Database Consultants Australia ("DCA") hereby encloses for the consideration of the Australian Competition and Consumer Commission ("ACCC") comments on the Digital Platform inquiry March 2024 report on data Brokers

About DCA

DCA is an Australian owned private company providing specialised software development, data engineering and business information services. We have provided services to corporate Australia and federal, state and local governments for over 25 years.

DCA has two trading companies that broadly fall within the scope of the ACCC report: IncNet and Marketbase. IncNet holds a database comprising business-to-business data, and Marketbase is a digital platform application that provides access to self-service segments of business information.

About this submission: key points

DCA submits this submission in good faith to extend the ACCC's understanding of the data brokerage market in Australia and to recommend specific areas of interest to the attention of the ACCC, including the following key points.

- There is significant need to distinguish between professional business information and personal information to secure Australians' private information while preserving the Australian data broker sector. Regulatory controls consistent with recent Singaporean and Canadian legislation are exemplary precedent in this regard.
- Data brokers in Australia are a significant enabler of competition. Small and medium businesses lack resources to compete with large organisations on the basis of first-party data, and data brokers are a vital bridge across that gap.
- International competition is fierce and the internet does not readily support geopolitically defined jurisdictional boundaries. Australians' business data is collected and used by organisations that are not registered in Australia, so any prospective regulation levied upon Australian registered businesses must be considered in the context of the international market.
- There is evident need to extend and improve the education of consumers as regards use of their data, particularly their personally identifiable data.

Question 2. How do data brokers compete? What factors do data brokers differentiate themselves on (e.g., price, range of data, specific types of data, analysis undertaken, additional services offered)?

Data brokers are not typically offering bulk caches of disorganised data—most of their customers would not have the skills or internal resources to use that information to any great effect. Brokers package data into specific services or products, and will generally offer recommendations to customers as to what kind of data service or product will best fit their requirements at that time.

For example, DCA's customers often require data services and products that can achieve the following goals:

- **Enrichment of first party customer data** to append missing information for sales, marketing, risk management and market research as well as compliance and accuracy

- **Service demand and supply analysis** to locate areas of investment need in order to meet changing demand in the market (especially for government and not for profit clients)
- **Market research** to understand the broader market for a new product or service
- **Prospect marketing** to identify promising potential customers or suppliers and contacting them professionally
- **Risk management** applications that enable organisations to avoid risky companies and markets based on their own risk appetite
- **Data governance and compliance** to ensure data is accurate, complete and up to date
- **Recruitment and talent management** to support recruiters and HR professionals to find the right resources
- **Business information reporting** by means of a combination of first party information and DCA's business information data to create new business intelligence reports
- **Spatial analytics** using geographical and technographical data to assist with connection of corporate services and assessing supply against demand
- **Company risk index research** to identify high risk segments according to public notice insolvencies
- **Lead generation tools** to identify the professional contact information of prospective target market

Question 3. How difficult is it for new data brokers to enter the Australian market? What are their entry strategies (e.g., expansion of overseas data brokers into Australia, expansion of other businesses into data broking, new entrants)? Does this differ depending on the types of data products or services provided?

The landscape is highly competitive. International business-to-business (B2B) data brokers compete directly against Australia brokers, often without an Australian registered business, taking market share and using their scale to process millions of professional contact records. It is a challenging market for Australian brokers to enter.

Most providers process professional business contact information and make their databases available to B2B customers with a password-protected key. Many of these international providers, process personal information under the basis of "legitimate interest" as described in Article (6 (1) (f) of the GDPR. Legitimate interest is also further emboldened by Recital 47, which states, "the processing of personal information for direct marketing purposes may be regarded as carried out for a legitimate interest."

DCA competes on this basis of our local knowledge of the market and our high quality, well-sourced data combined with skilled services. Increased data collection costs and impractical regulatory controls levied at Australian data brokers will make Australian businesses less competitive.

Question 4. What are the benefits of data brokers? Who do they benefit? Does this vary by data broker? If so, how?

Those companies able to collect information on a first-party basis are overwhelmingly large and well-resourced organisations. Examples in the Australian market include telecommunications giants and large financial institutions.

This concentration of size, scale and influence can also be extended to industries with market oligopolies, like retail grocery and rewards programs.

They have the scale and expertise to and deploy sophisticated data tools and techniques over their data and can design sophisticated marketing campaigns to improve profits and revenues

McKinsey's 2019 report, cited by the issues paper to which this submission responds, revealed that data analysis—particularly using "big data," which here means very large repositories of up to date and accurate information—is vital to organisations wishing to expand their market share. This is true in DCA's experience as well. That's why third-party data brokers are critical enablers of competition for smaller and medium sized businesses in Australia.

Businesses that have access to significant internal resources and large customer bases are unlikely to be as affected by regulations imposed on third-party data brokers as are small and medium businesses.

