share data to extract greater value from it.[297]

230. As more data is meshed, however, the new possibilities for personal data use could present implications and impact that the individual does not expect. The task of obtaining (and tracking) consent with the changing uses of the personal data (or correspondingly withdrawals) becomes more difficult. Internationally, data protection advocates have encouraged the use of innovative consent methods, such as dynamic or iterative approaches to consent, in-lieu of a one-off compliance tick-box.[298] Consent-taking is therefore an on-going and actively managed choice, with granular options offered to the individuals at relevant junctures.

231. Where obtaining consent is not possible given the large volume of personal data collected from individuals,[299] or where consent has unaccounted distributive effects[300] and social costs,[301] data protection authorities internationally have responded by creating regulatory frameworks that focus on accountability, and incorporate a degree of flexibility for organisations intending to use personal data for legitimate purposes or interests.[302] For example, the European Union General Data

---

[296] D. Boyd and K. Crawford (10 May 2012). *Critical Questions for Big Data*. Information, Communication and Society 15(5), pp. 664.

[297] World Economic Forum (February 2013). *Unlocking the value of personal data: From Collection to Usage*, pp. 10.

[298] See generally, L. Hutton and T. Henderson (10 May 2017) *"Beyond the EULA: Improving Consent for Data Mining",* T. Cerquitelli D. Quercia F. Pasquale (Eds), Transparent Data Mining for Big and Small Data 11, pp. 164.

[299] Craig Mundie (April 2014*). "Privacy Pragmatism; Focus on Data Use, Not Data Collection",* Foreign Affairs 93(2), pp. 28.

[300] While the consent-based model generally assumes that individuals would exercise meaningful control over their right to consent based on a weighing of cost-and-benefit to themselves, it does not follow that such individual decisions would collectively yield the most desirable social outcome. See generally, Lior Strahilevitz (20 May 2013). *Toward a Positive Theory of Privacy Law*, Harvard Law Review 126, pp. 2010.

[301] This is particularly relevant in the context of re-purposing data for evidence-based research or policy making, such as for research purposes that would lead to new or improved medical treatments. See generally, A. Acquisti et al. (14 June 2016*). The Economics of Privacy*, Journal of Economic Literature 52(2), pp. 5

[302] Jurisdictions that have included provisions for legitimate interests or purposes, includes the European Union and the United Kingdom.

Protection Regulation ("GDPR"), outlines a framework for "legitimate interests"[303] which provides a basis for data use where consent is unobtainable or impractical[304]. The legitimate interests of a data user would take into consideration the reasonable expectations of data subjects in the context of their relationship with the data users.

232. In Singapore, the PDPC recognising that relying only on consent for the collection, use and disclosure of personal data may have deleterious effects – for example in circumstances where it is not possible for organisations to anticipate the purposes for using and disclosing personal data at the outset, and where it is impractical to seek individuals' consent in every instance of data collection, or to attempt to identify the individuals in order to seek their consent for every new purpose – has released a *Public Consultation for Approaches to Managing Personal Data in the Digital Economy*[305] to seek opinion on parallel bases other than consent. These parallel bases cater to circumstances where consent is not feasible or desirable, and where the collection, use or disclosure would benefit the public (or sections thereof). The parallel bases other than relying on consent are: "notification of purpose" if the taking of consent is impractical; and where there is a "legal or business purpose" and it is not desirable or appropriate to obtain consent. The PDPC has also published a *Guide to Data Sharing*[306], which includes a framework for data sharing arrangements ("DSAs") that may be exempted under the PDPA in circumstances where obtaining consent is impractical or undesirable. This framework is intended to test the proposed parallel bases for consent. Under the framework, PDPC will consider granting an exemption from relevant PDPA obligations for data sharing arrangements that meet the following criteria:

a. Personal data shared under the DSA must be with a specified group of organisations for a specified period of time;

b. The purposes of the DSA must be defined and specific; and

[303] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regards to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC, Section 47, at L119/9.

[304] De Brauw Blackstone Westbroek (9 June 2014). *EU guidance on legitimate interests of data controller to support big data.*

[305] Personal Data Protection Commission (27 July 2017). *Public Consultation for Approaches to Managing Personal Data in the Digital Economy*.

[306] Personal Data Protection Commission (27 July 2017). *Guide to data sharing*.

c. Obtaining consent is impractical or undesirable wherein the proposed data sharing arrangement satisfies one of the following two circumstances:

1. Obtaining consent is impractical

- It is **impractical to obtain consent** (deemed consent does not apply); and
- Purpose is **not expected to have any adverse impact on the individuals**.

Example:
Organisation does not have individuals' contact information or accurate contact information; or burden or cost of seeking consent is unreasonable to the organisation or disproportionate to the individual's interests.

2. Obtaining consent is undesirable

- It is **not desirable or appropriate to obtain consent** for the purpose; and
- **Benefits** to the public (or section thereof) **clearly outweigh any adverse impact or risks to the individual**.

Example:
Organisation is unlikely to be able to obtain consent from individuals who are trying to avoid fraud detection, to share their personal data for the purpose of fraud detection.

Using anonymised data when meshing and pooling data

233. Big Data thrives on data proliferation – benefits are derived from the analysis of large amounts of personal data or its derived form.[307] The larger the amount of data available, the better and more numerous the insights derived.[308] Big Data proponents highlight that data analytics and related activities do not often require individuals to be identified, as data analytics is intended to draw out general insights rather than information about a specific individual.[309] These derived inferences and insights from aggregated or other forms of anonymised or de-identified data mean that *anonymisation* could be a feasible option when carrying out Big Data activities.

[307] Anonymised or de-identified. Anonymised data refers to data that does not identify any particular individual. De-identified data (or data with personal *identifiers* removed) may not necessarily be anonymised according to the PDPA definition of personal data. If the de-identified data combined with other data or information contains a serious possibility that an individual can be identified, then the de-identified data still qualifies as personal data under the definition of the PDPA, and therefore is not considered anonymised. See generally, Personal Data Protection Commission (Revised 28 March 2017). *Advisory Guidelines on the Personal Data Protection Act for Selected Topics*, pp. 9.

[308] See generally, Jules Polonetsky, and Omer Tene (April 2013). *Big Data for All: Privacy and User Control in the Age of Analytics*. Northwestern Journal of Technology and Intellectual Policy 11, pp. 246.

[309] See generally, Jules Polonetsky, and Omer Tene (April 2013). *Big Data for All: Privacy and User Control in the Age of Analytics*. Northwestern Journal of Technology and Intellectual Policy 11, pp. 247.

234. In Singapore, the use of anonymised data is not subject to the PDPA[310]. Under the PDPA, data would be considered anonymised if there is no serious possibility that an individual could be re-identified from the data, taking into consideration both:

a. the data itself, or the data combined with other information to which the organisation has or is likely to have access; and

b. the measures and safeguards (or lack thereof) implemented by the organisation to mitigate the risk of identification.

235. There are many circumstances in which the use of non-aggregated anonymised data could be beneficial to organisations, deriving better insights and creating greater efficiencies. That being said, whilst the use of anonymised data is a good way in which businesses can carry out their data analytics, there is a residual risk of re-identification that would need to be accounted for. The PDPC adopts a multi-factor risk management approach in assessing the risk of re-identification, taking into account technological, process, legal and administrative controls. This is particularly relevant for big data analytics – through data meshing, data that may not appear to be personal data from the outset (e.g. environmental data), it could, in combination with other information being meshed, result in individuals being identified. This counterparty risk is a relevant consideration in analysing the risk of re-identification.

236. Internationally, data protection authorities have sought to provide clarity and methods that can be used by organisations to ensure that anonymised data is not re-identified. The PDPC has also issued a set of guidelines on anonymisation highlighting the methods and measures that organisations can put in place to mitigate the risks of re-identification.[311]

Interface between competition policy and law, and personal data protection law

237. The earlier sections have outlined the competition policy and law, and data protection issues that may arise in the context of data-driven industries. The following

[310] In the event that an organisation intentionally re-identifies an individual, such deliberate actions will constitute collection of personal data, for which consent is required from the relevant individual. There may be situations where the re-identification is unintentional. Generally, unintentional re-identification is not considered collection of personal data. However, the organisation should immediately delete the personal data or re-identifying information and should evaluate whether the risk management controls in place are adequate. If the organisation uses or discloses such unintentionally re-identified personal data, its actions will be considered to be use or disclosure of personal data. Generally, where such collection, use or disclosure is carried out for a purpose to which the relevant individuals did not consent, the organisation will have breached its PDPA obligations. See generally, Personal Data Protection Commission (Revised 28 March 2017). *Advisory Guidelines on the Personal Data Protection Act for Selected Topics*. pp. 17.

[311] See generally, Personal Data Protection Commission (Revised 28 March 2017). *Advisory Guidelines on the Personal Data Protection Act for Selected Topics*, pp. 17.

paragraphs look at the possible interactions of competition law and personal data protection law in the context of data.

Objectives of competition policy and law, and data protection are not mutually exclusive

238. The objectives of competition policy and law, and data protection are not mutually exclusive. Personal data represents a core asset for data-driven industries and the volume and quality of acquired personal data is a key differentiator for services offered by such businesses.

239. An emerging issue is data portability. In the EU for example, data protection legislation provides for the right to "data portability"[312] under Article 20 of the European Union's General Data Protection Regulation.[313] Data portability provides individual consumers with the right to request the incumbent firm to transmit their personal data to another firm in a structured, commonly used and machine-readable format.

240. From a competition policy perspective, the right to port data could make it easier for individuals to switch between different providers. Data portability rights could also assist to constrain the market power of an incumbent and reduce the barriers to entry for new businesses seeking to enter the market. In this context, the objectives of data protection and competition policy are aligned, in that consumers potentially benefit from having individual rights to data portability while competition in the market is also enhanced by the existence of such rights.