Additionally, there exists the problematic perception that data brokers are used mainly for sales purposes. This perception is faulty. There are many reasons organisations connect with data brokers, and the benefits they receive, while valuable, may not be as easy to measure as sales figures.

As an example, DCA is a broker of the Australian Death Check, which is an Australian Government database containing more than 3 million death records. This is a popular service provided to non-profits in Australia—donors are often elderly, and many non-profits are strongly committed to handling the passing of valued donors with grace and sensitivity. They're typically averse to soliciting regular donations from individuals who are deceased, and want to be sensitive to grieving family members. The Australian Death Check is a service that can make families much more likely to receive a letter of condolence than a request for a monthly donation.

Instead of accessing this service directly, organisations wishing to use the data are required to go through an authorised data service broker.

This is one illustrative example of how data brokers offer benefits that are more difficult to quantify than simply maximising sales.

Question 7. Are there any particularly important or must-have sources of information for data brokers to collect? If so, what are they and who supplies these (e.g., digital platforms)?

In its capacity as a data broker, DCA primarily uses three information sources, which are of high value to its clients: Australian Government sources, Australia Post and publicly available information taken from digital platforms.

1. DCA collects information from a number Australian Government agencies.
   a. DCA deploys the Australian Bureau of Statistics (ABS) ANZSIC code to segment its data into industry sectors. This enables Australian businesses to conduct market research for purposes such as measuring the size of a market sector, to facilitate building a business case, or for reviewing an investment opportunity.

b. DCA also provides the "Australian Death Check," which is sourced from Registers of Births, Deaths and Marriages. This is used for the purposes of cleaning aged customer databases.

    i. It is worth noting in this discussion of data sources and their provisions, that services such as the Australian Death Check, of which DCA is a broker, require the dates of birth of relevant constituents to be provided. In seeking to manage its own risk in a climate of increasing regulation, DCA has ceased to use certain additional brokers to append these birth dates and now outsources this function to avert that risk. In the frankest terms: regulatory complexity, alongside lack of clarity, has already made competition more challenging within this market.

c. DCA augments its B2B business information data with ABS Census data. This assists with identifying supply and demand for services in conjunction with state government service providers and charity-based organisations. By way of example, DCA is able to identify high and low concentrations of health practitioner specialists. Such services can identify deficiencies of services in remote and rural locations and support national services like Nurse on Call.

d. DCA also uses geocoded address data and attributes on commercial properties. When combined with DCA's corporate data, opportunities for information and communications technology infrastructure upgrades can be identified, as can strong opportunities for renewable energy products. This information is also used for developing energy consumption modelling to assist small businesses to reduce their costs.

2. DCA uses information sourced from Australia Post

a. Australia Post is a critical information source for address changes in Australia. Often, organisations collect address information from their customers, but need assistance to preserve the accuracy of that information over time.

3. DCA uses publicly available information

a. Certain platforms exist for businesses, and professionals who are operating in their capacity as representatives of businesses, to list their information publicly. These include locations such as public industry registers (for example, national Boards for health practitioners, which appends primary practice post codes to each registered health practitioner, assisting with confirming geographical coverage for specialist services) or digital platforms such as LinkedIn, on which professionals post information about themselves with the intention of professional networking.

Key recommendation: maintain and enable data broker access to government information sources.

Question 16. What benefits do data broker products and services provide to consumers and small businesses?

As discussed in answers to question 4, data brokers are critical enablers of competition for smaller and medium sized businesses in our country.

Big data analytics have become important to business. That is what McKinsey found in 2019, and it is still true in 2023. But it is a highly problematic truth when it comes to the data strategies of smaller and medium-sized Australian businesses for two broad reasons:

1. Small and medium sized Australian companies rarely enjoy a sufficient customer base to be effective users of *first*-party data when compared with larger organisations. A larger, and more complete, sample reduces problems with bias and inaccurate outputs. This is just as true in business intelligence as it is in any other branch of research.
2. Small and medium sized Australian companies are rarely able to accrue the skilled data workers and necessary resources to operate "big data" analyses to the same benefit as larger organisations.

In its role as a data broker, the preponderance of DCA's customer base is small and medium organisations.

Key recommendation: the ACCC should carefully consider the changing landscape and the key role B2B brokers play in helping small businesses compete against larger businesses when reviewing potential regulatory action.

Question 18. What consumer harms may arise from the use of data products and services sold or provided by data brokers? Which consumers are most likely to be harmed and why?

There is a significant danger to consumers in the conflation of business and personal data. These two concepts must be explicitly defined and separated.

It is DCA's view that consumer harms arise chiefly from the unethical collection and distribution of identifiable personal, private information. To cite one well-known report from Human Rights Watch, the Covid-19 pandemic saw education technology solutions rolled out to machines primarily used by children without regard for their personal information. That report, *Children's Rights Violations by Governments that Endorsed Online Learning During the Covid-19 Pandemic,* can be found here.

A clear distinction between identifiable personal, private information and business and professional information is desirable because it will enable more significant protection to be afforded for the former, and clearer exemption to be provisioned for the latter.

This is of course a matter of interest for the ongoing review of privacy legislation in Australia, which, as acknowledged by the issues paper, is outside the ACCC's remit. But this necessary separation of business and professional information from personal information is also a matter for the attention of the ACCC, because:

a) the provision of data and data services to small and medium enterprises is critical to their ability to compete within Australia (as mentioned in question 16), and

b) the imposition of onerous regulations on this market has the potential to make Australian businesses less competitive both domestically, and on an international scale.

The internet does not easily support geographically limited jurisdictions, and information relating to Australians is collected by organisations hosting and processing their information outside Australia. Without taking drastic regulatory steps—like making entire digital services inaccessible to Australians—the imposition of significant regulations in this area would hamstring Australian businesses seeking to compete on an international level.

Looking to international examples, Singapore and Canada are both countries which have managed data protection and applied practical considerations on the use of business information. For example, Singapore has comprehensive privacy legislation covering all personal information: the Personal Data Protection Act (PDPA). The PDPA defines personal information as data about an individual who can be identified from that data, or other information to which the organisation has or is likely to have access. The PDPA generally does not apply to:

- Any individual acting in his or her capacity as employee with an organisation
- Business contact information such as individual's name, position or title, business telephone number, business address, business fax information and similar information. Additional information on PDPA can be found here.

Canada has also excluded business contact information from its PIPEDA. Additional information can be referenced here.

Australia also has at least one domestic example of legislation that makes a clear distinction between personal information and business information: the Do Not Call Register Act. It's impermissible under the Do Not Call Register Act to add primarily business numbers to the register, even if they are also used for personal and private communications otherwise. This is an example of a piece of legislation that draws a reasonable distinction between business and professional information and personal information.

Key recommendations:

1. **The ACCC should adopt regulatory controls and an approach consistent with the Singaporean and Canadian regulations, and in line with precedent set by other Australian legislation.**
2. **A clear distinction between personal information and business and professional information is desirable to preserve the competitive prowess of legitimate Australian data brokers while protecting vulnerable consumers' personal information.**

Question 19. What processes and controls do data brokers have in place to protect consumers? This may include efforts around the de-identification and aggregation of data, data verification processes to ensure data is accurate, or measures to protect stored data.

DCA and its customers are considered independent controllers of data. As such, it is incumbent upon both DCA and our customers to own independent compliance practices around the data collection, processing and storage of data. DCA adheres to several specific, internationally-recognised standards to protect stored data.

- ISO27001 certification is essentially a distillation of industry best practice standards for information security management systems. It's used to help companies limit their risk in a landscape of rising cybersecurity complexity, and protects the data held by those companies from exposure.
- PCI-DSS certification refers to the payment card industry data security standard, which ensures the highest standard of security for highly sensitive credit card information.

DCA is also a member of the Association for Data Driven Marketing and Advertising (ADMA), a peak industry body offering guidelines, industry education and support for businesses engaged with data driven marketing or advertising.

a) Are these controls adequate? What more could/should be done?

Data breaches are often the result of existing industry standards and otherwise good protocols not being correctly followed, rather than faulty protocols or standards.

In some cases, individuals within an organisation may be incentivised by compelling short-term business reasons to circumvent overly complex policies. In other cases, existing policies are not well understood across a whole organisation.

A combination of:

a) consumer and professional education as to the realities of the data security landscape, and

b) implementing stronger incentives to adhere to existing information security policies

may be efficacious in improving the security of stored data.

Question 20. To what extent are consumers aware that their data is being collected and used by data brokers? How are they are made aware?

Regarding information sources used by DCA, consumers are, broadly, aware that their data is collected and used by data brokers, although it should be acknowledged that they are not always aware of what data or to what extent. Consumers are aware that any information they elect to share about themselves in publicly accessible forums is available to any person or organisation who chooses to access it.

The notice and consent model is used by platforms where user data is collected, as well as surveys conducted by government agencies.

Question 21. What steps can consumers currently take to inspect and/or remove the data that is held about them or to otherwise raise a complaint with data brokers?

Ethical data brokers do provide a clear way for consumers to access, correct or opt-out of the use of identifiable personal data, as well as an appropriate avenue for complaints, and a notification that any unsatisfactorily resolved complaint may be referred to the OAIC.

DCA uses the privacy policy section of its website for this purpose.

Question 22. What bodies or resources exist to assist and support consumers in their dealings with data brokers? What more could be done to better educate and empower consumers?

The Office of the Australian Information Commissioner is the key resource for consumers about whom personal data may be held by brokers. Although the OAIC maintains a significant body of self-education materials about privacy and information rights, consumers must be proactive in seeking them out.

Significantly, more than half of the respondents to *the Australian Community Attitudes to Privacy Survey 2023* reported that they care about their data but do not know what to do about it. This identifies a clear public education gap that must be targeted for closure.