Compliance with one law used as a defence against the other

241. There may also be cases where businesses use compliance with data protection rules as a reason for not sharing data. For example, an upstream dominant firm possessing customers' data, may refuse to provide a downstream firm access to its database after the setting up of its own downstream subsidiary, on the basis of adhering to data protection rules. Such discriminatory access to data for competitors as discussed earlier may have an anti-competitive effect.[314] In assessing the legitimacy of such a claim, CCS will consider alternative ways in which businesses are actually able share data in compliance with data protection rules. For example, the sharing of anonymised data or aggregated data is unlikely to be subjected to the PDPA.[315] Even where personal data is shared, businesses could consider applying for exemption under PDPC's DSAs framework, should the criteria be met.

---

[312] A more detailed discussion on data portability can be found in Annex 2.

[313] Aysem Diker Vanberg and Mehmet Bilal Ünver (2017) *The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?* European Journal of Law and Technology 8(1), pp. 2.

[314] See discussion on discriminatory access to data at paragraphs 180 to 183 above.

[315] See paragraph 234 above on anonymised data.

242. There may also be instances where businesses use compliance with the Competition Act as an excuse for not sharing data. For example, a particular business may reject customers' requests to "port" their personal data over to their competitors on the basis that the sharing of commercially sensitive information with competitors may be caught under the Competition Act. However as discussed earlier in the data sharing section,[316] there is no concern with the sharing of data when it does not prevent, restrict or distort competition.

243. Given the possibility of such issues, CCS and PDPC will continue to work together to understand the boundaries of each agencies' regulations and assess the legitimacy of such claims by businesses.

Role of data protection in competition assessment

244. As discussed in Section VII, while there have been calls for competition law to be applied to promote data protection and privacy policy,[317] this is not consistent with the roles and function of the CCS. The mission of CCS is to make markets work well to create opportunities and choices for businesses and consumers in Singapore. In this regard, the CCS aims to ensure that markets are, and remain, competitive by protecting the competitive process. However, where data protection is a non-price competition factor, the treatment of personal data may affect how CCS considers and assess the competitive dynamics of a market.

[316] See discussion on data sharing at paragraphs 133 to 146 above.

[317] The EDPS suggests that competition law should be applied to promote data protection and privacy policy, and that data protection should be seen as a standalone factor in consumer welfare. This position is elaborated upon in the Preliminary Opinion of the EDPS (March 2014). *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*.

IX. IMPLICATIONS ON INTELLECTUAL PROPERTY RIGHTS

Intellectual property law

245. Intellectual property law regulates products of the human mind, or "intellect", and sets the legal boundaries of the type of conduct that may not be pursued without a right-holder's consent. The more common forms of recognised intellectual property rights across jurisdictions include: copyright and related rights; the protection of undisclosed information; trade marks; patents and industrial designs.[318]

246. Intellectual property rights enable rights-holders to exploit their intellectual property, and thereby recoup their investments in effort, time and financial resources expended in creating such property. This incentivises further creation and fosters an environment in which creativity and innovation can flourish.

247. In this age, intellectual property rights are far more than mere legal rights. They are highly valuable, strategic business assets; the market value of the world's top performing companies such as Apple, Microsoft, Amazon, and Facebook, lies in their intangible assets – such as patents, brands, data, and algorithms – and not their tangible ones.[319] As the cornerstone of the present innovation ecosystem, intellectual property is a powerful driver of growth for businesses and the economy in Singapore. Successful businesses leverage on their intellectual property rights to actively commercialise and monetise their intellectual property.

Intellectual property law issues relating to data analytics

248. Three broad issues will be discussed in the following sections. First, the extent to which intellectual property law protects data. Second, the emerging opportunities for commercialisation in the space where intellectual property rights, data and analytics converge. Third, the interface between intellectual property law and competition law, including what it means for providing supply of or access to any data and datasets protected under intellectual property law.

Extent of intellectual property protection over data

249. The fields of intellectual property law where issues of protection over data typically arise are copyright law and the law of confidence (in an action for breach of confidence). The below discussion is based on the position in Singapore, unless otherwise stated.

[318] Article 2 of the Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS) on the definition of the term "*intellectual property*" read with Sections 1 through 7 of Part II.
[319] Ocean Tomo LLC (March 2015). *Study of Intangible Asset Market Value*.

(a) Copyright Law

250. Facts and data *per se* are not protected under copyright law. However, a compilation of facts and data may be protected if it constitutes an intellectual creation by reason of the selection or arrangement of its contents.[320]

251. This distinction is exemplified in a series of cases where right-holders in various jurisdictions have sought copyright protection over telephone directories.[321] The individual listings of subscribers' names, telephone numbers and addresses may amount to facts and data that copyright law does not protect. It follows that the preparatory efforts or process of data collection, including any steps taken to verify the accuracy of the data, may also not be protected.[322] However, if these listings are selected or arranged with sufficient creativity, the selection or arrangement (but not the underlying facts and data) may attract copyright as a compilation – this could be the case where for example, the compiler arranges the data in a more ingenious manner than say, a mere alphabetical arrangement.[323]

252. This distinction reflects copyright law's goal of balancing private rights with public needs and interests: while copyright may protect for a limited period, right-holders' efforts in compiling facts and data, the facts and data per se must remain free for others to work on so that the public can benefit from further additions to the pool of

---

[320] Section 7A and 27 of the *Copyright Act*.

[321] Including in the United States (*Feist Publications, Inc v. Rural Telephone Service Company, Inc* 111 S Ct 1282 (1991); *Bellsouth Advertising & Publishing Corporation v. Donnelley Information Publishing, Inc* 999 F.2d 1436 (1993)); Australia (*Desktop Marketing Systems Py Ltd v. Telstra Corporation Ltd* 192 ALR 433 (2002)); and in Singapore, where the Court of Appeal recently opined on the issue in the case of *Global Yellow Pages Ltd v. Promedia Directories Pte Ltd and another matter* [2017] SGCA 28 **(*"Global Yellow Pages"*).**

[322] Such efforts may however, be protected outside the field of copyright law. The European Union for example, recognises a *sui generis* database right. Article 7(1) of the European Union Directive 96/9/EC of the European Parliament and Council of 11 March 1996 on the legal protection of databases requires member states to provide for a "*right for the maker of a database which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilisation of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database*". "*Database*" is defined in Article 2 as a "*collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means*".

[323] Refer to the Court of Appeal's observation in *Global Yellow Pages* that, "*[w]hat is common across the jurisdictions…is that each court seeks to characterise the human acts done and decisions made in reducing the universe of raw information into a work. There are, on the one hand, managerial decisions (whether to publish or update a phone directory) which clearly do not merit copyright protection. Then there are purely mechanical tasks (such as the algorithmic collection or arrangement of data) that, taken alone, would not cross the creativity threshold. Then there are choices in between that require human judgment and do impact the selection (such as the geographic area covered, the cut-off date, and the type of information that will be published) or the arrangement of the material (such as the order in which entries are sorted, and the order in which various fields of information are presented), and which might more properly be regarded as authorial in nature*".

results. Otherwise, the first compiler could gain a monopoly over the data in the compilation, particularly when the data can only be found in the compiler's work.[324] In such cases, a single compiler would have the power to control the growth of the pool of works for the consumption and benefit of the public.

253. This does not mean that the law does not offer any protection over facts and data *per se*; protection must simply be sought outside the field of copyright.

(b) Breach of Confidence

254. The law of confidence offers some measure of protection in this regard. Facts and data (and even databases) may be protected as confidential information in an action for breach of confidence. This involves enforcing an obligation of confidence that has arisen between parties in relation to some confidential information (the data) that has passed between them. Unlike copyright law, there is no need to distinguish between data and compilations, or satisfy any requirement for creative expression. Instead, the right-holder must satisfy the court that:

a. the data possesses the necessary quality of confidence about it. This means that the data must not be freely available in the public domain;

b. the data was imparted in circumstances importing an obligation of confidence; and

c. there was unauthorised use of the data, and in appropriate cases, to the detriment of the party who originally communicated it.

255. Confidential information that is of a sufficiently high degree of confidentiality may be protected as trade secrets. In such cases, former employees may be under implied obligations of confidence not to use or disclose trade secrets even after employment has ended. [325]

256. Examples of confidential information and trade secrets include information and data that businesses generate about their own activities, such as cost and pricing data, sales statistics, lists of customers and sources of supply, customer preferences, feasibility studies, market projections, and details of promotional strategies and expansion plans. Such business information may have vital competitive significance – it may in its own right carry a competitive advantage for a particular business, or serve

[324] This may be the case where the compiler is solely responsible for generating the data, or has obtained exclusive contractual rights of access to the data.

[325] Refer to the Court of Appeal's decision in *Man Financial (S) Pte Ltd (formerly known as E D & F Man International (S) Pte Ltd v. Wong Bark Chuan David* [2008] 1 SLR 663 at [85]. For the factors taken into consideration as to whether or not something constitutes a trade secret, refer to [83] of that decision.

an important auxiliary function in maintaining the competitive advantage conferred by the use of confidential information and trade secrets.[326]

257. Finally, over and above the protection afforded under intellectual property law, data may be protected by way of contract. Dealings[327] with data can potentially be enforced as contractual obligations independent of any intellectual property rights. Such obligations run the gamut – non-disclosure agreements, confidentiality clauses, employment contracts, collaboration agreements, and the terms of use of a website or a database.

Data analytics – New opportunities for commercialisation

(a) Proposed copyright exception for "text and data mining"

258. In the course of performing data analytics, copyrighted works (including compilations of facts and data) may be copied or reproduced, which may give rise to liability for copyright infringement. Such copying or reproduction could occur during the data collection[328] and data integration[329] processes described earlier in this paper. It could occur as part of an automated process,[330] particularly where big data is concerned, the manual analysis of a large volume of facts and data may simply be impossible or unfeasible.

259. Data analytics and interpretation present many new opportunities for businesses to monetise such work. At a national level, the insights gleaned from data analytics help to create and disseminate knowledge to the benefit of the public. Such activities are integral to Singapore's Smart Nation initiatives. To facilitate and encourage such activities, as part of a review of Singapore's copyright regime, a new exception to copyright infringement has been proposed to permit "*text and data mining*" activities.[331]

260. The proposed exception will allow the copying or reproduction of copyrighted works for the purpose of data analysis. Users of such copyrighted works must have legitimate access to the works in the first place (such as through paid subscriptions or access that is not locked behind a pay-wall[332]). While both commercial and non-commercial activities would be permitted under the proposed exception, the copying and reproduction must be for the purpose of data analysis to benefit from the

---

[326] Tanya Aplin, Lionel Bently et. al. (2012). "*Gurry on Breach of Confidence",* Oxford University Press, 2nd Edition, pp.178 – 179.

[327] Such as the data collection, integration, analytics, interpretation, sharing and monetisation identified earlier in this paper See para 22 to 26 above.

[328] See para 22(a) above.

[329] See para 22(b) above.

[330] Such as through the use of data analytics software described above: see para 22 to 23 above.

[331] Proposal 9, Public Consultation on Proposed Changes to Singapore's Copyright Regime, Ministry of Law and the Intellectual Property Office of Singapore, 23 August 2016.

[332] An arrangement where content is accessible only after payment.

exception; the exception is not intended to cover situations where the commercial benefit comes from the actual copies of the copyrighted works, instead of the data analysis.

261. Public consultation on the proposal has concluded, and the responses are currently under consideration by the Ministry of Law and IPOS. A further public consultation will be held in 2018 on any legislative amendments arising from the copyright review, including the introduction of the proposed exception.

(b) New opportunities for intellectual property commercialisation

262. In the field of patent law for example, data analytics has already begun to unlock new commercialisation opportunities.

263. Manual searches for patents are traditionally expensive and time-consuming. Often, only big businesses have the financial means to conduct extensive manual searches. With the advent of data analytics technology however, patent searches can be conducted far more economically, efficiently and accurately. Data analytics is hence accelerating patent commercialisation and dissemination of the knowledge embodied in these patents in a growing number of ways, including:

a. creating greater opportunities to match existing patent capabilities with the goals and needs of businesses. This includes opportunities for patents to complement offensive and defensive strategies in patent enforcement, revocation and litigation. [333] These opportunities increase the likelihood that a patent will be successfully commercialised;

b. assisting inventors and businesses in building their patent portfolios and business strategies – through the application of data analytics to conduct searches for prior art and review search results;[334] and

where used by search and examination authorities, improved prior art searches reduce legal and licensing barriers by preventing the registration of weak patents where prior art already exists.

---

[333] For example, data analytics may be used to conduct searches for prior art and review search results. Based on the search results, businesses may acquire patents to challenge its competitors' patents on the grounds of lack of novelty and create potential infringement risks for competitors. Building up a defensive patent portfolio can provide businesses with leverage for negotiating cross-licensing agreements with their competitors and grounds for a counterclaim in patent infringement proceedings.

[334] Section 14(2) of the Patents Act defines the state of the art (ie. prior art) as "*all matter (whether a product, a process, information about either, or anything else) which has at any time before the priority date of that invention been made available to the public (whether in Singapore or elsewhere) by written or oral description, by use or in any other way*".

Interface between competition policy and law, and intellectual property law

264. Both intellectual property law and competition law share the same basic objective of promoting economic efficiency and innovation.[335] Intellectual property law does this through the creation of legally-sanctioned zones of exclusivity, thereby creating incentives for innovation and the commercialisation and distribution of resultant products and services. Intellectual property protection restricts others from free-riding on the efforts of right-holders. Competition law, on the other hand, does this through the promotion of competitive markets and safeguarding of the competitive process.

265. Section 47 of the Competition Act promotes competitive markets by prohibiting companies possessing substantial market power from using their market power to exclude rivals to stifle competition. At first glance, this may appear to be in conflict with the operation of intellectual property law, which essentially gives the right to exclude use by others. However, the possession of an intellectual property right does not necessarily create market power in itself – the creation of a legal monopoly does not automatically create an economic monopoly.[336]

266. The legitimate exercise of an intellectual property right, even by a dominant undertaking, will not, in general, be regarded as an abuse of a dominant position. Typically, it is only in limited circumstances that the refusal to authorise a third party to use an intellectual property right may amount to a violation of competition law. Foreclosure through a refusal to supply may constitute an abuse of dominance to the extent that it is an attempt to maintain a monopoly in the market by, for example, edging out existing players, or preventing or discouraging the entry of new players. This is a factual analysis and has to be assessed in the context of the jurisdiction in which it arises.

267. In relation to data or data sets, the competition authority or courts in general are unlikely to require an intellectual property right-holder to grant access, unless such data or datasets are viewed as an essential facility,[337] or objectively necessary such that denying access would clearly foreclose competition and prevent the emergence of new products or services which the dominant player is not offering, thereby stifling innovation. The aforementioned ECJ cases as set out in section VII above are rare

---

[335] *CCS Guidelines on the Treatment of Intellectual Property Rights*, Para 2.1.

[336] *CCS Guidelines on Section 47 Prohibition 2016*, Para 4.2.

[337] This refers to the essential facilities doctrine as formulated by different courts in the United States but which is generally applied only under limited circumstances to give rise to antitrust liability. This aspect was highlighted by a report published by the United States Department of Justice and the Federal Trade Commission in April 2007 (*Antitrust Enforcement and Intellectual Property Rights: Promoting Innovation and Competition (2007)*, at pp. 28, quoting the decision in *Verizon Communications Inc. v. Law Offices of Curtis V. Trinko*, 540 U.S. 398, 408 (2004): "*compelling negotiation between competitors may facilitate the supreme evil of antitrust: collusion." The agencies noted that "imposing liability for such refusals [to license] arguably would go beyond requiring firms to refrain from anticompetitive conduct that harms rivals and would instead compel firms to reach out and affirmatively assist their rivals*."

instances and subject to very limited conditions for a finding of abuse of market dominance. Since data or data sets are accorded limited protection under Singapore's intellectual property laws (as explained in this section) and raw data sets are usually replicable, it is unlikely that competition authorities or courts would compel the supply of or access to data sets. What is key is the importance of innovation to foster competition when assessing an infringement of the section 47 prohibition.

X. CONCLUDING REMARKS AND NEXT STEPS

268. The accumulation, sharing, and analysis of data can bring about a wide range of benefits. For Singapore, the ability to capitalise on data analytics and data sharing provides a new avenue to promote economic growth through innovation and improvement in productivity. As illustrated in the KPMG report, these benefits include the optimisation of business operations and encouragement of innovation across all sectors. Consumers also benefit from reduced information asymmetry and search costs, and improved customer experience with more customised offerings. Beyond the economic benefits, there are also social benefits, including better-informed government policies through data analytics. However, these benefits may not be fully realised if businesses engage in anti-competitive conduct, or misuse personal data. Competition law ensures that businesses and consumers are protected from harmful anti-competitive conduct; personal data protection law ensures that an individual's personal data is safeguarded and businesses are able to leverage on personal data for legitimate use and innovation; while intellectual property rights provides incentives for individuals and businesses to innovate and conduct research.

Accumulation of data

269. The accumulation of a large data set in and of itself does not necessarily imply that a firm is dominant – having a large data set is but one of the factors to be considered in assessing whether a firm is dominant.[338] Dominance may be strengthened due to network effects, but can be weakened due to the existence of multi-homing, ease of access, substitutability of data, and the dynamics of markets. Even if a firm is found to be dominant, competition concerns will only arise when the firm engages in anti-competitive conduct that has an adverse effect on the process of competition, for example, by preventing competitors from competing effectively in the market.

270. A large data set may also not be protected by intellectual property rights. Firstly, copyright does not subsist in data collected by businesses. Copyright could subsist in a compilation of data, if sufficient creativity has been expended on it. Secondly, for data sets to be accorded the status of confidential information and protected against unauthorised disclosure, the conditions under the law of confidence as set out in paragraph 254 of this paper must be fulfilled.

[338] See paragraphs 163 to 177 on the considerations in assessing market power.

Sharing of data and use of algorithms

271. The sharing of data within the framework of existing rules can be pro-competitive. There is generally no competition concerns when the data shared is:

a. historical;

b. sufficiently aggregated and cannot be attributed to a particular business; and

c. not sensitive, strategic or confidential.

In contrast, the sharing of commercially sensitive data, such as existing or future prices or production data, with competitors, is likely to infringe the Competition Act.

272. PDPC has released a Guide to Data Sharing to provide greater clarity to businesses on how data can be shared in compliance with the PDPA, including for the purposes of data analytics. This guide also includes a framework for data sharing arrangements that may be exempted under the PDPA in circumstances where obtaining consent is impractical or undesirable.

273. The proposed amendment to the Copyright Act, if implemented, would clarify the use of legitimately accessed copyrighted works for data analytics, and thereby encourage data sharing and access for such purposes.

274. The use of algorithms allows businesses to make predictions and decisions more efficiently. They also help businesses achieve greater customisation in their product offerings. However, where algorithms are used to implement or facilitate collusive outcomes or anti-competitive agreements, either directly as between competitors or through a third party intermediary, this would likely infringe the Competition Act.

Data privacy

275. While there have been calls for competition law to be applied to promote data protection and privacy policy,[339] this is not consistent with the roles and functions of CCS. In this regard, CCS aims to ensure that markets are, and remain, competitive by protecting the competitive process. Where data protection is a non-price competition

[339] The EDPS suggests that competition law should be applied to promote data protection and privacy policy, and that data protection should be seen as a standalone factor in consumer welfare. This position is elaborated upon in the Preliminary Opinion of the EDPS (March 2014). *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*.

factor, the treatment of personal data may affect how CCS considers and assess the competitive dynamics of a market.

Next steps

276. Issues in competition law and policy, personal data protection law and intellectual property rights are expected to overlap in the context of data-driven industries. One of the areas where there is a potential overlap is data portability. Data portability seeks to enhance competition between businesses by reducing switching costs and facilitating the switching from one service provider to another. At the same time, it will also create a more user-friendly environment and builds trust, potentially leading to a virtuous cycle of users being more willing to provide personal data to companies. In this regard, PDPC and CCS will be embarking on a joint study to explore consumer protection and competition related issues of data portability, alongside PDPC's study of the benefits and risks in the increased use of algorithms in profiling and automated decision making in Singapore.

277. Overall, while the ease of compilation of large data sets and proliferation of data analytics may be fresh developments, the existing analytical frameworks are sufficiently flexible and robust to deal with the competition issues that may arise in data-driven industries. Nonetheless, CCS will stay vigilant, monitoring new developments to ensure it has the necessary tools to detect and deter any possible harm to competition in markets in Singapore that emerges from the use of technologies. Businesses should continue to operate on a level playing field even in a Big Data environment, to innovate, stay competitive, and better serve their customers.

ANNEX 1: Summary of data protection obligations under the PDPA

1. Consent Obligation

An organisation should only collect, use or disclose personal data for purposes for which an individual has given his or her consent.

An organisation should allow individuals to withdraw consent, with reasonable notice, and inform them of the likely consequences of withdrawal. Upon withdrawal of consent to the collection, use or disclosure for any purpose, an organisation must cease such collection, use or disclosure of the personal data.

2. Purpose Limitation Obligation

An organisation may collect, use or disclose personal data about an individual for the purposes that a reasonable person would consider appropriate in the circumstances and for which the individual has given consent.

An organisation may not, as a condition of providing a product or service, require the individual to consent to the collection, use or disclosure of his or her personal data beyond what is reasonable to provide that product or service.

3. Notification Obligation

An organisation must notify individuals of the purposes for which it is intending to collect, use or disclose their personal data on or before such collection, use or disclosure of personal data.

4. Access and Correction Obligation

Upon request, the personal data of an individual and information about the ways in which his or her personal data has been or may have been used or disclosed within a year before the request should be provided. However, organisations are prohibited from providing an individual access if the provision of the personal data or other information could reasonably be expected to:

- cause immediate or grave harm to the individual's safety or physical or mental health;
- threaten the safety or physical or mental health of another individual;
- reveal personal data about another individual;
- reveal the identity of another individual who has provided the personal data, and the individual has not consented to the disclosure of his or her identity; or
- be contrary to national interest.

Organisations are also required to correct any error or omission in an individual's personal data upon his or her request. Unless an organisation is satisfied on reasonable grounds that the correction should not be made, organisations should correct the personal data as soon as practicable and send the corrected data to other

organisations to which the personal data was disclosed within a year before the correction is made (or, with the individual's consent, only to selected organisations).

5. Accuracy Obligation

Organisations should make reasonable efforts to ensure that personal data collected by or on behalf of the organisation is accurate and complete, if it is likely to be used to make a decision that affects the individual, or if it is likely to be disclosed to another organisation.

6. Protection Obligation

Organisations should make reasonable security arrangements to protect the personal data that it possesses or controls to prevent unauthorised access, collection, use, disclosure or similar risks.

7. Retention Limitation Obligation

Organisations should cease retention of personal data or remove the means by which the personal data can be associated with particular individuals when it is no longer necessary for any business or legal purpose.

8. Transfer Limitation Obligation

Organisations should transfer personal data to another country only according to the requirements prescribed under the regulations, to ensure that the standard of protection provided to the personal data so transferred will be comparable to the protection under the PDPA, unless exempted by the PDPC.

9. Openness Obligation

Organisations should make information about its data protection policies, practices and complaints process available on request.

Organisations should also designate one or more individuals as a Data Protection Officer to ensure that the organisation complies with the PDPA, including the implementation of personal data protection policies within the organisation. The business contact information of at least one of such individuals should also be made available to the public. Compliance with the PDPA remains the responsibility of the organisation.

There are, however, exceptions to these rules and they are generally purpose-based. For example, some of these exceptions relate to emergency situations, investigations, publicly available data or where the personal data is used for evaluative purposes. The exceptions are contained within the Second to Sixth Schedules of the PDPA.

ANNEX 2: Primer on Data Portability

1. An emerging issue arising from data protection legislation is the right to "data portability." Article 20 of the GDPR creates a new right to data portability, which can be viewed as an extension to right of access.[340] Individuals making use of their right of access under the Data Protection Directive 95/46/EC were constrained by the format chosen by the data controller to provide the requested information. The right to data portability, by contrast, extends this right to access and consists of two main elements, namely: the right of data subjects to receive the personal data that they have provided to a controller; and the right to receive this personal data in a structured, commonly used and machine-readable format, and to transmit the data to another data controller. The purpose of this new right is to empower the data subject and accord more control over the personal data concerned[341].

2. Given the right to data portability also includes the direct transmission of personal data from one data controller to another, the right to data portability is also intended to support the free flow of personal data in the EU and foster competition between data controllers. Personal data represent a core asset for Internet companies and the volume and quality of acquired personal data is a key differentiator for services offered by such companies. The acquisition of such data creates a "first mover advantage", for large Internet companies, but by extension, raises the barriers to entry for their competitors.[342] The EU envisions that data portability will facilitate the ease of switching between different service providers and foster the development of new services under its envisaged Digital Single Market. The EU has further argued that this data portability right also represents an opportunity to "re-balance" the relationship between data subjects and data controllers, through the affirmation of individuals'

[340] Aysem Diker Vanberg and Mehmet Bilal Ünver (2017). *The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?* European Journal of Law and Technology 8(1), pp. 2.

[341] Article 20 Right to data portability 1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and (b) the processing is carried out by automated means. 2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible. 3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. 4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others. See, European Commission. (27 April 2016). *EU General Data Protection Regulations 2016*. Office Journal of the European Union, pp. 45.

[342] D. Geradin and M. Kuschewsky (February 2012). *Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue*, pp. 2.

personal rights and control over the personal data concerning them. Crucially, it was highlighted in the Working Party 29 guidelines,[343] that the primary aim of data portability is to facilitate switching from one service provider to another, thus enhancing competition between services (by making it easier for individuals to switch between different providers). The advantages of data portability, therefore, are largely envisioned from the consumer protection perspective. Easier transfers from one service provider to another for users of online services, will create a more user-friendly environment and could build trust, potentially leading to a virtuous cycle of users more willing to provide personal data to companies.[344]

3. Criticisms of the right to data portability have included the potential commercial disincentives of data portability requirements from the perspective that valuable proprietary information, which concedes significant advantage over competitors[345], and intellectual property arising from the accumulation of an individual's personal data, could discourage companies/service providers from collecting and creating the proprietary information in the first place.[346] In particular, such companies or service providers will, in most cases, be required to transfer the data to their direct competitors. This creates intellectual property risks, as the demarcation between who owns the data and to what extent the data is considered personal data (and hence the right of the individual to port), remains unclear.[347]

4. Interoperability and requirements for portability are not new concepts in the context of encouraging competition. A case in point is that of operator portability for telephony. Operator portability refers to the ability to retain a telephone number when switching a carrier.[348] Many countries require telephone and mobile service providers to put in place mechanisms to enable number portability. Arguments supporting portability have often been made in relation to the advantages of consumer choice. That, in turn, results in a more competitive telecommunications market, as well as limits the market power of the large players in a given industry.[349] However, whether

---

[343] Article 29 Data Protection Working Party (Revised 5 Apr 2017) *Guidelines on the right to data portability*, pp. 5.

[344] Barbara Van der Auwermeulen (February 2017). *How to attribute the right to data portability in Europe: A comparative analysis of legislations*. Computer Law and Security Review 33(1), pp. 59.

[345] D. Geradin and M. Kuschewsky (February 2012). *Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue*, pp. 3.

[346] Aysem Diker Vanberg and Mehmet Bilal Ünver (2017). *The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?* European Journal of Law and Technology 8(1), pp. 5.

[347] Barbara Van der Auwermeulen (February 2017). *How to attribute the right to data portability in Europe: A comparative analysis of legislations*. Computer Law and Security Review 33(1), pp. 60.

[348] Reiko Aoki and John Small (August 2010). *The Economics of Number Portability: Switching Costs and Two-Part Tariffs*. Hitotsubashi University Repository, pp. 4.

[349] Stefan Buehler et al. (August 2006). *Mobile Number Portability in Europe*. Telecommunications Policy Vol. 30, pp.386.

operator portability requirements translate into positive effects on competition and consumer choice has been called into question. For example, in the United States, a study found that the number of consumers switching was about 25% of the initial predicted figures, and smaller mobile subscribers did not necessarily add new subscribers, whereas bigger carriers did.[350]

5. When compared to the data portability requirements under the GDPR, operator portability is comparatively simpler, and likely to incur lower costs to facilitate –given that tracking a database of phone numbers and porting numbers is technically more straightforward than ensuring entire datasets about an individual are in a machine readable and compatible format. Notably, the broad application of the GDPR means that where competition law would typically seek to limit market dominance (and potential abuse of market dominance) by large incumbent market players,[351] in this case, the data portability requirements apply equally to even the smallest start-ups.

6. The cost of compliance to the GDPR data portability requirements remains untested. If compliance costs turn out to be significant, the effect of the GDPR's data portability requirements could result in similar market effects experienced by telephone operators in the US. This, coupled with the potential loss of proprietary rights over data collected, would likely stifle innovative small start-ups and further cementing the positions of industry incumbents.

7. Other concerns raised by commentators on data portability requirements relate to privacy and security risks, particularly when data is transferred from one data controller to another, certainly as the number of requests for transfers increase, and the relative security capabilities of companies transferring could vary significantly. Preliminary interoperable solutions suggested in the GDPR have also been criticised as potentially aggravating security concerns,[352] at the expense of uniform rules and processes and that interoperability increases the risk of security vulnerabilities.[353]

[350] Dong Hee Shin (February 2007). *A study of mobile number portability effects in the United States*. Telematics and Informatics 24(1), pp. 2.
[351] Peter Swire and Yianna Lagos (31 May 2013). *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*. Maryland Law Review 72(2), pp. 339.
[352] Aysem Diker Vanberg and Mehmet Bilal Ünver (2017). *The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?* European Journal of Law and Technology 8(1), pp. 6.
[353] Stefan Weiss (August 2009). *Privacy threat model for data portability in social network applications*. International Journal of Information Management. 29(4), pp. 251.